RSA Identity Governance and Lifecycle Collector Data Sheet For Oracle Internet Directory

Version 1.2 | November 2017

Table of Contents

Revision History

Revision Number	Description
Version 1.0	Oracle Internet Directory
Version 1.1	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle Oracle Internet Directory Identity Data Collector, Account Data Collector and Entitlement Data Collector
Version 1.2	Updated document with minimum version support.

Purpose

This data sheet provides the configuration information required to create a new data collector for Oracle Internet Directory.

Supported Software

RSA Identity Management and Governance 6.9.1 and later

RSA Identity Governance and Lifecycle 7.0.1 and later

Collector Type(s): Identity Data Collector, Account Data Collector, Entitlement Data Collector

Endpoint Application: Oracle Internet Directory 11.1.1.6.0

Prerequisites

The following software must be installed on your network before configuring the collector:

- Oracle Internet Directory should be installed and configured properly.

Manage Endpoint Credentials Using Password Vault

To use a third-party password vault to manage endpoint credentials, perform the following steps.

1. *Configure the password vault according to the third-party provider's instructions.*
2. *Create a new password vault profile in the RSA Identity Governance and Lifecycle system for retrieving the Oracle Internet Directory password from the vault. See the RSA Identity Governance and Lifecycle Help for more information about creating a password vault profile.*

Ensure that an Open LDAP account has been created at the configured password vault for storing the password.

Note: To use the dynamic password feature, step 1 must be completed. If a third-party password vault is not configured, configure the collector with a static password.

Identity Data Collector

Configuration

The configuration of the Account data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen while creating the Collector.

Field Name	**Value**
Collector Name	Oracle Internet Directory Identity Data Collector
Description	Oracle Internet Directory Identity Data Collector
Data Source Type	LDAP
Agent	AveksaAgent
Directory	N/A
Status	Active
Copy from	N/A
Scheduled	N/A

Configuration Information

The following table lists the parameters on the “Configuration Information” screen while creating the Collector.

For more information about using static or dynamic passwords during collector creation and in the configuration wizard, see Manage Endpoint Credentials Using a Password Vault in the Prerequisites section.

Field Name	**Value**
Host	<Host-Name or IP Address of machine hosting the Active Directory server>
Port	<Port Number to the server (Default Non SSL – 389 and SSL - 636)>

BindDN	<The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin)>
Static Password	Select this option to provide the password statically/manually. Enter the password for the Oracle Internet Directory administrator in the area provided.
Dynamic Password	*Select this option to use a configured password vault to manage the endpoint credentials.* After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during collector deployment and connection tests.
UseSSL	<Whether SSL should be used to connect or not>
Skip Certificate Validation	<If SSL is used then specify whether certificate should be skipped to validate> WARNING: NOT RECOMMENDED as it skips certificate chain validation.
Select Certificate	<Select correct certificate retrieved from Server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from Oracle Internet Directory in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server

Select Types of Identity Data to Collect

Select 'Users' as identity data type.

Field Name	**Value**
Users	<Enable the check-box to collect user identities. (Default: **true**)>

Map Collector Attributes to User Attributes

The following table lists the parameters on the "Map Collector Attributes to User Attributes" screen, while creating the Collector.

Field Name	**Value**
User Base DN	<Base DN of the OID user from where user identities are to be collected. (for

	example: OU=xx,DC=xx,DC=xx)>
User Search Scope	Search scope for users (can be ‘Subtree’ or ‘One Level’)
User Search Filter	User Search Filter
User ID	User ID (for example: cn)
Business Unit Id	<Business Unit Id>
Backup Supervisor	<Backup Supervisor>
Email Address	<mail attribute of the user>
First Name	<givenName attribute of the user>
Last Name	<sn attribute of the user>
Title	<title attribute of the user such as dn>
Unique Id	<uid attribute of the user>

Account Data Collector

Configuration

The configuration of the Account data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen while creating the Collector:

Field Name	**Value**
Collector Name	Oracle Internet Directory Account Data Collector
Description	Oracle Internet Directory’s Account Data Collector
Data Source Type	LDAP
Agent	AveksaAgent
Directory	A OID directory
Status	Active
Copy from	N/A
Scheduled	N/A

Configuration Information

The following table lists the parameters on the “Configuration Information” screen while creating the Collector.

For more information about using static or dynamic passwords during collector creation and in the configuration wizard, see Manage Endpoint Credentials Using a Password Vault in the Prerequisites section.

Field Name	**Value**
Host	<Host-Name or IP Address of machine hosting the Active Directory server>
Port	<Port Number to the server (Default Non SSL – 389 and SSL - 636)>

BindDN	<The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin)>
Static Password	Select this option to provide the password statically/manually. Enter the password for the Oracle Internet Directory administrator in the area provided.
Dynamic Password	*Select this option to use a configured password vault to manage the endpoint credentials.* After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during collector deployment and connection tests.
UseSSL	<Whether SSL should be used to connect or not. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using Secure Sockets Layer (SSL) technology. Before you configure SSL at your end, you must first make sure that LDAP over SSL (also known as LDAPS or LDAP over TLS) is enabled on your Oracle Internet Directory server. LDAP connections are not enabled by default. SSL should be used if you wish to add users with passwords or to change their domain passwords>
Skip Certificate Validation	<If SSL is used then specify whether certificate should be skipped to validate> WARNING: NOT RECOMMENDED as it skips certificate chain validation
Select Certificate	<Select Correct Certificate retrieved from OID in PEM format. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin)> Note: Keep this field blank if one wants to use default truststore of JVM or Server

Depending on the type of Account data selected following tables will help you with the screens that appear:

Mapping for Account and User Account Attributes

The following table lists the parameters on the “Map Collector Attributes to Account Attributes” screen while creating the Collector:

Field Name	**Value**
Account Base DN	<Base DN of the OID account from where accounts are to be collected. (for example: ou=people,dc=maxcrc,dc=com)>

Account Search Scope	<Define the search scope for collection. (for example, sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter (for example, (objectClass=inetOrgPerson))>
Account ID	<Any unique value for the accounts. (Default: cn)>
Account Disabled	pwdAccountLockedTime
Account Locked	pwdAccountLockedTime
External id	dn
User Account Control	-

Edit User Resolution Rules

The following table lists the parameters on the “Edit User Resolution Rules” screen while creating the Collector.

Field Name	**Value**
Target Collector	<Any created LDAP ADC. (Default: Users)>
User Attribute	<Unique attribute for mapping. (Default: User Id)>

Map Collector Attributes to Group Attributes

The following table lists the parameters on the “Map Collector Attributes to Group Attributes” screen while creating the Collector:

Field Name	**Value**
Group Base DN	<Base DN for group starting from where groups are to be collected. (for example: n=testGroups,dc=aveksa1,dc=local)>
Group Search Scope	<Define the search scope for collection. (for example, sub-tree or one level)>

Group Search filter	<Searches the groups based on the provided filter. (Default: (objectclass=group))>
Collect Primary Group Members	<enable the check-box if primary group member collection is desired. (Default: false)>
Group ID/Name	<Any unique value for the groups. (Default: cn)>
Member of Group	<member attribute for group. (Default: member)>
Owner	<Attribute to map to the group owner>

Edit Member Account Resolution Rules

The following table lists the parameters on the “Edit Member Account Resolution Rules” screen, while creating the Collector:

Field Name	**Value**
Target Collector	<OID Account Data Collector>
Account Attribute	<Account Name>

Edit Sub-group Resolution Rules

The following table lists the parameters on the “Edit Sub-group Resolution Rules” screen, while creating the Collector.

Field Name	**Value**
Target Collector	<OID Account Data Collector>
Group Attribute	<Name>

Entitlement Data Collector

Configuration

The configuration of the Entitlement data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen, while creating the Collector.

Field Name	**Value**
Collector Name	Oracle Internet Directory Entitlement Data Collector
Description	Oracle Internet Directory Entitlement Data Collector
Data Source Type	LDAP
Agent	AveksaAgent or any configured agent.
Directory	Directory name under which Data Collector is being created such as OID, LDAP Directory
Status	Active
Copy from	Select already created OID EDC Collector If you want to copy details from it.
Scheduled	Select Yes if You want to Schedule Collector.

Configuration Information

The following table lists the parameters on the “Configuration Information” screen, while creating the Collector.

For more information about using static or dynamic passwords during collector creation and in the configuration wizard, refer to Manage Endpoint Credentials Using a Password Vault in the Prerequisites section.

Field Name	**Value**
Host	<Host name or IP address of the server>

Port	<Port number of the server(Default: 389)>
Bind DN	<The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin)>
Static Password	Select this option to provide the password statically/manually. Enter the password for the Oracle Internet Directory administrator in the area provided.
Dynamic Password	*Select this option to use a configured password vault to manage the endpoint credentials.* After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during collector deployment and connection tests.
Use SSL	<Whether SSL should be used to connect or not. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using Secure Sockets Layer (SSL) technology. Before you configure SSL at your end, you must first make sure that LDAP over SSL (also known as LDAPS or LDAP over TLS) is enabled on your LDAP server. LDAP connections are not enabled by default. SSL should be used if you wish to add users with passwords or to change their domain passwords>
Skip Certificate Validation	<If SSL is used then specify whether certificate should be skipped to validate> WARNING: NOT RECOMMENDED as it skips certificate chain validation
Select Certificate	<Select Certificate retrieved from OID. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from OID in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server

Depending on the type of entitlement data selected, following screens will appear:

User Data Attribute Modeling Options

The following table helps you with the parameters on “User Data Attribute Modeling” while creating the Collector:

Field Name	**Value**
User Base DN	<Base DN of the OID user from where users are to be collected. (for example:

	CN=Users,dc=aveksadev,dc=com)>
User Search Scope	<Define the search scope for collection. (for example, sub-tree or one level)>
User Search filter	<Searches the users based on the provided filter> (for example: (objectClass=inetOrgPerson))
User ID	<Any unique value for the users. (Default: cn)>
Custom Attributes	<The attribute names specified in 'Collect attribute value as resource' and 'Collect attribute value as application role' will be stored as the custom attribute selected>

There are three ways to collect attributes:

a. Collect attribute name values as resource-action pairs

b. Collect attribute value as resource

c. Collect attribute value as application role

Field Name	**Value**
Attributes To Extract	<List of attributes to extract> (for example: cn)

Note: At least one of the above listed three **MUST** be selected.

Map Collector Attributes to Group Attributes

The following table lists the parameters on the “Map Collector Attributes to Group Attributes” screen while creating the Collector:

Field Name	**Value**
Group Base DN	<Base DN for group starting from where groups are to be collected. (for example: OU=TestGroups,o=oid)>
Group Search Scope	<Define the search scope for collection. (for example, sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (Default: (objectclass=groupOfNames))>
Collect Primary Group Members	<enable the check-box if primary group member collection is desired. (Default: false)>

Group ID/Name	<Any unique value for the groups. (Default: cn)>
Member of Group	<member attribute for group. (Default: member)>

Entitled User Evaluation

The following table helps you with parameters on “Entitled User Evaluation” screen while creating the Collector

Field Name	**Value**
Associated Identity Collector	<Created LDAP Identity Collector>
Entitled user value evaluates to	<User Id>

For collecting account entitlement follow the below configuration:

Account Data Attribute Modeling Options

The following table lists the parameters on the “Account data attribute modeling options” screen while creating the Collector

Field Name	**Value**
Account Base DN	<Base DN of the OID account starting from where accounts are to be collected. (for example: OU=xx,dc=xx,dc=xx)>
Account Search Scope	<Define the search scope for collection. (for example, sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter> (for example: objectClass=inetOrgPerson)
Account ID	<Any unique value for the accounts. (Default: cn)>
Custom Attributes	<The attribute names specified in 'Collect attribute value as resource' and 'Collect attribute value as application role' will be stored as the custom attribute selected>

There are three ways to collect attributes:

a. Collect attribute name values as resource-action pairs

b. Collect attribute value as resource

c. Collect attribute value as application role

The following table helps you with any of the above cases:

Field Name	**Value**
Attributes To Extract	<List of attributes to extract> (for example: cn)

Note: At least one of the above listed three **MUST** be selected.

COPYRIGHTS

TRADEMARKS