Contents

Preface

Audience vi
Documentation Accessibility vi
Related Documents vi
Conventions vii

What's New in This Guide

New Features in Release 12c (12.2.1.3.0) viii
New Features in Release 12c (12.2.1.2.0) ix
New Features in Release 12c (12.2.1.1.0) ix

1 Introduction to Identity Governance Framework

1.1 Overview of the Identity Governance Framework 1-1
   1.1.1 Benefits of Identity Governance Framework to Organizations 1-2
   1.1.2 Benefits of Identity Governance Framework to Developers 1-2
1.2 Understanding Identity Governance Framework APIs 1-3
1.3 System Requirements and Certification for Identity Governance Framework 1-4

2 Using the Identity Directory API

2.1 Overview of the Identity Directory API 2-1
   2.1.1 Understanding Identity Directory API 2-2
   2.1.2 Identity Directory Service Architecture 2-2
2.2 Identity Directory API Configuration 2-4
   2.2.1 Logical Entity Configuration for an Identity Directory Service 2-5
      2.2.1.1 Properties of a Logical Entity Configuration 2-5
      2.2.1.2 Attributes of a Logical Entity Configuration 2-5
      2.2.1.3 Properties of a Logical Entity Definition 2-6
      2.2.1.4 Properties of a Logical Entity Relationship 2-7
   2.2.2 Physical Identity Store Configuration for an Identity Directory Service 2-7
   2.2.3 Operational Configuration for an Identity Directory Service 2-7
2.3 Design Recommendations for Identity Directory API 2-8
2.3.1 Minimizing Use of defaultFetch Attributes 2-8
2.3.2 Initializing the Identity Directory Once 2-8
2.4 Examples of Using the Identity Directory API 2-8
2.4.1 Initializing and Obtaining Identity Directory Handle 2-10
2.4.2 Initializing and Obtaining Identity Directory Handle from JPS Context 2-12
2.4.3 Initializing and Obtaining In-Memory Identity Directory Handle 2-13
2.4.4 Adding a User 2-15
2.4.5 Obtaining a User for Given Principal 2-15
2.4.6 Modifying a User 2-16
2.4.7 Obtaining a User for Given ID Value 2-16
2.4.8 Searching Users Using Complex Search Filter 2-16
2.4.9 Changing User Password 2-17
2.4.10 Resetting User Password 2-17
2.4.11 Authenticating a User 2-18
2.4.12 Deleting a User 2-18
2.4.13 Creating a Group 2-18
2.4.14 Searching Groups 2-19
2.4.15 Obtaining Management Chain 2-19
2.4.16 Obtaining Reportees of a User 2-19
2.4.17 Adding a Member to a Group 2-20
2.4.18 Deleting a Member From a Group 2-20
2.4.19 Obtaining All The Groups For Which User is a Member 2-21
2.4.20 Using Logical NOT Operator in a Search Filter 2-21

3 Using the ArisID API

3.1 About the ArisID API 3-2
3.2 Configuring the ArisID API 3-3
3.2.1 Examining CARML Files 3-4
3.2.2 Configuring the Identity Repository 3-4
3.2.3 Configuring the Mapping File 3-5
3.3 Design Recommendations for the ArisID API 3-5
3.3.1 About Unique Identifier Configuration 3-6
3.3.2 About Unique Key Attribute Specification 3-6
3.3.3 About Multiple Language Support 3-6
3.3.4 Handling Large Results 3-7
3.3.5 Securing the Application 3-7
3.3.5.1 Applying Domain Level Credentials 3-8
3.3.5.2 Applying Application Level Credentials 3-8
3.3.6 Configuring the Timeout Interval 3-9
4 Migrating to Identity Directory API

4.1 Overview of Migrating to Identity Directory API 4-1
4.2 Migrating the Application to Identity Directory API 4-2
    4.2.1 Initializing API 4-2
    4.2.2 Getting UserManager and GroupManager Handle 4-3
    4.2.3 Searching Filter 4-3
    4.2.4 Performing CRUD Operations 4-3
        4.2.4.1 APIs to Find a User 4-4
        4.2.4.2 APIs to Search a User 4-4
        4.2.4.3 APIs to Create a User 4-4
        4.2.4.4 APIs to Delete a User 4-5
        4.2.4.5 APIs to Authenticate a User 4-5
        4.2.4.6 APIs to Modify Users and Manage Related Entities 4-5
    4.3 Understanding the Comparison Between User and Role API With IDS API 4-6
        4.3.1 Comparison of User-Related APIs With Identity Directory APIs 4-6
        4.3.2 Comparison of Role-Related APIs With Identity Directory APIs 4-9
    4.4 Moving From a Test to a Production Environment 4-11
        4.4.1 Overview of Moving Between Environments 4-12
        4.4.2 Modifying Identity Directory Service/libOVD Move Plan 4-12
            4.4.2.1 Locating Identity Directory Service/libOVD configGroup Elements 4-13
            4.4.2.2 Properties to Customize for Identity Directory Service/libOVD Move Plan 4-14
    4.5 Tuning Configuration Parameters for IDS 4-15
        4.5.1 Configuration Parameters for IDS 4-16
        4.5.2 WLST Commands to Set Tuning Parameters Using File-Based Configuration 4-17
        4.5.3 Constants to Set Tuning Parameters Using In-Memory Configuration 4-18
        4.5.4 Handling Firewall and Load Balancer Timeout Errors 4-19
        4.5.5 Configuring TLS Protocol Versions and Cipher Suites for Secure Connections 4-19
    4.6 Allowing Pass-through Attributes in IDS 4-19
Preface

This guide provides an introduction to Identity Governance Framework and describes how to use the related developer APIs Oracle has made available. It describes the Identity Directory API, which is a common service for identity management applications to access and manage identity information.

• Audience
• Documentation Accessibility
• Related Documents
• Conventions

Audience

This document is intended for developers who are writing applications that use the Oracle Fusion Middleware Identity Governance Framework based APIs.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

• Java API Reference for Identity Governance Framework Identity Directory
• Java API Reference for Identity Governance Framework IDXUserRole
• Java API Reference for Identity Governance Framework UserRole
• Securing Applications with Oracle Platform Security Services
• Oracle® Fusion Middleware Infrastructure Security WLST Command Reference
• Javadocs for Project Aristotle - ArisID Attribute Services, at: http://arisid.sourceforge.net/javadocs/arisId_1.1_javadoc/
Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
What's New in This Guide

Review the new features and significant product changes for the Identity Governance Framework (IGF) and the related developer APIs.

- **New Features in Release 12c (12.2.1.3.0)**
  The new features and major changes introduced in release 12.2.1.3.0 are as follows:

- **New Features in Release 12c (12.2.1.2.0)**
  This revision contains no new features. Minor updates were made throughout the guide.

- **New Features in Release 12c (12.2.1.1.0)**
  The new features and major changes introduced in release 12.2.1.1.0 are as follows:

---

**New Features in Release 12c (12.2.1.3.0)**

The new features and major changes introduced in release 12.2.1.3.0 are as follows:

- **Support for TLS Protocol Versions and Cipher Suites for Secure Connections**
- **Deprecated Features**
- **Support for TLS Protocol Versions and Cipher Suites for Secure Connections**
- **Deprecated Features**
  Identity Governance Framework introduces some behavioral changes in the 12c (12.2.1.3.0) release. This includes deprecated and desupported features and components.

---

**Support for TLS Protocol Versions and Cipher Suites for Secure Connections**

You can configure TLS protocol version and cipher suites using the WLST commands for the libOVD adapter.

See [Configuring TLS Protocol Versions and Cipher Suites for Secure Connections](#).

---

**Deprecated Features**

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

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

This section contains the following topics:

• From 12c (12.2.1.3.0) release onward, the following Javadocs are deprecated:
  – Java API Reference for Identity Governance Framework IDXUserRole
  – Java API Reference for Identity Governance Framework UserRole
Oracle recommends the use of Identity Directory API. See Java API Reference for Identity Governance Framework Identity Directory.

• Deprecation of Using the ArisID API functionality from 12c (12.2.1.3.0) onward.

New Features in Release 12c (12.2.1.2.0)

This revision contains no new features. Minor updates were made throughout the guide.

New Features in Release 12c (12.2.1.1.0)

The new features and major changes introduced in release 12.2.1.1.0 are as follows:

• New IDS Tuning Configuration Parameters

• New IDS Tuning Configuration Parameters
  New configuration parameter Protocols has been added for tuning your IDS deployment.

New IDS Tuning Configuration Parameters

New configuration parameter Protocols has been added for tuning your IDS deployment.

See Configuration Parameters for IDS.
1

Introduction to Identity Governance Framework

The Identity Governance Framework (IGF) initiative enables secure exchange of identity-related information between users and applications and service providers. It provides privacy and governance semantics to applications and services infrastructure.

The following topics provide an introduction to the Identity Governance Framework and the related developer APIs Oracle has made available:

• Overview of the Identity Governance Framework
• Understanding Identity Governance Framework APIs
• System Requirements and Certification for Identity Governance Framework

1.1 Overview of the Identity Governance Framework

The Identity Governance Framework enables enterprises to define standards that secures the exchange of identity information and regulates compliance between applications both internally and with the external world. Identity information may include data such as names, addresses, numbers, and other information associated with an individual's identity.

The Identity Governance Framework is designed to meet the following goals:

• To simplify the development of identity information access regardless of where that information is stored.
• To simplify the management (also known as governance) of how applications use identity data, in particular, sensitive data.
The specifications provide a common framework for defining usage policies, attribute requirements, and developer APIs pertaining to the use of identity-related information. These enable businesses to ensure full documentation, control, and auditing regarding the use, storage, and propagation of identity-related data across systems and applications.

This section contains the following topics:

- Benefits of Identity Governance Framework to Organizations
- Benefits of Identity Governance Framework to Developers
- Benefits of Identity Governance Framework to Organizations

The Identity Governance Framework makes use of the policies and standards that help support enterprise security and provides an assurance to the users that the identity information is secured and managed appropriately by the parties to whom it has been entrusted.

- Benefits of Identity Governance Framework to Developers

The Identity Governance Framework is an agreed-upon process for specifying how identity-related data is treated when writing applications. This provides developers a standard approach to write applications that use this data so that governing policies can be used to control it. This results in faster development of privacy aware applications.

1.1.1 Benefits of Identity Governance Framework to Organizations

The Identity Governance Framework makes use of the policies and standards that help support enterprise security and provides an assurance to the users that the identity information is secured and managed appropriately by the parties to whom it has been entrusted.

Organizations need to maintain control and integrity of sensitive personal information about their customers, employees, and partners. Data related to social security numbers, credit card numbers, medical history and more are increasingly under scrutiny by regulations seeking to prevent abuse or theft of such information. Privacy conscious organizations frequently have reacted to these requirements by enforcing overly strict controls and processes that hinder business operations and impact productivity, flexibility, and efficiency. At the opposite end of the spectrum, some organizations do not take the care needed to safeguard this information, potentially putting identity-related data at risk without sufficient oversight and control. The Identity Governance Framework enables a standards-based mechanism for enterprises to establish "contracts" between their applications so that identity related information can be shared securely and with confidence that this data will not be abused, compromised, or misplaced. Using this framework, organizations have complete visibility into how identity information is stored, used, and propagated throughout their business. This enables organizations to automate controls to streamline business processes without fear of compromising the confidentiality of sensitive identity related information.

1.1.2 Benefits of Identity Governance Framework to Developers

The Identity Governance Framework is an agreed-upon process for specifying how identity-related data is treated when writing applications. This provides developers a standard approach to write applications that use this data so that governing policies
can be used to control it. This results in faster development of privacy aware applications.

IGF enables the decoupling of identity-aware applications from a specific deployment infrastructure. Specifically, using IGF enables developers to defer deciding how identity related information will be stored and accessed by their application. Developers do not need to worry about whether they should use a SQL database, an LDAP directory, or other system. In the past, developers were forced to write highly specific code, driving technology and vendor lock-in.

For example, the Identity Directory API provides methods for accessing and managing identity information in a directory server that is the domain identity store. Entity definitions, entity relationships, and the physical identity store details can be configured using either the Identity Directory Configuration APIs or Mbeans. The Identity Directory API is used to initialize the Identity Directory Service. The Identity Directory Service provides an interface to both access and modify users and group information from different identity stores. See Using the Identity Directory API.

Another example is the ArisID API, which handles the hard work of data retrieval, transformation, and policy-enforcement when it comes to identity-based information. By using a Client Attribute Requirement Markup Language (CARML) file and declarations, applications will support flexible deployment in a wide range of environments without the need for ongoing specialized developer enhancements. See Using the ArisID API.

1.2 Understanding Identity Governance Framework APIs

The Identity Governance Framework depends on two specific API modules that enables the organizations to implement the data model requirements required to ensure security and compliance while exchange of identity information.

Oracle has made the following APIs available that are based on the Identity Governance Framework:

- **Identity Directory API**
  The Identity Directory API is a common service for identity management applications to access and manage identity information. The service can be used in both Java EE and Java SE modes. See Using the Identity Directory API.

- **ArisID API**
  The ArisID API provides enterprise developers and system architects a library for building identity-enabled applications using multiple identity protocols. The ArisID API enables developers to specify requirements for identity attributes, roles, and search filters by using Client Attribute Requirements Markup Language (CARML). See Using the ArisID API.
1.3 System Requirements and Certification for Identity Governance Framework

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information. Both of these documents are available on Oracle Technology Network (OTN).

For more information, see Oracle Fusion Middleware System Requirements and Specifications.

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, and third-party products. For more information, see Oracle Fusion Middleware Supported System Configurations.
Using the Identity Directory API

The Identity Directory API supports accessing and managing users, groups, organizations, and can be extended to support new entity types with relationships defined between these entities.

The following topics describe the architecture and key functionality of the Identity Governance Framework, Identity Directory API, and Identity Directory Service.

- Overview of the Identity Directory API
- Identity Directory API Configuration
- Design Recommendations for Identity Directory API
- Examples of Using the Identity Directory API

2.1 Overview of the Identity Directory API

The Identity Directory API provides a service for identity management applications to access and manage identity information. The API is flexible and can be fully configured by clients supporting heterogeneous identity stores having standard and specific schemas, and is robust with both high-availability and failover support.

The API uses the Identity Governance Framework and provides all the benefits of Identity Governance for identity information regulation and control. The API can be used in both Java EE and Java SE modes. For more information about the Identity Governance Framework, see Introduction to Identity Governance Framework.

The API supports the following actions:

- Create/Read/Update/Delete (CRUD) operations on User, Group, Org, and generic entities
- Get operation on User Account State
• Identity Directory API configuration sharing

• Support for directory servers such as Oracle Internet Directory, Oracle Unified Directory, Oracle Directory Server EE, and Active Directory.

Identity Directory Service consists of the following:

• **Identity Directory API**
  The Identity Directory API provide methods for accessing and managing identity information in a directory server that is the domain identity store. Entity definitions, entity relationships, and the physical identity store details can be configured using either the Identity Directory Configuration APIs or Mbeans. Directory service instance capabilities can be queried using getter methods.

• **Identity Directory API Configuration**
  Identity Directory API configuration comprises logical entity configuration and physical identity store configuration.

This section contains the following topics:

• **Understanding Identity Directory API**

• **Identity Directory Service Architecture**

• **Understanding Identity Directory API**
  The Identity Directory Service is a common service used by identity management products to access and manage an Identity Directory. The Identity Directory API is used to initialize the Identity Directory Service.

• **Identity Directory Service Architecture**
  To use the Identity Directory Service APIs, it is essential to understand the architecture to learn how the identities are integrated, and how they can be used.

### 2.1.1 Understanding Identity Directory API

The Identity Directory Service is a common service used by identity management products to access and manage an Identity Directory. The Identity Directory API is used to initialize the Identity Directory Service.

The Identity Directory Service provides an interface to both access and modify users and group information from different identity stores. An Identity Directory is an instance of the Identity Directory Service having:

• a unique name (IDS name)

• a logical entity configuration

• a physical identity store configuration

For more information about the Identity Directory Service, also referred to as the Identity Store Service, see Introduction to the Identity Store Service in Oracle® Fusion Middleware Securing Applications with Oracle Platform Security Services.

### 2.1.2 Identity Directory Service Architecture

To use the Identity Directory Service APIs, it is essential to understand the architecture to learn how the identities are integrated, and how they can be used.

**Figure 2-1** shows the logical architecture of the Identity Directory Service.
Figure 2-2 shows the relationship between the Identity Directory Service components.
2.2 Identity Directory API Configuration

The Identity Directory API provides an interface to access and modify users and group information from different identity stores. It is a combination of the logical entity configuration, the physical identity store configuration, and the operational configuration.

The logical entity configuration and operational configuration is stored in ids-config.xml. This file is located in the same directory as jps-config.xml. For example, in a Java EE environment the location is:

```
DOMAIN_HOME/config/fmwconfig/ids-config.xml
```

The physical identity store configuration is stored in ovd/ids/adapters.os.xml. For example, in a Java EE environment the ovd directory is located in:

```
DOMAIN_HOME/config/fmwconfig
```

This section contains the following topics:

- Logical Entity Configuration for an Identity Directory Service
- Physical Identity Store Configuration for an Identity Directory Service
- Operational Configuration for an Identity Directory Service
- Logical Entity Configuration for an Identity Directory Service

It is important to maintain and control the attributes and properties that are associated with a logical entity configuration for an Identity Directory.

- Physical Identity Store Configuration for an Identity Directory Service

It is imperative to identify and document the physical characteristics of a configuration item for an Identity Directory, so that it can used as needed.

- Operational Configuration for an Identity Directory Service

You must explore and identify the functional and operational aspects associated with a configuration item for an Identity Directory Service.
2.2.1 Logical Entity Configuration for an Identity Directory Service

It is important to maintain and control the attributes and properties that are associated with a logical entity configuration for an Identity Directory.

The following topics describe the logical entity configuration information for an Identity Directory Service:

- Properties of a Logical Entity Configuration
- Attributes of a Logical Entity Configuration
- Properties of a Logical Entity Definition
- Properties of a Logical Entity Relationship
- Properties of a Logical Entity Configuration

You must keep in mind the properties of a logical entity configuration.

2.2.1.1 Properties of a Logical Entity Configuration

You must keep in mind the properties of a logical entity configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name that uniquely identifies the Identity Directory Service.</td>
</tr>
<tr>
<td>ovd.context</td>
<td>Valid values are default or ids. Use default for connecting to the same identity store configured in OPSS. Use ids to connect to any physical identity store configured independent of OPSS. Only out-of-the-box identity directories, that is userrole and idxuserrole, use default value.</td>
</tr>
<tr>
<td>app.name</td>
<td>Optional property to specify the specific application for which the Identity Directory Service is being configured.</td>
</tr>
</tbody>
</table>

2.2.1.2 Attributes of a Logical Entity Configuration

The following table describes the logical entity attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Logical attribute name.</td>
</tr>
<tr>
<td>dataType</td>
<td>Valid data type values are as follows: string, boolean, integer, double, datetime, binary, x500name, and rfc822name.</td>
</tr>
<tr>
<td>description</td>
<td>Detailed description of the logical attribute.</td>
</tr>
<tr>
<td>readOnly</td>
<td>Default is false. Use true if the attribute is read-only.</td>
</tr>
</tbody>
</table>
Beginning with the 12c (12.1.3) release, the Identity Directory API supports entity attribute pass-through. With pass-through support, you do not need to include each and every attribute in attribute definitions (described in table in Attributes of a Logical Entity Configuration) and in attribute references under the entity definition (described in table in Properties of a Logical Entity Definition).

The IDS API allows any attribute in an add, modify, requested attributes, or search filter operation. The entity definition can hold a minimal set of attributes either to define entity relationships using logical attribute names that are different from the back-end identity store or for the default fetch of attributes.

If an input attribute is not in the identity store schema, the IDS API returns the error thrown by the identity store.

### 2.2.1.3 Properties of a Logical Entity Definition

You must keep in mind the properties required in each logical entity definition.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the entity.</td>
</tr>
<tr>
<td>type</td>
<td>Valid entity values are as follows: user, group, org and other.</td>
</tr>
<tr>
<td>idAttr</td>
<td>Logical attribute that uniquely identifies the entity.</td>
</tr>
<tr>
<td>create</td>
<td>Use true if creating this entity is allowed. Use false otherwise.</td>
</tr>
<tr>
<td>modify</td>
<td>Use true if modifying this entity is allowed. Use false otherwise.</td>
</tr>
<tr>
<td>delete</td>
<td>Use true if deleting this entity is allowed. Use false otherwise.</td>
</tr>
<tr>
<td>search</td>
<td>Use true if search of this entity to be allowed. Use false otherwise.</td>
</tr>
</tbody>
</table>

Attribute References

List of entity attribute references that contain the following details:

- **name**: Logical attribute name.
- **defaultFetch**: Default value is true. Use true if the attribute will be fetched by default. For example, when the entity is read using Identity Directory API, this attribute value is fetched from the identity store even though this attribute is not included in the requested attributes.
- **filter**: Search filter type with one of the following valid values: none, dynamic, equals, notequals, beginswith, contains, doesnotcontain, endswith, greaterequal, lessequal, greaterthan, and lessthan. **Value none** means no filter support.
2.2.1.4 Properties of a Logical Entity Relationship

You must keep in mind the properties required in each logical entity relationship definition.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the entity relationship.</td>
</tr>
<tr>
<td>type</td>
<td>Valid entity values are as follows: OneToOne, OneToMany, ManyToOne, and ManyToMany.</td>
</tr>
<tr>
<td>fromEntity</td>
<td>Name of the first entity in the Entity Relationship.</td>
</tr>
<tr>
<td>fromAttr</td>
<td>The first entity's attribute. Value of this attribute relates to the second entity in the relationship.</td>
</tr>
<tr>
<td>toEntity</td>
<td>Name of the second entity in the Entity Relationship.</td>
</tr>
<tr>
<td>toAttr</td>
<td>The second entity's attribute. Value of the fromAttr property maps to this attribute in second entity.</td>
</tr>
<tr>
<td>recursive</td>
<td>Use true if the entity relationship is recursive. Default is false.</td>
</tr>
</tbody>
</table>

2.2.2 Physical Identity Store Configuration for an Identity Directory Service

It is imperative to identify and document the physical characteristics of a configuration item for an Identity Directory, so that it can used as needed.

The following table describes the physical identity store configuration properties:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host and Port</td>
<td>Host and Port information of the Identity Store. Alternate Host and Port details also can be setup for failover.</td>
</tr>
<tr>
<td>Directory Type</td>
<td>Type of directory. Valid values are: OID, ACTIVE_DIRECTORY, IPLANET, EDIRECTORY, OPEN_LDAP, WLS_OVD, and OUD.</td>
</tr>
<tr>
<td>Bind DN and Password</td>
<td>Credentials to connect to the directory.</td>
</tr>
</tbody>
</table>

2.2.3 Operational Configuration for an Identity Directory Service

You must explore and identify the functional and operational aspects associated with a configuration item for an Identity Directory Service.

The operational configuration contains mainly base, name attribute, and objectclass configuration for each of the entities.

The following table describes the operational configuration entities:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>entity.searchbase</td>
<td>Container under which the entity should be searched.</td>
</tr>
<tr>
<td>entity.createbase</td>
<td>Container where the new entity will be created.</td>
</tr>
<tr>
<td>entity.name.attr</td>
<td>RDN attribute of the entity.</td>
</tr>
</tbody>
</table>
2.3 Design Recommendations for Identity Directory API

There are some essential design guidelines that one must keep in mind while creating an Identity Directory API.

The following topics describe these recommendations:

- Minimizing Use of defaultFetch Attributes
- Initializing the Identity Directory Once
- Minimizing Use of defaultFetch Attributes
- Initializing the Identity Directory Once

You must keep the number of entity attributes to minimal while configuring a new Identity Directory.

The entity attribute is defined by defaultFetch value. Also, try to have large attributes like jpegphoto configured with a defaultFetch value of false. The reason is every time the entity is read from the backend, all the defaultFetch attributes from backend directory will be retrieved. Too many defaultFetch attributes will affect the performance.

2.3.2 Initializing the Identity Directory Once

Initialization of Identity Directory has some overhead to initialize the entire ArisId stack. Therefore, you must initialize the Identity Directory once.

The Identity Directory API is used to initialize the Identity Directory Service. It has some overhead. As a result, applications should initialize the Identity Directory once, preferably on application startup, and use only one handle throughout.

2.4 Examples of Using the Identity Directory API

Use the sample codes for performing various operations associated with the Identity Directory API.

The following topics describe operations associated with the Identity Directory API:

- Initializing and Obtaining Identity Directory Handle
- Initializing and Obtaining Identity Directory Handle from JPS Context
• Initializing and Obtaining In-Memory Identity Directory Handle
• Adding a User
• Obtaining a User for Given Principal
• Modifying a User
• Obtaining a User for Given ID Value
• Searching Users Using Complex Search Filter
• Changing User Password
• Resetting User Password
• Authenticating a User
• Deleting a User
• Creating a Group
• Searching Groups
• Obtaining Management Chain
• Obtaining Reportees of a User
• Adding a Member to a Group
• Deleting a Member From a Group
• Obtaining All The Groups For Which User is a Member
• Using Logical NOT Operator in a Search Filter
• Initializing and Obtaining Identity Directory Handle
  You must first call an initialization function to use the functionality of Identity
  Directory Service. The Identity Directory handle then obtained is used to perform
  basic User and Group CRUD operations.
• Initializing and Obtaining Identity Directory Handle from JPS Context
  You can initialize and obtain the Identity Directory handle from JPS context. Use
  the sample code to perform the task.
• Initializing and Obtaining In-Memory Identity Directory Handle
  You can initialize and obtain the in-memory Identity Directory handle. Use the
  sample code perform this task.
• Adding a User
  After obtaining the Identity Directory handle, you can perform CRUD operations on
  users and groups. Use the sample code to add a user to the identity store.
• Obtaining a User for Given Principal
  You can retrieve users for a given principal. Use the sample code to perform the
  task.
• Modifying a User
  Once you have created the users, then you can modify the existing attributes of
  the user or can add attributes by modifying the user. Use the sample code to
  perform this task.
• Obtaining a User for Given ID Value
  You can retrieve the user details based on the identity value of the user. For this
  you need to create a retrieval query to fetch the details. Use the sample code to
  perform this task.
• **Searching Users Using Complex Search Filter**
  You might have to create complex filters in the user retrieval query, which match the given criteria and return the target search operation results. Use the sample code to perform this task.

• **Changing User Password**
  After you have created a user, you can modify the attributes of a user. Use the sample code to modify the password of a user.

• **Resetting User Password**
  You can reset the password of the created user in Identity Directory. Use the sample code to perform this task.

• **Authenticating a User**
  It is imperative to authenticate a user before granting the access to perform various operations. You can authenticate a user using APIs.

• **Deleting a User**
  You can delete a user that already exists in the identity store using the Identity Directory API. Use the sample code to perform this task.

• **Creating a Group**
  It is beneficial to create Groups as it is easier to grant or deny privileges to a groups of users instead of applying those privileges to each user individually. You can create user groups in Identity Directory.

• **Searching Groups**
  You can define search filters to search groups matching the desired criteria.

• **Obtaining Management Chain**
  You can obtain the management hierarchy for any given user in Identity Directory. Use the sample code to perform this task.

• **Obtaining Reportees of a User**
  You can obtain the reportees of a user by defining target search filters in Identity Directory.

• **Adding a Member to a Group**
  You can logically group an existing user in Identity Directory by adding them to a specific group. Use the sample code to perform this task.

• **Deleting a Member From a Group**
  A user who is a member of a group can be isolated from the given group using the Identity Directory API. Use the sample code to perform this task.

• **Obtaining All The Groups For Which User is a Member**
  For an existing user in Identity Directory, you can obtain all the groups to which the user belongs to using Identity Directory API. Use the sample code to perform this task.

• **Using Logical NOT Operator in a Search Filter**
  Identity Directory supports the use of NOT operator in a search filter. You can easily define a NOT operator in a search filter for obtaining results that match the criteria.

### 2.4.1 Initializing and Obtaining Identity Directory Handle

You must first call an initialization function to use the functionality of Identity Directory Service. The Identity Directory handle then obtained is used to perform basic User and Group CRUD operations.
import oracle.igf.ids.UserManager;
import oracle.igf.ids.GroupManager;
import oracle.igf.ids.config.OperationalConfig;
import oracle.igf.ids.IdentityDirectoryFactory;
import oracle.igf.ids.IdentityDirectory;
import oracle.igf.ids.IDSException;

public class IdsSample {
    private IdentityDirectory ids;
    private UserManager uMgr;
    private GroupManager gMgr;

    public IdsSample() throws IDSException {
        // Set Operational Config
        OperationalConfig opConfig = new OperationalConfig();

        // Set the application credentials (optional). This overrides
        // the credentials set in
        // physical ID store configuration
        opConfig.setApplicationUser("cn=user1,dc=us,dc=example,dc=com");
        opConfig.setApplicationPassword("password".toCharArray());

        // Set search/crate base, name, objclass, etc. config
        // (optional). This overrides default operational configuration
        // in IDS
        opConfig.setEntityProperty("User", opConfig.SEARCH_BASE,
                                  "dc=us,dc=example,dc=com");
        opConfig.setEntityProperty("User", opConfig.CREATE_BASE,
                                  "dc=us,dc=example,dc=com");
        opConfig.setEntityProperty("User", opConfig.FILTER_OBJCLASSES,
                                  "person");
        opConfig.setEntityProperty("User", opConfig.CREATE_OBJCLASSES,
                                  "inetorgperson");
        opConfig.setEntityProperty("Group", opConfig.SEARCH_BASE,
                                  "cn=groups,dc=us,dc=example,dc=com");
        opConfig.setEntityProperty("Group", opConfig.CREATE_BASE,
                                  "cn=groups,dc=us,dc=example,dc=com");
        opConfig.setEntityProperty("Group", opConfig.FILTER_OBJCLASSES,
                                  "groupofuniquenames");
        opConfig.setEntityProperty("Group", opConfig.CREATE_OBJCLASSES,
                                  "groupofuniquenames");

        // Get IdentityDirectory "ids1" configured in IDS config
        IdentityDirectoryFactory factory = new
        IdentityDirectoryFactory();
        ids = factory.getIdentityDirectory("ids1", opConfig);

        // Get UserManager and GroupManager handles
        uMgr = ids.getUserManager();
        gMgr = ids.getGroupManager();
    }
}
If you plan to use Tivoli as the authentication provider, then you need to select OPEN_LDAP as the authentication provider type. This is because Oracle WebLogic Server does not support Tivoli.

When Identity Governance Framework or Identity Directory Service is initialized to obtain the directory handle for Tivoli, then the generated adapters.os.xml file contains the following parameter:

```xml
<param name="mapAttribute" value="orclGUID=entryUUID"/>
```

In this scenario, for Tivoli, you need to map `orclGUID` attribute to `ibm-entryUUID` as follows:

```xml
<param name="mapAttribute" value="orclGUID=ibm-entryUUID"/>
```

You need to update the adapters.os.xml file manually to reflect these changes. In addition, you must restart the Oracle WebLogic Server for any attribute mapping update to work.

### 2.4.2 Initializing and Obtaining Identity Directory Handle from JPS Context

You can initialize and obtain the Identity Directory handle from JPS context. Use the sample code to perform the task.

```java
import oracle.igf.ids.UserManager;
import oracle.igf.ids.GroupManager;
import oracle.igf.ids.config.OperationalConfig;
import oracle.igf.ids.IdentityDirectoryFactory;
import oracle.igf.ids.IdentityDirectory;
import oracle.igf.ids.IDSException;
import oracle.security.jps.JpsContext;
import oracle.security.jps.JpsContextFactory;
import oracle.security.jps.service.idstore.IdentityStoreService;

public class IdsSample {
    private IdentityDirectory ids;
    private UserManager uMgr;
    private GroupManager gMgr;

    public IdsSample() throws IDSException {
        // Get IdentityDirectory from JpsContext
        try {
            JpsContext context = JpsContextFactory.getContextFactory().getContext();
            IdentityStoreService idstore = (IdentityStoreService)context.getServiceInstance(IdentityStoreService.class);
            ids = idstore.getIdentityStore();
        } catch (Exception e) {
            throw new IDSException(e);
        }
    }
}
```
2.4.3 Initializing and Obtaining In-Memory Identity Directory Handle

You can initialize and obtain the in-memory Identity Directory handle. Use the sample code to perform this task.

```java
import java.util.ArrayList;
import java.util.List;
import oracle.igf.ids.UserManager;
import oracle.igf.ids.GroupManager;
import oracle.igf.ids.config.AttributeDef;
import oracle.igf.ids.config.AttributeRef;
import oracle.igf.ids.config.EntityDef;
import oracle.igf.ids.config.EntitiesConfig;
import oracle.igf.ids.config.EntityRelationship;
import oracle.igf.ids.config.IdentityStoreConfig;
import oracle.igf.ids.config.OperationalConfig;
import oracle.igf.ids.IdentityDirectoryFactory;
import oracle.igf.ids.IdentityDirectory;
import oracle.igf.ids.IDSException;

public class IdsSample {
    private IdentityDirectory ids;
    private UserManager uMgr;
    private GroupManager gMgr;
    public IdsSample() throws IDSException {
        // Add Attribute definitions
        List<AttributeDef> attrDefs = new ArrayList<AttributeDef>();
        attrDefs.add(new AttributeDef("cn", AttributeDef.DataType.STRING));
        attrDefs.add(new AttributeDef("firstname", AttributeDef.DataType.STRING));
        attrDefs.add(new AttributeDef("sn", AttributeDef.DataType.STRING));
        attrDefs.add(new AttributeDef("telephonenumber", AttributeDef.DataType.STRING));
        attrDefs.add(new AttributeDef("uid", AttributeDef.DataType.STRING));
        attrDefs.add(new AttributeDef("uniquemember", AttributeDef.DataType.STRING));

        // Add User entity definition
        List<EntityDef> entityDefs = new ArrayList<EntityDef>();
        EntityDef userEntityDef = new EntityDef("User", EntityDef.EntityType.USER, "cn");
        userEntityDef.addAttribute(new AttributeRef("cn"));
        userEntityDef.addAttribute(new AttributeRef("firstname"));
        userEntityDef.addAttribute(new AttributeRef("sn"));
        userEntityDef.addAttribute(new AttributeRef("telephonenumber"));
        userEntityDef.addAttribute(new AttributeRef("uid"));
        entityDefs.add(userEntityDef);

        // Add Group entity definition
        EntityDef groupEntityDef = new EntityDef("Group", EntityDef.EntityType.GROUP, "cn");
    }
}
```
groupEntityDef.addAttribute(new AttributeRef("cn"));
groupEntityDef.addAttribute(new AttributeRef("uniquemember", false,
AttributeRef.FilterType.EQUALS));
etTypeDef.add(groupEntityDef);

// Add Entity relationship definition
List<EntityRelationship> entityRelations = new
ArrayList<EntityRelationship>();
entityRelations.add(new EntityRelationship("user_memberOfGroup",
EntityRelationship.RelationshipType.MANYTOMANY, "User",
"principal", "Group", "uniquemember"));
entityRelations.add(new EntityRelationship("group_memberOfGroup",
EntityRelationship.RelationshipType.MANYTOMANY, "Group",
"principal", "Group", "uniquemember", true));
EntitiesConfig entityCfg = new EntitiesConfig(attrDefs,
etTypeDefs, entityRelations);

// Create physical Identity Store configuration
"password").toCharArray(), IdentityStoreConfig.IdentityStoreType.OID);
idStoreCfg.setHighAvailabilityOption(IdentityStoreConfig.HAOption.FAILOVER);
idStoreCfg.setProperty(IdentityStoreConfig.HEARTBEAT_INTERVAL, "60");
idStoreCfg.setProperty(IdentityStoreConfig.MIN_POOLSIZE, "5");
idStoreCfg.setProperty(IdentityStoreConfig.MAX_POOLSIZE, "10");
idStoreCfg.setProperty(IdentityStoreConfig.MAX_POOLWAIT, "1000");

// Set operational config
OperationalConfig opConfig = new OperationalConfig();
opConfig.setEntityProperty(opConfig.USER_ENTITY, opConfig.SEARCH_BASE,
"cn=users,dc=us,dc=example,dc=com");
opConfig.setEntityProperty(opConfig.USER_ENTITY, opConfig.CREATE_BASE,
"cn=users,dc=us,dc=example,dc=com");
opConfig.setEntityProperty(opConfig.USER_ENTITY, opConfig.NAME_ATTR,
"cn");
opConfig.setEntityProperty(opConfig.USER_ENTITY, opConfig.FILTER
_OBJCLASSES, "inetorgperson");
opConfig.setEntityProperty(opConfig.USER_ENTITY, opConfig.CREATE
_OBJCLASSES, "inetorgperson");
opConfig.setEntityProperty(opConfig.GROUP_ENTITY, opConfig.SEARCH_BASE,
"cn=groups,dc=us,dc=example,dc=com");
opConfig.setEntityProperty(opConfig.GROUP_ENTITY, opConfig.CREATE_BASE,
"cn=groups,dc=us,dc=example,dc=com");
opConfig.setEntityProperty(opConfig.GROUP_ENTITY, opConfig.NAME_ATTR,
"cn");
opConfig.setEntityProperty(opConfig.GROUP_ENTITY, opConfig.FILTER
_OBJCLASSES, "groupofuniquenames");
opConfig.setEntityProperty(opConfig.GROUP_ENTITY, opConfig.CREATE
_OBJCLASSES, "groupofuniquenames");

// Initialize Identity Store Service
IdentityDirectoryFactory factory = new IdentityDirectoryFactory();
ids = factory.getIdentityDirectory("ids1", entityCfg, idStoreCfg,
2.4.4 Adding a User

After obtaining the Identity Directory handle, you can perform CRUD operations on users and groups. Use the sample code to add a user to the identity store.

```java
Principal principal = null;
List<Attribute> attrs = new ArrayList<Attribute>();
attrs.add(new Attribute("commonname", "test1_user1"));
attrs.add(new Attribute("password", "mypassword".toCharArray()));
attrs.add(new Attribute("firstname", "test1"));
attrs.add(new Attribute("lastname", "user1"));
attrs.add(new Attribute("mail", "test1.user1@example.com"));
attrs.add(new Attribute("telephone", "1 650 123 0001"));
attrs.add(new Attribute("title", "Senior Director"));
attrs.add(new Attribute("uid", "tuser1"));
try {
    CreateOptions createOpts = new CreateOptions();
    principal = uMgr.createUser(attrs, createOpts);
    System.out.println("Created user " + principal.getName());
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.5 Obtaining a User for Given Principal

You can retrieve users for a given principal. Use the sample code to perform the task.

```java
User user = null;
try {
    ReadOptions readOpts = new ReadOptions();
    user = uMgr.getUser(principal, readOpts);
    System.out.println("user " + user.getName());
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```
2.4.6 Modifying a User

Once you have created the users, then you can modify the existing attributes of the user or can add attributes by modifying the user. Use the sample code to perform this task.

```java
try {
    ModifyOptions modifyOpts = new ModifyOptions();
    List<ModAttribute> attrs = new ArrayList<ModAttribute>();
    attrs.add(new ModAttribute("description", "modified test user 1");
    user.modify(attrs, modifyOpts);
    System.out.println("Modified user " + user.getName());
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.7 Obtaining a User for Given ID Value

You can retrieve the user details based on the identity value of the user. For this you need to create a retrieval query to fetch the details. Use the sample code to perform this task.

```java
try {
    ReadOptions readOpts = new ReadOptions();
    User user = uMgr.searchUser("tuser1", readOpts);
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.8 Searching Users Using Complex Search Filter

You might have to create complex filters in the user retrieval query, which match the given criteria and return the target search operation results. Use the sample code to perform this task.

```java
try {
    // Complex search filter with nested AND and OR conditions
    SearchFilter filter = new SearchFilter(
        SearchFilter.LogicalOp.OR,
        new SearchFilter(SearchFilter.LogicalOp.AND,
            new SearchFilter("firstname", SearchFilter.Operator.BEGINS_WITH, "test"),
            new SearchFilter("telephone", SearchFilter.Operator.CONTAINS, "650")),
        new SearchFilter(SearchFilter.LogicalOp.AND,
            new SearchFilter("firstname", SearchFilter.Operator.BEGINS_WITH, "demo"),
            new SearchFilter("orgunit", SearchFilter.Operator.BEGINS_WITH, "demo"))
    );
    // Use the filter to search users
    List<User> users = uMgr.searchUsers(filter);
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```
new SearchFilter("orgunit", SearchFilter.Operator.BEGINS_WITH,
    "it"),
new SearchFilter("telephone", SearchFilter.Operator.CONTAINS,
    "650"));

    // Requesting attributes
    List<String> reqAttrs = new ArrayList<String>();
    reqAttrs.add("jpegphoto");

    SearchOptions searchOpts = new SearchOptions();
    searchOpts.setPageSize(100);
    searchOpts.setRequestedAttrs(reqAttrs);
    searchOpts.setSortAttrs(new String[]{"firstname");

    ResultSet<User> sr = uMgr.searchUsers(filter, searchOpts);
    while (sr.hasMore()) {
        User user = sr.getNext();
        System.out.println(user.getSubjectName());
    }
}

} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}

2.4.9 Changing User Password

After you have created a user, you can modify the attributes of a user. Use the sample
code to modify the password of a user.

ModifyOptions modOpts = new ModifyOptions();

try {
    user.changePassword("welcome123".toCharArray(),
        "welcome1".toCharArray(), modOpts);
    System.out.println("Changed user password");
} catch (Exception e) {
    System.out.println("Failed to change user password");
    e.printStackTrace();
}

2.4.10 Resetting User Password

You can reset the password of the created user in Identity Directory. Use the sample
code to perform this task.

ModifyOptions modOpts = new ModifyOptions();

try {
    user.resetPassword("welcome123".toCharArray(), modOpts);
    System.out.println("Reset user password");
} catch (Exception e) {
    System.out.println("Failed to reset user password");
    e.printStackTrace();
}
2.4.11 Authenticating a User

It is imperative to authenticate a user before granting the access to perform various operations. You can authenticate a user using APIs.

```java
ReadOptions readOpts = new ReadOptions();
try {
    User user = uMgr.authenticateUser("tuser1", "mypassword".toCharArray(), readOpts);
    System.out.println("authentication success");
} catch (Exception e) {
    System.out.println("Authentication failed. " + e.getMessage());
    e.printStackTrace();
}
```

2.4.12 Deleting a User

You can delete a user that already exists in the identity store using the Identity Directory API. Use the sample code to perform this task.

```java
try {
    DeleteOptions deleteOpts = new DeleteOptions();
    uMgr.deleteUser(principal, deleteOpts);
    System.out.println("Deleted user " + principal.getName());
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.13 Creating a Group

It is beneficial to create Groups as it is easier to grant or deny privileges to a groups of users instead of applying those privileges to each user individually. You can create user groups in Identity Directory.

```java
Principal principal = null;
List<Attribute> attrs = new ArrayList<Attribute>();
attrs.add(new Attribute("name", "test1_group1"));
attrs.add(new Attribute("description", "created test group 1"));
attrs.add(new Attribute("displayName", "test1 group1"));
try {
    CreateOptions createOpts = new CreateOptions();
    principal = gMgr.createGroup(attrs, createOpts);
    System.out.println("Created group " + principal.getName());
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```
2.4.14 Searching Groups

You can define search filters to search groups matching the desired criteria.

```java
public void searchGroups() {
    try {
        SearchFilter filter = new SearchFilter("name",
                SearchFilter.Operator.BEGINS_WITH, "test");

        SearchOptions searchOpts = new SearchOptions();
        searchOpts.setPageSize(10);

        ResultSet<Group> sr = gMgr.searchGroups(filter, searchOpts);
        while (sr.hasMore()) {
            Group group = sr.getNext();
            System.out.println(group.getSubjectName());
        }
    } catch (Exception e) {
        System.out.println(e.getMessage());
        e.printStackTrace();
    }
}
```

2.4.15 Obtaining Management Chain

You can obtain the management hierarchy for any given user in Identity Directory. Use the sample code to perform this task.

```java
try {
    ReadOptions readOpts = new ReadOptions();
    User user = uMgr.searchUser("tuser1", readOpts);

    SearchOptions searchOpts = new SearchOptions();
    searchOpts.setPageSize(10);
    int nLevels = 0;

    ResultSet<User> sr = user.getManagementChain(nLevels, searchOpts);
    while (sr.hasMore()) {
        User u = sr.getNext();
        System.out.println(u.getSubjectName());
    }
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.16 Obtaining Reportees of a User

You can obtain the reportees of a user by defining target search filters in Identity Directory.

```java
// Get Reportees with target search filter
public void getReportees() {
    try {
        ReadOptions readOpts = new ReadOptions();
        // Code here...
    }
```
User user = uMgr.searchUser("tuser1", readOpts);

SearchOptions searchOpts = new SearchOptions();
searchOpts.setPageSize(20);
int nLevels = 0;

// get all the direct/indirect reporting of tuser1 who are developers
SearchFilter filter = new SearchFilter("title",
SearchFilter.Operator.CONTAINS, "developer");
ResultSet<User> sr = user.getReportees(nLevels, filter, searchOpts);
while (sr.hasMore()) {
    User u = sr.getNext();
    System.out.println(u.getSubjectName());
}
}

2.4.17 Adding a Member to a Group

You can logically group an existing user in Identity Directory by adding them to a specific group. Use the sample code to perform this task.

try {
    ReadOptions readOpts = new ReadOptions();
    User user = uMgr.searchUser("tuser1", readOpts);
    Group group = gMgr.searchGroup("test1_group1", readOpts);
    ModifyOptions modOpts = new ModifyOptions();
    user.addMemberOf(group, modOpts);
    System.out.println("added tuser1 as a member of test1_group1");
}

2.4.18 Deleting a Member From a Group

A user who is a member of a group can be isolated from the given group using the Identity Directory API. Use the sample code to perform this task.

try {
    ReadOptions readOpts = new ReadOptions();
    User user = uMgr.searchUser("tuser1", readOpts);
    Group group = gMgr.searchGroup("test1_group1", readOpts);
    ModifyOptions modOpts = new ModifyOptions();
    group.deleteMember(user, modOpts);
    System.out.println("deleted tuser1 from the group test1_group1");
}

} catch (Exception e) {
    System.out.println(e.getMessage());
e.printStackTrace();
}
2.4.19 Obtaining All The Groups For Which User is a Member

For an existing user in Identity Directory, you can obtain all the groups to which the user belongs to using Identity Directory API. Use the sample code to perform this task.

```
try {
    ReadOptions readOpts = new ReadOptions();
    User user = uMgr.searchUser("tuser1", readOpts);

    SearchOptions searchOpts = new SearchOptions();
    searchOpts.setPageSize(10);
    int nLevels = 0;

    ResultSet<Group> sr = user.getMemberOfGroups(nLevels, null, searchOpts);
    while (sr.hasMore()) {
        Group group = sr.getNext();
        System.out.println(group.getSubjectName());
    }
} catch (Exception e) {
    System.out.println(e.getMessage());
    e.printStackTrace();
}
```

2.4.20 Using Logical NOT Operator in a Search Filter

Identity Directory supports the use of NOT operator in a search filter. You can easily define a NOT operator in a search filter for obtaining results that match the criteria.

```
try {
    SearchFilter f1 = new SearchFilter("firstname", SearchFilter.Operator.BEGINS_WITH, "demo");
    SearchFilter f2 = new SearchFilter("orgunit", SearchFilter.Operator.CONTAINS, "myorg");
    f2.negate();
    SearchFilter filter = new SearchFilter(SearchFilter.LogicalOp.AND, f1, f2);

    ResultSet<User> sr = uMgr.searchUsers(filter, searchOpts);
}
The ArisID API provides enterprise developers and system architects a library for building identity-enabled applications using multiple identity protocols. The ArisID API enables developers to specify requirements for identity attributes, roles, and search filters by using Client Attribute Requirements Markup Language (CARML).

**Note:**
This chapter and all its subsections have been deprecated in 12c (12.2.1.3.0) release. By deprecate, we mean that the feature is no longer being enhanced but is still supported for the full life of the 12c (12.2.1.3.0) release. Where indicated, a deprecated feature may be desupported in a future major release.

The following topics describe the architecture and key functionality of the Identity Governance Framework ArisID API:

- **About the ArisID API**
- **Configuring the ArisID API**
- **Design Recommendations for the ArisID API**
- **Generating ArisID Beans**
- **Examples of Using IDX User and Role Beans**
- **Understanding OpenLDAP Considerations**
- **About the ArisID API**
  The Identity Governance Framework ArisID API represents a common core service through which all identity information exchanged should be passed. While not an official name, the ArisID API is often referred to as Identity Beans by developers.
- **Configuring the ArisID API**
  ArisID API supports several configuration options which allow for easier and flexible deployment in Web Server environments.
- **Design Recommendations for the ArisID API**
  The default CARML and mapping files make certain assumptions about the deployment scenario. You may need to modify these details depending on your deployment requirements.
- **Generating ArisID Beans**
  When you have finished editing your CARML file, you can generate the ArisID Beans to use in your application. The ArisID Beans provide Java APIs as a layer on top of the ArisID API that have various action methods associated with them.
Examples of Using IDX User and Role Beans
It is imperative to understanding the use of IDX User and Role Beans. Use the sample applications to understand how to integrate IDX User/Role Beans into your application.

Understanding OpenLDAP Considerations
OpenLDAP specifies some mandatory attributes for implementing the APIs. You must keep in mind these attributes while implementing your applications.

3.1 About the ArisID API

The Identity Governance Framework ArisID API represents a common core service through which all identity information exchanged should be passed. While not an official name, the ArisID API is often referred to as Identity Beans by developers.

If you have installed Oracle WebLogic Server and Oracle Identity Management, all the necessary jar files for developing applications with this API are already installed on your computer.

The Identity Governance Framework open source API jar files are as follows:

- openliberty.arisld_1.1.jar — Provides the core ArisID API with library functions and providers that can be used to retrieve identity subjects that contain collections of attributes. See http://arisid.sourceforge.net/javadocs/arisId_1.1_javadoc/.
- org.openliberty.arisIdBeans_1.1.jar — Provides the ArisID beans, which provide Java object abstractions on top of the ArisID API. These convert the transactional approach of the ArisID API to an object or bean approach. See http://arisid.sourceforge.net/javadocs/arisId_1.1_javadoc/.

The ArisID API jar files are as follows:

- idxuserrole.jar — Provides the Standard User and Role identity read-only operations. This jar is generated from the standard idxuserrole.xml CARML file. See Java API Reference for Identity Governance Framework IDXUserRole.
- userrole.jar — Provides the User and Role identity read/write operations for updating identity information. See Java API Reference for Identity Governance Framework UserRole.
- arisId-stack-ovd.jar — This jar file is an implementation of the IAttrSvcStack interface with the Oracle Virtualization library to connect to different backends and provide an abstract view of the identity store entities.

The ArisID beans provide the Java APIs required for initialization and accessing CARML interactions. The bean generator generates a set of java files for each entity in the CARML file using Apache Velocity. The CARML file is a declarative document that describes the attribute usage requirements of your application. The ArisID beans are in the jar files idxuserrole.jar and userrole.jar.

The following figure provides a high-level view of the ArisID API architecture.
3.2 Configuring the ArisID API

ArisID API supports several configuration options which allow for easier and flexible deployment in Web Server environments.

The Identity Governance Framework ArisID supports the basic development process, which is Create > Modify > Test > Deploy. Creation requires CARML XML files and modifying them to suit your environment. Testing the application can be done in Oracle WebLogic Server embedded LDAP directory server.

This section contains the following topics:

- Examining CARML Files
- Configuring the Identity Repository
- Configuring the Mapping File
- Examining CARML Files
  CARML is an XML-based declarative format to define the attribute usage requirements of an application. Administrators examine the CARML file to connect to the appropriate back-end resources.
- Configuring the Identity Repository
  An identity repository is a data store where information about users and groups in a company is stored. You can configure the identity repository to be used by the ArisID beans.
• **Configuring the Mapping File**

The mapping file allows you to map CARML attributes to LDAP attributes, objectclasses, and search parameters. You can customize your mapping file for the LDAP-based directory server at your site.

### 3.2.1 Examining CARML Files

CARML is an XML-based declarative format to define the attribute usage requirements of an application. Administrators examine the CARML file to connect to the appropriate back-end resources.

To determine whether the existing ArisID beans meet your application's needs, you need to examine idxuserrole.xml (read-only operations) and userrole.xml (read-only and read/write operations) CARML files. These CARML files are located in DOMAIN_HOME/config/fmwconfig/carml.

### 3.2.2 Configuring the Identity Repository

An identity repository is a data store where information about users and groups in a company is stored. You can configure the identity repository to be used by the ArisID beans.

The identity repository to be used by the ArisID beans must be available. You can use the Oracle WebLogic Server embedded LDAP-based directory server or any LDAP directory supported by 11g Oracle Virtual Directory. The ArisID API is integrated with Oracle Platform Security Services. It automatically connects to the LDAP-based identity store configured in Oracle Platform Security Services. For more information about the identity stores supported by Oracle Platform Security Services, see System Requirements and Certification for Identity Governance Framework.

If you must use a different identity store from the Oracle Platform Security Services identity store, then set the following system property:

```java
igf.ovd.config.dir=DOMAIN_HOME/config/fmwconfig/arisidprovider/conf
```

Next, edit the adapters.os_xml file to include the host, port and credentials of the directory to be connected to. The `igf.ovd.config.dir` property can be set to any other directory containing adapters.os_xml and other configuration files with the right settings.

### Directory Limitations

The following LDAP directory limitations apply:

- When using OpenLDAP 2.2 or Novell eDirectory, there is no paging support. Paging APIs, for example, `searchUsersByPage()`, `searchRolesByPage()`, etc., do not work. There is no Multiple Language Support (MLS).
- When using Oracle WebLogic Server embedded LDAP-based directory server, there is no Multiple Language Support (MLS).
3.2.3 Configuring the Mapping File

The mapping file allows you to map CARML attributes to LDAP attributes, objectclasses, and search parameters. You can customize your mapping file for the LDAP-based directory server at your site.

When a CARML file is created a corresponding mapping file is created in the same location. The default mapping file has attribute details specific to Oracle WebLogic Server embedded directory server, which is the Oracle Platform Security Services default identity store. If you are using a default CARML file and the Oracle Platform Security Services identity store, you do not need to configure mapping. The configuration parameters in Oracle Platform Security Services override the parameters in the mapping file.

3.3 Design Recommendations for the ArisID API

The default CARML and mapping files make certain assumptions about the deployment scenario. You may need to modify these details depending on your deployment requirements.

The following topics describe the configuration parameters that can be modified:

- About Unique Identifier Configuration
- About Unique Key Attribute Specification
- About Multiple Language Support
- Handling Large Results
- Securing the Application
- Configuring the Timeout Interval
- Specifying Wildcard Characters in Search Filters
- About Unique Identifier Configuration
  It is imperative to ensure that all users are uniquely identifiable. The default configuration, email, is used as a unique identifier for identifying user entries.
- About Unique Key Attribute Specification
  Attribute uniqueness is enforced by defining constraints on attributes.
- About Multiple Language Support
  Multiple Language Support (MLS) is provided for applications that need locale-specific results.
- Handling Large Results
  There are situations when you retrieve large result sets. This could cause a performance and resource problem. Use the sample code to manage large result sets.
- Securing the Application
  There are two common security scenarios for executing create, read, update, and delete (CRUD) operations on the target system. You must review these scenarios for a better understanding.
- Configuring the Timeout Interval
  You can configure the timeout intervals for LDAP operations. These intervals specify the amount of time after which the LDAP operation times out.
3.3.1 About Unique Identifier Configuration

It is imperative to ensure that all users are uniquely identifiable. The default configuration, email, is used as a unique identifier for identifying user entries.

When you are searching for a user, the default attribute expected for search is `email`. For example:

```java
SearchUser(String uniqueid, Map<String, Object>)
```

For performance reasons, the attribute used as a unique identifier must be a searchable attribute in the backend. The mapping between the application’s choice of `uniquekey` and the backend attribute is handled at configuration time. This is a configuration in Oracle Virtual Directory mapping. The `HashMap` is used to provide the optional context information to be used while performing the operation. In the current release it supports the following options:

- The Principal user that performs the search - (`ArisIdConstants.APP_CTX_AUTHUSER`, `Principal`)
- The language constraint if any - (`ArisIdConstants.APP_CTX_LOCALE`, "fr")
- Pagination support if any - (`ArisIdConstants.APP_CTX_PAGESIZE`, 10)

3.3.2 About Unique Key Attribute Specification

Attribute uniqueness is enforced by defining constraints on attributes.

An application occasionally stores the entries accessed from the identity repository’s backend in their own application-specific repository. In such cases, you must carefully consider which attribute should be persisted. For instance, if the backend is an LDAP-based repository, you should use the `GUID` attribute as the persisting attribute because this is the only unique key on the LDAP-based backend. All other LDAP attributes are modifiable.

If the backend is a relational database, choose an attribute on which uniqueness constraint is enforced as the unique key. You can specify this in the ArisID mapping property file. The method to search for a user based on the unique key is:

```java
searchUserOnUniqueKey(String UniqueKey, Map<String, Object>)
```

The `HashMap` is used to provide the optional context information to be used while performing the operation. In the current release it supports the following options:

- The Principal user that performs the search - (`ArisIdConstants.APP_CTX_AUTHUSER`, `Principal`)
- The language constraint if any - (`ArisIdConstants.APP_CTX_LOCALE`, "fr")
- Pagination support if any - (`ArisIdConstants.APP_CTX_PAGESIZE`, 10)

3.3.3 About Multiple Language Support

Multiple Language Support (MLS) is provided for applications that need locale-specific results.
The attributes and the appropriate MLS code are stored in the ArisID properties file in the `multiLanguageAttributes` element.

```xml
<multiLanguageAttributes>...
</multiLanguageAttribute>
```

The `displayName` is the most commonly used multiple language attribute, therefore it is configured by default as a multi-language attribute. Other attributes can be added as needed in the ArisID mapping file.

**Restrictions**

Any API to which locale is specified as an argument will return the locale-specific values for all the attributes listed in the ArisID properties file as `<multiLanguageAttributes>` that have locale-specific values. For all other attributes it returns the default values stored.

In the backend system, the data is returned in a form conforming to ISO-3166. For example, if there is a French locale (in addition to English), it is stored as `cn,:fr` for the `cn` attribute. The locale for the client applications should be specified in the properties `HashMap` as `ArisIdConstants.APP_CTX_LOCALE, "fr"` and the ArisID properties file should contain `cn` as `multiLanguageAttribute` and map this attribute.

### 3.3.4 Handling Large Results

There are situations when you retrieve large result sets. This could cause a performance and resource problem. Use the sample code to manage large result sets.

When applications access identity data, the result set for a search is frequently too large to be handled by the application. In such cases you have the option of dividing the result into manageable sized pages. You do this by defining the number of objects to be returned in the page.

The following example shows a typical usage pattern:

```java
RoleManager rm = new RoleManager(env);
List<PropertyFilterValue> attrFilters = new ArrayList<PropertyFilterValue>();
attrFilters.add(new PropertyFilterValue(Role.NAME, "admin", AttributeFilter.OP_CONTAINS));

HashMap<String, Object> map = new HashMap<String, Object>();
map.put("ArisIdConstants.APP_CTX_PAGESIZE","2");
SearchResults<Role> sr = rm.searchRolesByPage(attrFilters, map);

while(sr.hasMore())
{
    List<Role> roles = sr.getNextSet();
    for (int i=0; i<roles.size(); i++)
        //do the operations with roles.get(i)
}
```

### 3.3.5 Securing the Application

There are two common security scenarios for executing create, read, update, and delete (CRUD) operations on the target system. You must review these scenarios for a better understanding.

They are as follows:
3.3.5 Applying Domain Level Credentials

In this scenario, all applications in a domain use common credentials to connect to the target system and perform operations with those credentials. The application does not maintain a footprint in the target system.

The LDAP Adapter's configuration file, `adapters.os.xml`, contains credentials to connect to the backend directory, along with the host and port details. If you do not provide any other credentials during initialization, the application connects to the target system using the credentials in the LDAP Adapter's configuration file.

If proxy user (logged in user id) is not specified in the API's application context, ArisID operation will be executed with the credentials that are in LDAP Adapter's configuration file.

If your application connects using common credentials, you must build security into the application itself so that it displays or modifies data only for an authorized user.

Consider the following example where the LDAP adapter's configuration file `adapters.os.xml` is configured with domain level userid and encrypted password to connect to backend directory. The following is a snippet of `adapters.os.xml`.

```xml
<binddn>cn=admin</binddn>
<bindpass>{OMASK}C2QXW1Nmf+s=</bindpass>
```

While initializing the ArisID API do not provide any credentials.

```java
Map env = new HashMap();
// Do not set UserManager.SECURITY_PRINCIPAL & SECURITY_CREDENTIALS
UserManager uMgr = new UserManager(env);

// Search Operation (with no proxy user in app context)
List<PropertyFilterValue> attrFilters = new ArrayList<PropertyFilterValue>();
attribFilters.add(new PropertyFilterValue("User.FIRSTNAME", "app1",
AttributeFilter.OP_CONTAINS));
attribFilters.add(new PropertyFilterValue("User.LASTNAME", "user1",
AttributeFilter.OP_BGNSWITH));
Map<String, Object> appCtx = null;
users = um.searchUsers(attrFilters, appCtx);
```

3.3.5.2 Applying Application Level Credentials

In this scenario, each application uses application level credentials to connect to the target system and performs CRUD operations with those credentials.

In this case you provide the application's user id and password while initializing the ArisID API. When you do that, the application connects to the target system using those credentials.
If no proxy user is specified in the API's application context then ArisID operation will be executed with the application's credentials.

This scenario has the following features:

- Each application has different privileges to view and update the data in the target system
- You can audit the modifications performed by each application in the target system

Consider the scenario where the LDAP adapter's configuration file adapters.os.xml is configured with domain level userid and encrypted password to connect to backend directory. The following is a snippet of adapters.os.xml.

```xml
<binddn>cn=admin</binddn>
<bindpass>{OMASK}C2QXW1Nmf+s=</bindpass>
```

While initializing the ArisID API, provide the application user credentials.

```java
Map env = new HashMap();
env.put(UserManager.SECURITY_PRINCIPAL, "cn=app1_user,cn=users,dc=example,dc=com");
env.put(UserManager.SECURITY_CREDENTIALS, "mypassword");
UserManager uMgr = new UserManager(env);

// Search Operation (with no proxy user in app context)
List<PropertyFilterValue> attrFilters = new ArrayList<PropertyFilterValue>();
attrFilters.add(new PropertyFilterValue("User.FIRSTNAME", "app1", AttributeFilter.OP_CONTAINS));
attrFilters.add(new PropertyFilterValue("User.LASTNAME", "user1", AttributeFilter.OP_BGNSWITH));
Map<String, Object> appCtx = null;
users = um.searchUsers(attrFilters, appCtx);
```

3.3.6 Configuring the Timeout Interval

You can configure the timeout intervals for LDAP operations. These intervals specify the amount of time after which the LDAP operation times out.

The default connect/read timeout is configured to be 15 seconds. For example, if the LDAP operation on IdentityStore is taking more than 15 seconds, the operation will timeout and throw the following IGF exception:

```
org.openliberty.arisid.stack.ConnectionException
```

If the IdentityStore has many entries and the applications are using filters with "contains" and search with paging/sorting, those queries may timeout.

The recommendation is to set the timeout value to 0 (no timeout) and increase the pool size to 20. If the application has a timeout interval, set the value to greater than 0.

To configure the timeout interval:

1. Run the following WLST command to list all adapters.
   ```
   listAdapters()
   ```
2. Run the following command for each adapter to set timeout and maxpoolsize.
   ```
   a. modifyLDAPAdapter('"<ADAPTER NAME>"', 'OperationTimeout', 0)
   b. modifyLDAPAdapter('"<ADAPTER NAME>"', 'MaxPoolSize', 20)
   ```
3.3.7 Specifying Wildcard Characters in Search Filters

Oracle Internet Directory supports wildcard search for DN attributes.

Directories other than Oracle directories might not support wildcard search. Therefore, if you perform a search operation through Identity Governance Framework API with say Microsoft Active Directory as the backend and using a DN in a search filter, then you must provide the `AttributeFilter.OP_EQUALS` operator to successfully execute the operation.

3.4 Generating ArisID Beans

When you have finished editing your CARML file, you can generate the ArisID Beans to use in your application. The ArisID Beans provide Java APIs as a layer on top of the ArisID API that have various action methods associated with them.

To generate the ArisID Beans run the following command:

```bash
java BeanGenerator [-genmap] <package name> <output dir> [<relationship file>] <carml file>
```

where:

- `-genmap`: Generates the CARML-ArisIDStack map file in the same location where the CARML file is.
- `package name`: Is the package name for the generated bean classes.
- `output dir`: Location to write the generated bean classes.
- `relationship file`: File containing the relationship definitions between entities.
- `carml file`: The CARML declaration file.

To build ORG beans from a CARML file:

1. Create a CARML file name org.xml with the appropriate attributes/interactions for ORG entity.
2. Generate org beans (OrgManager.java and Org.java) using the Bean Generator. The build.xml file should resemble the following sample:

```xml
<path id="ArisIDBeans.classpath">
    <pathelement location="MW_HOME/oracle_common/modules/velocity-dep-1.4.jar" />
    <pathelement location="MW_HOME/oracle_common/modules/oracle.jrf_11.1.1/jrf.jar" />
</path>
<property name="BeanGeneratorClassPath" refid="ArisIDBeans.classpath"/>
<target name="generatebeans" description="generate arisid beans">
    <java classname="org.openliberty.arisidbeans.BeanGenerator" dir="${generatedsource.dir}" fork="true">
        <arg value="${generatedbean.userrole.packagename}"/>
        <arg value="."/>
        <arg value="${carml.dir}/org.xml"/>
        <classpath>
            <pathelement path="${BeanGeneratorClassPath}"/>
        </classpath>
        <sysproperty key="org.openliberty.arisid.policy.wspolicy.class">
```

3-10
3. Compile the generated java files Org.java and OrgManager.java.

4. Edit the generated mapping file (igf-map-config-.xml) to update basesearch, objectclass, OVD attribute names with their values.

5. An application can use the generated ORG APIs for the interactions defined in the CARML file (org.xml). After the application is deployed in application server:
   a. Copy the mapping file under DOMAIN_HOME/config/fmwconfig/arisdprovider/conf, and
   b. Copy the CARML file under DOMAIN_HOME/config/fmwconfig/carml

3.5 Examples of Using IDX User and Role Beans

It is imperative to understanding the use of IDX User and Role Beans. Use the sample applications to understand how to integrate IDX User/Role Beans into your application.

The following topics describe the use of IDX User/Role Beans:

- Searching Users Using IDX User and Role Beans: SearchUsers.jsp
- Searching Users Using IDX User and Role Beans: SearchUsers.html
- Searching Users Using IDX User and Role Beans: SearchUsers.jsp
  Use IDX User/Role Beans Java version to search users.
- Searching Users Using IDX User and Role Beans: SearchUsers.html
  Use the IDX User/Role Beans code to search users.

3.5.1 Searching Users Using IDX User and Role Beans: SearchUsers.jsp

Use IDX User/Role Beans Java version to search users.

```java
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<%@page import="org.openliberty.arisid.*"%>
<%@page import="org.openliberty.arisidbeans.*"%>
<%@page import="oracle.igf.userrole.*"%>
<%@page import="java.util.*"%>
<%@page import="java.net.URI"%>
<%!public static UserManager uMgr = null;
    try {
        uMgr = new UserManager(null);
    } catch (Exception e) {
        e.printStackTrace();
    }
%
<html>
<head>
```
String firstname = request.getParameter("firstname");
String lastname = request.getParameter("lastname");
String telephone = request.getParameter("telephone");

List<PropertyFilterValue> attrFilters = new ArrayList<PropertyFilterValue>();
attrFilters.add(new PropertyFilterValue("firstname", firstname,
AttributeFilter.OP_BGNSWITH));
attrFilters.add(new PropertyFilterValue("lastname", lastname,
AttributeFilter.OP_BGNSWITH));
attrFilters.add(new PropertyFilterValue("telephone", telephone,
AttributeFilter.OP_CONTAINS));

List<User> subjs = uMgr.searchUsers(attrFilters);

Iterator<User> sIter = subjs.iterator();
while (sIter.hasNext()) {
    User subj = sIter.next();
    Map<String, IAttributeValue> vals = subj.getAllAttributes();
    Iterator<IAttributeValue> iter = vals.values().iterator();
    while (iter.hasNext()) {
        IAttributeValue val = iter.next();
        String name = val.getNameIdRef();
        String value = null;
        if (val.size() > 0)
            value = val.get(0);
        if (value != null)
            <tr>
                <td><%=name%></td>
                <td><%=value%></td>
            </tr>
    }
}
3.5.2 Searching Users Using IDX User and Role Beans: SearchUsers.html

Use the IDX User/Role Beans code to search users.

First Name Starting with <INPUT TYPE=TEXT NAME=firstname SIZE=30><BR><BR>
Last Name Starting with <INPUT TYPE=TEXT NAME=lastname SIZE=30><BR><BR>
Telephone Number containing <INPUT TYPE=TEXT NAME=telephone SIZE=15><BR><BR>

3.6 Understanding OpenLDAP Considerations

OpenLDAP specifies some mandatory attributes for implementing the APIs. You must keep in mind these attributes while implementing your applications.

For OpenLDAP, Role.MEMBER is a mandatory attribute for the following APIs:

- createRole(List<PropertyValue> attrVals, Map<String,Object> appCtxMap)
- createRole(List<PropertyValue> attrVals)

If the Role.MEMBER is not included in the input attrVals list, role creation will fail.
Migrating to Identity Directory API

Use the topics to understand how to migrate applications from the User and Role API to the Identity Directory API.

• **Overview of Migrating to Identity Directory API**
  The Identity Directory API allows applications to access identity information (users and other entities) in a uniform and portable manner. If you have an application that uses the User and Role API, then you can migrate it to use Identity Directory API.

• **Migrating the Application to Identity Directory API**
  You need to implement some code changes while migrating an application from the User and Role API to the Identity Directory API.

• **Understanding the Comparison Between User and Role API With IDS API**
  It is essential that you understand the mapping between the User and Role API and Identity Directory API before implementing the change in your application.

• **Moving From a Test to a Production Environment**
  Moving from one environment to another, especially from a test environment to production environment, provides you the flexibility to test applications in a test environment and then roll them out in the production environment.

• **Tuning Configuration Parameters for IDS**
  Tuning is the adjustment or modification of parameters to meet specific deployment requirements. The default IDS configuration must be tuned for your deployment scenario.

• **Allowing Pass-through Attributes in IDS**
  In IDS while executing the Search or Update operation, you need to define every attribute that is used by IDS APIs in the entity definition. However, Identity Directory allows you to dynamically add attributes on runtime. These are referred to as the pass-through attributes.

### 4.1 Overview of Migrating to Identity Directory API

The Identity Directory API allows applications to access identity information (users and other entities) in a uniform and portable manner. If you have an application that uses the User and Role API, then you can migrate it to use Identity Directory API.

The Identity Directory API also picks up the LDAP-based identity store confirmation from the jps-config file. As such, when migrating an application from the User and Role API to the Identity Directory API, you need to ensure that the LDAP connection and configuration are set up correctly.
API to the Identity Directory API you do not need to change the configuration in the jps-config file.

Applications that initialize the User and Role API with a programmatic configuration can use a similar method to initialize the Identity Directory API, as described in Initializing and Obtaining In-Memory Identity Directory Handle.

4.2 Migrating the Application to Identity Directory API

You need to implement some code changes while migrating an application from the User and Role API to the Identity Directory API.

The following topics describe the code changes needed while migration:

- Initializing API
- Getting UserManager and GroupManager Handle
- Searching Filter
- Performing CRUD Operations

4.2.1 Initializing API

All applications must initialize the API to obtain the Identity Directory handle. The program should perform the initialization only once. Use the sample code to initialize an API.

The process of initializing is similar to using IdentityStoreService.GetIdmStore() for getting oracle.security.idm.IdentityStore handle. Identity Directory Service uses IdentityStoreService.getIdentityStore() to get IdentityDirectory handle. For example:

```java
import oracle.igf.ids.IdentityDirectory;
import oracle.igf.ids.IDSException;
import oracle.security.jps.JpsContext;
import oracle.security.jps.service.idstore.IdentityStoreService;

// Get IdentityDirectory from JpsContext
JpsContext context = JpsContextFactory.getContextFactory().getContext();
```
IdentityStoreService idstore = (IdentityStoreService) context.getServiceInstance(IdentityStoreService.class);
Identity Directory ids = idstore.getIdentityStore();

4.2.2 Getting UserManager and GroupManager Handle

All operations on a user instance are handled by a user manager and all operations on a group are handled by a group manager. Use the sample code to perform CRUD operations on users and groups instance respectively.

User related CRUD operations can be performed with oracle.igf.ids.UserManager and Role related CRUD operations can be performed with oracle.igf.ids.GroupManager. UserManager and GroupManager handles can be obtained from IdentityDirectory object. For example:

import oracle.igf.ids.UserManager;
import oracle.igf.ids.GroupManager;

// Get UserManager and GroupManager handles
UserManager uMgr = ids.getUserManager();
GroupManager gMgr = ids.getGroupManager();

4.2.3 Searching Filter

You can create simple or complex search filter to be used in searching the identity repository. Use the sample code to facilitate a variety of search operations.

You can build a simple or complex search filter using oracle.igf.ids.SearchFilter. For example:

import oracle.igf.ids.SearchFilter;

// Simple search filter for (firstname equals "john")
SearchFilter filter1 = new SearchFilter("firstname",
SearchFilter.Operator.EQUALS, "john");

// Complex search filter for
// ((title contains "manager") and (org equals "amer")) or
// ((title contains "senior manager") and (org equals "apac"))
SearchFilter filter = new SearchFilter(
SearchFilter.LogicalOp.OR,
new SearchFilter(SearchFilter.LogicalOp.AND,
new SearchFilter("manager", SearchFilter.Operator.CONTAINS,
"manager"),
new SearchFilter("org", SearchFilter.Operator.EQUALS, "amer")),
new SearchFilter(SearchFilter.LogicalOp.AND,
new SearchFilter("manager", SearchFilter.Operator.CONTAINS,
"senior manager"),
new SearchFilter("org", SearchFilter.Operator.EQUALS, "apac"));

4.2.4 Performing CRUD Operations

You can perform Create/Read/Update/Delete (CRUD) operations on User, Group, Org, and generic entities. This requires that the CRUD APIs be implemented for use in the applications.
The following topics describes these CRUD operations:

- APIs to Find a User
- APIs to Search a User
- APIs to Create a User
- APIs to Delete a User
- APIs to Authenticate a User
- APIs to Modify Users and Manage Related Entities
- APIs to Find a User
- APIs to Search a User
- APIs to Create a User
- APIs to Delete a User
- APIs to Authenticate a User

You can create a user using an API.

- APIs to Authenticate a User
  It is a common mechanism to authenticate users via an API.

- APIs to Modify Users and Manage Related Entities

### 4.2.4.1 APIs to Find a User

The following APIs are used for finding a user:

- Get user for given principal identifier. For example:
  ```java
  User getUser(Principal principal, ReadOptions opts)
  ```

- Search for user matching given id attribute value that uniquely identifies the user. For example:
  ```java
  User searchUser(String id, ReadOptions opts)
  ```

- Finds user matching given attribute name and value. For example:
  ```java
  User searchUser(String attrName, String attrVal, ReadOptions opts)
  ```

- Search for user matching given GUID value that uniquely identifies the user. For example:
  ```java
  searchUserByGuid(String guid, ReadOptions opts)
  ```

### 4.2.4.2 APIs to Search a User

The following is an example of the API for searching a user.

```java
ResultSet<User> searchUsers(SearchFilter filter, SearchOptions opts)
```

### 4.2.4.3 APIs to Create a User

You can create a user using an API.

The following is an example of the API for creating a user.

```java
Principal createUser(List<Attribute> attrVals, CreateOptions opts)
```
4.2.4.4 APIs to Delete a User

You can delete a user using an API.

The following are examples of the API for deleting a user.

- **Delete the user given the principal identifier.**
  
  void deleteUser(Principal principal, DeleteOptions opts)

- **Delete the user given the id attribute value.**
  
  void deleteUser(String id, DeleteOptions opts)

4.2.4.5 APIs to Authenticate a User

It is a common mechanism to authenticate users via an API.

The following are examples of the API for user authentication.

- **Authenticate the user matching the given id attribute value.**
  
  User authenticateUser(String id, char[] password, ReadOptions opts)

- **Authenticate the user for given principal identifier.**
  
  boolean authenticateUser(Principal principal, char[] password)

4.2.4.6 APIs to Modify Users and Manage Related Entities

The APIs for modifying user attributes and for getting the related entities are in User object instead of UserManager.

Modifying a User

The following are examples of the API for modifying a user.

- **Modify user attributes.**
  
  void User.modify(List<ModAttribute> attrVals, ModifyOptions opts)

- **Set the user attribute value.**
  
  void User.setAttributeValue(String attrName, String attrVal, ModifyOptions opts)

Managing Related Entities

The following are examples of the APIs for managing entities.

- **Get the management chain.**
  
  ResultSet<User> getManagementChain(int nLevels, SearchOptions opts)

- **Check if the given user is manager of this user.**
  
  boolean isManager(User user, boolean direct, ReadOptions opts)

- **Set the given user as manager of this user.**
  
  void setManager(User user, ModifyOptions opts)
• Get all the reportees of this user.
  ResultSet<User> getReportees(int nLevels,
  SearchFilter targetFilter, SearchOptions opts)

• Get all the groups this user is a member of and matching the given filter criteria.
  ResultSet<Group> getMemberOfGroups(int nLevels, SearchFilter targetFilter, SearchOptions opts)

• Check if this user is a member of the given group.
  boolean isMemberOf(Group group, boolean direct, ReadOptions opts)

• Add this user as a member to given group.
  void addMemberOf(Group group, ModifyOptions opts)

• Delete this user as a member to given group.
  void deleteMemberOf(Group group, ModifyOptions opts)

4.3 Understanding the Comparison Between User and Role API With IDS API

It is essential that you understand the mapping between the User and Role API and Identity Directory API before implementing the change in your application.

The following topics describe the differences:

• Comparison of User-Related APIs With Identity Directory APIs
• Comparison of Role-Related APIs With Identity Directory APIs
• Comparison of User-Related APIs With Identity Directory APIs
  You must understand the mapping between the endpoints for the User API with those in the Identity Directory API.
• Comparison of Role-Related APIs With Identity Directory APIs
  You must understand the mapping between the endpoints for the User/Role API with those in the Identity Directory API.

4.3.1 Comparison of User-Related APIs With Identity Directory APIs

You must understand the mapping between the endpoints for the User API with those in the Identity Directory API.

The following table maps the User-related API method with its corresponding Identity Directory API method.
<table>
<thead>
<tr>
<th>Functionality</th>
<th>User/Role API Method</th>
<th>Identity Directory Service Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Creation</td>
<td>User Manager.createUser(String name, char[] password)</td>
<td>Principal UserManager.createUser(List&lt;Attribute&gt; attrVals, CreateOptions opts)</td>
</tr>
<tr>
<td></td>
<td>User Manager.createUser(String name, char[] password, PropertySet pset)</td>
<td></td>
</tr>
<tr>
<td>Delete User</td>
<td>void UserManager.dropUser(UserProfile user)</td>
<td>void UserManager.deleteUser(Principal principal, DeleteOptions opts)</td>
</tr>
<tr>
<td></td>
<td>void UserManager.dropUser(User user);</td>
<td>void UserManager.deleteUser(String id, DeleteOptions opts)</td>
</tr>
<tr>
<td>Authenticate User</td>
<td>User Manager.authenticateUser(String user_id, char[] passwd)</td>
<td>User Manager.authenticateUser(String id, char[] password, ReadOptions opts)</td>
</tr>
<tr>
<td></td>
<td>User Manager.authenticateUser(User user, char[] passwd)</td>
<td>boolean UserManager.authenticateUser(Principal principal, char[] passwd)</td>
</tr>
<tr>
<td></td>
<td>User Manager.authenticateUser(String user_id, String authProperty, char[] passwd)</td>
<td></td>
</tr>
<tr>
<td>Check if create User is supported</td>
<td>boolean UserManager.isCreateUserSupported()</td>
<td>boolean UserManager.getCapabilities().isCreateCapable()</td>
</tr>
<tr>
<td>Check if modify User is supported</td>
<td>boolean UserManager.isModifyUserSupported()</td>
<td>boolean UserManager.getCapabilities().isUpdateCapable()</td>
</tr>
<tr>
<td>Check if drop User is supported</td>
<td>boolean UserManager.isDropUserSupported()</td>
<td>boolean UserManager.getCapabilities().isDeleteCapable()</td>
</tr>
<tr>
<td>Search Users by given search criteria</td>
<td>IdentityStore.searchUsers(SearchParameters params)</td>
<td>ResultSet&lt;User&gt; UserManager.searchUsers(SearchFilter filter, SearchOptions opts)</td>
</tr>
<tr>
<td>Search an User by name/uniqueName / guid</td>
<td>User IdentityStore.searchUser(String name)</td>
<td>User UserManager.searchUser(String id, ReadOptions opts)</td>
</tr>
<tr>
<td></td>
<td>User IdentityStore.searchUser(String attrName, String attrVal, ReadOptions opts)</td>
<td></td>
</tr>
<tr>
<td>Check if User exists in the repository for a given User object</td>
<td>boolean IdentityStore.exists(User user)</td>
<td>User getUser(Principal principal, ReadOptions opts)</td>
</tr>
<tr>
<td>Functionality</td>
<td>User/Role API Method</td>
<td>Identity Directory Service Method</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Simple search filter (search based on a single attribute name, type and value)</td>
<td>SimpleSearchFilter</td>
<td>SearchFilter(String propertyName, Operator op, String propertyVal)</td>
</tr>
<tr>
<td>Complex search filter (search based on more than one attribute with filter conditions and nested filters)</td>
<td>ComplextSearchFilter</td>
<td>SearchFilter(LogicalOp op, SearchFilter... searchFilters)</td>
</tr>
<tr>
<td>Getting a property value for a given property name</td>
<td>User.getPropertyVal(String propName) (User Role API fetches the attribute values from cache. If it misses cache, it fetches from repository)</td>
<td>String User.getAttributeValue(String attrName) Limitation: Returns attribute values from User object that has been already fetched from the repository.</td>
</tr>
<tr>
<td>Getting the User property for a given property name</td>
<td>User.getProperty(String propName)</td>
<td>Attribute User.getAttribute(String attrName)</td>
</tr>
</tbody>
</table>
| Getting the user properties for a given set of property names | User.getProperties() | Map<String, Attribute>
| Get all user properties from the repository for a user | User.getAllUserProperties() | Map<String, Attribute>
| Get all user property names from the schema | IdentityStore.getUserPropertyNames() Returns the names of all the properties in the schema | List<String>
| Changing the attribute value in the repository of an user | User.setProperty(ModProperty mprop) | void User.setAttributeValue(String attrName, String attrVal, ModifyOptions opts) |
| Changing the set of attribute values in the repository for an user | User.setProperties(ModProperty[] modPropObjs) | void User.modify(List<ModAttribute> attrVals, ModifyOptions opts) |
| Get all the reportees of an User either direct or indirect | User.getReportees(boolean direct) | ResultSet<User> User.getReportees(int nLevels, SearchFilter targetFilter, SearchOptions opts) |
| Get Management chain of an user | User.getManagementChain(int max, String upToManagerName, String upToTitle) | ResultSet<User> User.getManagementChain(int nLevels, SearchOptions opts)
| List<User> User.getManagementChain(int nLevels, String manager, String title, SearchOptions opts) |
### Functionality

<table>
<thead>
<tr>
<th>User/Role API Method</th>
<th>Identity Directory Service Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Get/Set of Binary Attributes</strong></td>
<td>Returns base64 encoded value</td>
</tr>
<tr>
<td>Property in User/Role API supports binary attributes</td>
<td>While setting the value either base64 encoded value or byte[] can be used for creating ModAttribute.</td>
</tr>
<tr>
<td><code>byte[] user.getJPEGPhoto()</code></td>
<td></td>
</tr>
<tr>
<td><code>void user.setJPEGPhoto(String imgPath)</code></td>
<td></td>
</tr>
<tr>
<td><strong>Selecting the Realm</strong></td>
<td>This is part of IDS Operational configuration. At API level searchbase and createbase can be specified as well.</td>
</tr>
<tr>
<td>Available</td>
<td></td>
</tr>
<tr>
<td><code>env.put(OIDIdentityStoreFactory.RT_SUBSCRIBER_NAME, &quot;&lt;realm dn&gt;&quot;);</code></td>
<td></td>
</tr>
<tr>
<td><code>IdentityStoreFactory.getEntityStoreInstance(env);</code></td>
<td></td>
</tr>
</tbody>
</table>

### 4.3.2 Comparison of Role-Related APIs With Identity Directory APIs

You must understand the mapping between the endpoints for the User/Role API with those in the Identity Directory API.

The following table maps the Role-related API method with its corresponding Identity Directory API method.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>User/Role API Method</th>
<th>Identity Directory Service Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Creating a Role</strong></td>
<td>Role</td>
<td>Principal</td>
</tr>
<tr>
<td><code>RoleManager.createRole(String name, int scope)</code></td>
<td>GroupManager.createGroup(List&lt;Attribute&gt; attrVals, CreateOptions opts)</td>
<td></td>
</tr>
<tr>
<td><code>RoleManager.createRole(String name)</code></td>
<td>GroupManager.getCapabilities().isCreateCapable()</td>
<td></td>
</tr>
<tr>
<td><strong>Deleting a Role</strong></td>
<td>void</td>
<td>void</td>
</tr>
<tr>
<td><code>RoleManager.dropRole(RoleProfile role)</code></td>
<td>GroupManager.deleteGroup(Principal principal, DeleteOptions opts)</td>
<td></td>
</tr>
<tr>
<td><code>RoleManager.dropRole(Role role)</code></td>
<td>GroupManager.getCapabilities().isDeleteCapable()</td>
<td></td>
</tr>
<tr>
<td><strong>Check if create role is supported</strong></td>
<td>boolean</td>
<td>boolean</td>
</tr>
<tr>
<td><code>RoleManager.isCreateRoleSupported()</code></td>
<td>GroupManager.getCapabilities().isCreateSupported()</td>
<td></td>
</tr>
<tr>
<td><strong>Check if modify role is supported</strong></td>
<td>boolean</td>
<td>boolean</td>
</tr>
<tr>
<td><code>RoleManager.isModifyRoleSupported()</code></td>
<td>GroupManager.getCapabilities().isUpdateSupported()</td>
<td></td>
</tr>
<tr>
<td><strong>Check if delete role is supported</strong></td>
<td>boolean</td>
<td>boolean</td>
</tr>
<tr>
<td><code>RoleManager.isDropRoleSupported()</code></td>
<td>GroupManager.getCapabilities().isDeleteSupported()</td>
<td></td>
</tr>
<tr>
<td><strong>Is the Group owned by a User</strong></td>
<td>boolean</td>
<td>boolean</td>
</tr>
<tr>
<td><code>RoleManager.isGranted(Role parent, Principal principal)</code></td>
<td>Group.isMember(User user, boolean direct, ReadOptions opts)</td>
<td></td>
</tr>
<tr>
<td><code>User.isMemberOf(Realm group, boolean direct, ReadOptions opts)</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td>User/Role API Method</td>
<td>Identity Directory Service Method</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is the Group owned by a User</td>
<td>boolean RoleManager.isOwnedBy(Role parent, Principal principal)</td>
<td>boolean User.isOwnerOf(Group group, boolean direct, ReadOptions opts)</td>
</tr>
<tr>
<td>Is the group managed by a User</td>
<td>boolean RoleManager.isManagedBy(Role parent, Principal principal)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Get all the members of a Role either direct / indirect</td>
<td>SearchResponse Role.getGrantees(SearchFilter filter, boolean direct)</td>
<td>ResultSet&lt;User&gt; Group.getMembers(int nLevels, SearchFilter targetFilter, SearchOptions opts)</td>
</tr>
<tr>
<td>Add an user as a member to a role</td>
<td>void RoleManager.grantRole(Role parent, Principal principal)</td>
<td>void Group.addMember(User user, ModifyOptions opts)</td>
</tr>
<tr>
<td>Remove a user from being member of a role</td>
<td>void RoleManager.revokeRole(Role parent, Principal principal)</td>
<td>void Group.deleteMember(User user, ModifyOptions opts)</td>
</tr>
<tr>
<td>Get all the owners of a specific Role either direct / indirect</td>
<td>SearchResponse Role.getOwners(SearchFilter filter, boolean direct)</td>
<td>ResultSet&lt;User&gt; Group.getOwners(int nLevels, SearchFilter targetFilter, SearchOptions opts)</td>
</tr>
<tr>
<td>Add a user as an owner of a role</td>
<td>void Role.addOwner(Principal principal)</td>
<td>void Group.addOwner(User user, ModifyOptions opts)</td>
</tr>
<tr>
<td>Remove a user from being a owner of a Role</td>
<td>void Role.removeOwner(Principal principal)</td>
<td>void Group.deleteOwner(User user, ModifyOptions opts)</td>
</tr>
<tr>
<td>Get all the managers of a Role either direct / indirect</td>
<td>SearchResponse Role.getManagers(SearchFilter filter, boolean direct)</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Add a user as a manager of a Role</td>
<td>void Role.addManager(Principal principal)</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Remove a user from being a manager of a Role</td>
<td>void Role.removeManager(Principal principal)</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Getting the role property</td>
<td>Property Role.getProperty(String propName)</td>
<td>Attribute Group.getAttribute(String attrName)</td>
</tr>
</tbody>
</table>

Note: User Role API fetches these attribute values from cache. If it misses cache, it fetches from repository.
<table>
<thead>
<tr>
<th>Functionality</th>
<th>User/Role API Method</th>
<th>Identity Directory Service Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the Role Type</td>
<td>Role.isUserApplicationRole</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>Role.isUserEnterpriseRole</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Role.isUserSeeded</td>
<td></td>
</tr>
<tr>
<td>Search Roles for a given search criteria</td>
<td>SearchResponse IdentityStore.searchRoles(int scope, SearchParameters params)</td>
<td>ResultSet&lt;Group&gt; GroupManager.searchGroups(SearchFilter filter, SearchOptions opts)</td>
</tr>
<tr>
<td>Search a Role by name/uniquename / guid</td>
<td>Role IdentityStore.searchRole(int searchType, String value)</td>
<td></td>
</tr>
<tr>
<td>Search both User and Roles for a given filter</td>
<td>SearchResponse IdentityStore.search(SearchParameters params)</td>
<td></td>
</tr>
<tr>
<td>Get all the roles assigned to user/group</td>
<td>SearchResponse getGrantedRoles(Principal principal, boolean direct)</td>
<td></td>
</tr>
<tr>
<td>Get all the roles owned by user/group</td>
<td>SearchResponse getOwnedRoles(Principal principal, boolean direct)</td>
<td></td>
</tr>
<tr>
<td>Get all the roles managed by user/group</td>
<td>SearchResponse getManagedRoles(Principal principal, boolean direct)</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

4.4 Moving From a Test to a Production Environment

Moving from one environment to another, especially from a test environment to production environment, provides you the flexibility to test applications in a test environment and then roll them out in the production environment.

The following topics describe the Identity Directory Service/libOVD properties that you need to modify while moving from a test environment to production environment:

- **Overview of Moving Between Environments**
- **Modifying Identity Directory Service/libOVD Move Plan**
- **Overview of Moving Between Environments**

You can move Identity Directory Service/libOVD to a new environment or from a test to a production environment. Moving Identity Directory Service/libOVD installation diminishes the amount of work that would otherwise be required to
reapply all the customization and configuration changes made in one environment to another.

- **Modifying Identity Directory Service/libOVD Move Plan**
  A move plan contains configuration settings of the source environment. You can customize the move plan settings for Oracle Fusion Middleware entities and components.

### 4.4.1 Overview of Moving Between Environments

You can move Identity Directory Service/libOVD to a new environment or from a test to a production environment. Moving Identity Directory Service/libOVD installation diminishes the amount of work that would otherwise be required to reapply all the customization and configuration changes made in one environment to another.

You can install, configure, customize, and validate Identity Directory Service/libOVD in a test environment. Once the system is stable and performs as required, you can create the production environment by moving a copy of the server and its configuration from the test environment, instead of redoing all the changes that were incorporated into the test environment.

### 4.4.2 Modifying Identity Directory Service/libOVD Move Plan

A move plan contains configuration settings of the source environment. You can customize the move plan settings for Oracle Fusion Middleware entities and components.

When you move between environments, you run the extractMovePlan script to create a move plan for the entity that you are moving. The extractMovePlan script extracts configuration information from the archive into a move plan. It also extracts any needed configuration plans. Before you apply the archive to the target, you must edit the move plan to reflect the values of the target environment.

You can modify properties with the scope of READ_WRITE. Do not modify the properties with the scope of READ_ONLY. For a comprehensive description and the procedure to follow for moving between environments, see About Changing the Network Configuration in *Administering Oracle Fusion Middleware*.

This section contains the following topics:

- **Locating Identity Directory Service/libOVD configGroup Elements**
- **Properties to Customize for Identity Directory Service/libOVD Move Plan**
- **Locating Identity Directory Service/libOVD configGroup Elements**
  Move plans usually contain multiple configGroup elements. When a property is associated with a particular configGroup element, the tables listing the properties group the properties by configGroup element.
- **Properties to Customize for Identity Directory Service/libOVD Move Plan**
  You can customize the properties of a move plan.
4.4.2.1 Locating Identity Directory Service/libOVD configGroup Elements

Move plans usually contain multiple configGroup elements. When a property is associated with a particular configGroup element, the tables listing the properties group the properties by configGroup element.

To locate Identity Directory Service/libOVD ConfigGroup, in the generated move plan, you must look for <type>LIBOVD_ADAPTERS</type>. This tag provides comprehensive information about the libOVD adapter properties that you might have to update. A property is associated with a particular configGroup element.

Each adapter is represented by a configProperty id tag of the form:

"LDAP:<context_name>:<adapter_name>"

Consider the following example: "LDAP:ids:myOID"

Table 4-1 shows the properties for the move plan for libOVD.

The following example shows a section of the move plan for Identity Directory Service/libOVD, with portion of the LIBOVD_ADAPTERS configGroup elements:

```xml
<configGroup>
  <type>LIBOVD_ADAPTERS</type>
  <configProperty id="LDAP:ids:myOID">
    <configProperty>
      <name>Context Name</name>
      <value>ids</value>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_ONLY</scope>
      </itemMetadata>
    </configProperty>
    <configProperty>
      <name>Adapter Name</name>
      <value>myOID</value>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_ONLY</scope>
      </itemMetadata>
    </configProperty>
    <configProperty>
      <name>LDAP URL</name>
      <value>ldap://hostname:1389</value>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_WRITE</scope>
      </itemMetadata>
    </configProperty>
    <configProperty>
      <name>LDAP Host Read Only</name>
      <value>false</value>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_WRITE</scope>
      </itemMetadata>
    </configProperty>
    <configProperty>
      <name>LDAP Host Percentage</name>
      <value>100</value>
    </configProperty>
  </configProperty>
</configGroup>
```
4.4.2.2 Properties to Customize for Identity Directory Service/libOVD Move Plan

You can customize the properties of a move plan.

Table 4-1 describes the move plan properties you can customize for Identity Directory Service/libOVD adapter.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context Name</td>
<td>The libOVD context to use with which the adapter is associated.</td>
<td>ids</td>
</tr>
<tr>
<td></td>
<td>This is a read-only property.</td>
<td></td>
</tr>
<tr>
<td>Adapter Name</td>
<td>The name of the adapter. This is a read-only property.</td>
<td>myOID</td>
</tr>
<tr>
<td>LDAP URL</td>
<td>The LDAP URL value for the adapter in the form of ldap://host:port.</td>
<td>ldap://slc05kym:1389</td>
</tr>
<tr>
<td>DN</td>
<td>The DN of the user to connect to the backend LDAP. This is a read-write property.</td>
<td>cn=orcladmin</td>
</tr>
<tr>
<td>Password File</td>
<td>The absolute path to the secure file containing the password of the user. This is a read-write property.</td>
<td>/tmp/p.txt</td>
</tr>
<tr>
<td>LDAP Host Read Only</td>
<td>The flag indicating if the given host is read only. The default value is false. This is a read-write property.</td>
<td>false</td>
</tr>
</tbody>
</table>
Table 4-1  (Cont.) Move Plan Properties for libOVD

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Host Percentage</td>
<td>It specifies the load percentage value for the given LDAP host. The default value is 100. This is a read-write property.</td>
<td>100</td>
</tr>
</tbody>
</table>

4.5 Tuning Configuration Parameters for IDS

Tuning is the adjustment or modification of parameters to meet specific deployment requirements. The default IDS configuration must be tuned for your deployment scenario.

You must review the requirements and recommendations in this section carefully.

This section contains the following topics:

- **Configuration Parameters for IDS**
- **WLST Commands to Set Tuning Parameters Using File-Based Configuration**
- **Constants to Set Tuning Parameters Using In-Memory Configuration**
- **Handling Firewall and Load Balancer Timeout Errors**
- **Configuring TLS Protocol Versions and Cipher Suites for Secure Connections**
- **Configuration Parameters for IDS**
  You can use configuration parameters to tune performance and to balance memory requirements for a real-time deployment scenario. Tuning these parameters based on your requirements can greatly enhance the scalability characteristics of an application.
- **WLST Commands to Set Tuning Parameters Using File-Based Configuration**
  The configuration information is stored in an XML file. You must use the WebLogic Scripting Tool (WLST) to modify the tuning parameters using the file-based configuration.
- **Constants to Set Tuning Parameters Using In-Memory Configuration**
  Use the constants to configure the tuning parameters using in-memory configuration.
- **Handling Firewall and Load Balancer Timeout Errors**
  It is imperative to set up timeout on firewalls and load balancers to improve the communication process. It helps to detect issues in a distributed system.
- **Configuring TLS Protocol Versions and Cipher Suites for Secure Connections**
  You can configure TLS protocol version and cipher suites using the WLST commands for the underlying libOVD adapter.
4.5.1 Configuration Parameters for IDS

You can use configuration parameters to tune performance and to balance memory requirements for a real-time deployment scenario. Tuning these parameters based on your requirements can greatly enhance the scalability characteristics of an application.

Table 4-2 lists the configuration parameters for IDS that require tuning for real deployment scenarios.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InitialPoolSize</td>
<td>The initial number of LDAP connections created when the LDAP connection pool is set up.</td>
</tr>
<tr>
<td>MaxPoolSize</td>
<td>The maximum number of LDAP connections allowed in the LDAP connection pool.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If a deployment has numerous concurrent requests coming in, then you must set this value appropriately to prevent running out of connections or waiting for a connection during an operation.</td>
</tr>
<tr>
<td>MaxPoolWait</td>
<td>These parameters determine the waiting time for free LDAP connection when all the LDAP connections in the connection pool are in use. IDS waits for MAX_POOLWAIT and MAX_POOLCHECKS milliseconds for a free connection to be available first and then tries to expand the connection pool.</td>
</tr>
<tr>
<td>MaxPoolChecks</td>
<td>This specifies the maximum idle time for an LDAP connection. In an LDAP connection remains idle for this amount of time, it will be closed when the next LDAP connection pool cleanup timer runs.</td>
</tr>
<tr>
<td>PoolCleanupInterval</td>
<td>This is the timer interval (in seconds) used by the LDAP connection pool cleanup timer. The LDAP connection pool cleanup timer runs using this timer interval to perform pool cleanup tasks like shrinking the connection pool based on the idle connection if needed.</td>
</tr>
<tr>
<td>MaxPoolConnectionIdleTime</td>
<td>This specifies the maximum idle time for an LDAP connection. In an LDAP connection remains idle for this amount of time, it will be closed when the next LDAP connection pool cleanup timer runs.</td>
</tr>
<tr>
<td>OperationTimeout</td>
<td>The amount of time in milliseconds IDS waits for an LDAP request to be acknowledged by the LDAP remote host.</td>
</tr>
<tr>
<td>ConnectTimeout</td>
<td>This specifies the LDAP connection timeout duration in milliseconds. If a connection cannot be established in this period, then the connection attempt is aborted.</td>
</tr>
<tr>
<td>HeartbeatInterval</td>
<td>This is the interval in seconds to check the availability of backend LDAP.</td>
</tr>
<tr>
<td>SocketOptions</td>
<td>This parameters set SO_TIMEOUT (in seconds), SO_REUSEADDR, TCP_NODELAY, SO_KEEPALIVE properties for the underlying JNDI sockets in the LDAP connection.</td>
</tr>
<tr>
<td>MaxPoolConnectionReuseTime</td>
<td>This specifies the maximum time any connection can potentially be reused after which the pool removes and closes a connection. The value is specified in seconds.</td>
</tr>
</tbody>
</table>
### Table 4-2 (Cont.) Configuration Parameters for IDS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolConnectionReclaimTime</td>
<td>This specifies the time duration in seconds that a borrowed connection can remain unused before it is automatically reclaimed by the pool.</td>
</tr>
<tr>
<td>Protocols</td>
<td>This specifies the protocol versions supported by IDS.</td>
</tr>
</tbody>
</table>

#### 4.5.2 WLST Commands to Set Tuning Parameters Using File-Based Configuration

The configuration information is stored in an XML file. You must use the WebLogic Scripting Tool (WLST) to modify the tuning parameters using the file-based configuration.

You use the following WLST commands to configure the tuning parameters:

**Note:**
In all the WLST command examples in this section, `ADAPTER_NAME` refers to the name of the IDS repository. For instance, the libOVD adapter name.

- **For** `InitialPoolSize`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='InitialPoolSize', value=10, contextName='ids')
  ```

- **For** `MaxPoolSize`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='MaxPoolSize', value=100, contextName='ids')
  ```

- **For** `MaxPoolWait` and `MaxPoolCheck`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='MaxPoolWait', value=1000, contextName='ids')
  
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='MaxPoolChecks', value=10, contextName='ids')
  ```

- **For** `PoolCleanupInterval`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='PoolCleanupInterval', value=300, contextName='ids')
  ```

- **For** `MaxPoolConnectionIdleTime`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='MaxPoolConnectionIdleTime', value=3600, contextName='ids')
  ```

- **For** `OperationTimeout`:
  ```
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='OperationTimeout', value=120000, contextName='ids')
  ```

- **For** `ConnectTimeout`
modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='ConnectTimeout', value=10000, contextName='ids')

- **For** HeartbeatInterval:
  
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='HeartBeatInterval', value=60, contextName='ids')

- **For** SocketOption:
  
  modifySocketOptions(adapterName='ADAPTER_NAME', reuseAddress=false, keepAlive=false, tcpNoDelay=true, readTimeout=1800, contextName='ids')

- **For** MaxPoolConnectionReuseTime
  
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='MaxPoolConnectionReuseTime', value=3600, contextName='ids')

- **For** PoolConnectionReclaimTime
  
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='PoolConnectionReclaimTime', value=180, contextName='ids')

- **For** Protocols
  
  modifyLDAPAdapter(adapterName='ADAPTER_NAME', attribute='Protocols', value='TLSv1.2', contextName='ids')

**Note:**

You must run the `activateLibOVDConfigChanges('ids')` WLST command or restart the WebLogic server for configuration changes to take effect.

### 4.5.3 Constants to Set Tuning Parameters Using In-Memory Configuration

Use the constants to configure the tuning parameters using in-memory configuration.

The configuration information is stored by the IDS consumer and is passed during run-time to IDS by invoking the `IdentityStoreConfig` class. For more information about using the class and its properties, see *Oracle Fusion Middleware Java API Reference for Identity Governance Framework Identity Directory*.

You can modify the following configuration parameters using the Java API class:

**Table 4-3  Field Name for Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Field Name to Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>InitialPoolSize</td>
<td>IdentityStoreConfig.INITIAL_POOLSIZE</td>
</tr>
<tr>
<td>MaxPoolSize</td>
<td>IdentityStoreConfig.MAX_POOLSIZE</td>
</tr>
<tr>
<td>MaxPoolWait</td>
<td>IdentityStoreConfig.MAX_POOLWAIT</td>
</tr>
<tr>
<td>MaxPoolChecks</td>
<td>IdentityStoreConfig.MAX_POOLCHECK</td>
</tr>
<tr>
<td>PoolCleanupInterval</td>
<td>IdentityStoreConfig.POOL_CLEANUP_INTERVAL</td>
</tr>
</tbody>
</table>

Chapter 4  
Tuning Configuration Parameters for IDS  
4-18
Table 4-3  (Cont.) Field Name for Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Field Name to Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxPoolConnectionIdleTime</td>
<td>IdentityStoreConfig.MAX_POOL_CONNECTION_IDLE_TIME</td>
</tr>
<tr>
<td>OperationTimeout</td>
<td>IdentityStoreConfig.CONN_TIMEOUT</td>
</tr>
<tr>
<td>ConnectTimeout</td>
<td>IdentityStoreConfig.CONNECT_TIMEOUT</td>
</tr>
<tr>
<td>HeartbeatInterval</td>
<td>IdentityStoreConfig.HEARTBEAT_INTERVAL</td>
</tr>
<tr>
<td>SocketOptions</td>
<td>IdentityStoreConfig.SOCKET_READTIMEOUT</td>
</tr>
<tr>
<td></td>
<td>IdentityStoreConfig.SOCKET_REUSEADDRESS</td>
</tr>
<tr>
<td></td>
<td>IdentityStoreConfig.SOCKET_KEEPALIVE</td>
</tr>
<tr>
<td></td>
<td>IdentityStoreConfig.SOCKET_TCP_NODELAY</td>
</tr>
<tr>
<td>MaxPoolConnectionReuseTime</td>
<td>IdentityStoreConfig.MAX_POOL_CONNECTION_REUSE_TIME</td>
</tr>
<tr>
<td>PoolConnectionReclaimTime</td>
<td>IdentityStoreConfig.POOL_CONNECTION_RECLAIM_TIME</td>
</tr>
</tbody>
</table>

4.5.4 Handling Firewall and Load Balancer Timeout Errors

It is imperative to set up timeout on firewalls and load balancers to improve the communication process. It helps to detect issues in a distributed system.

SocketOptions setting helps detect and safely close orphan socket connections caused by remote server failure. TCP waits for the configured duration of time for a response from the remote server before closing the socket. However, when there is a firewall or a Load Balancer between libOVD and the backend LDAP, then you must set the readTimeout value in the SocketOptions appropriately to prevent timeout errors. It is recommended that you set this value to a value which is less than the firewall or the Load Balancer timeout.

4.5.5 Configuring TLS Protocol Versions and Cipher Suites for Secure Connections

You can configure TLS protocol version and cipher suites using the WLST commands for the underlying libOVD adapter.

Use the modifyLDAPAdapter WLST command to configure the TLS protocol version for the underlying libOVD adapter. See modifyLDAPAdapter in Oracle® Fusion Middleware WLST Command Reference for Infrastructure Security.

You can configure the cipher suites by using the addCipherSuite and removeCipherSuite WLST commands respectively for the underlying libOVD adapter. See addCipherSuite and removeCipherSuite in Oracle® Fusion Middleware WLST Command Reference for Infrastructure Security.

4.6 Allowing Pass-through Attributes in IDS

In IDS while executing the Search or Update operation, you need to define every attribute that is used by IDS APIs in the entity definition. However, Identity Directory
allows you to dynamically add attributes on runtime. These are referred to as the pass-through attributes.

In certain scenarios attributes are specified dynamically. In other words, they could be used in requested attributes or filters without being defined in the entity definition. The pass-through feature implements this usage and does not throw any exception.