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

Version 1.1 | July 2017

Table of Contents

Revision History

Revision Number	**Description**
Version 1.0	Oracle Directory Server
Version 1.1	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle Oracle Directory Server Identity Data Collector, Account Data Collector and Entitlement Data Collector

Purpose

This data sheet provides the configuration information required to create a new Oracle Directory Server Identity Data Collector, Account Data Collector and Entitlement Data Collector.

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 Directory Server

Prerequisites

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

- Oracle Directory Server

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 Directory Server password from the vault. See the RSA Identity Governance and Lifecycle Help for more information about creating a password vault profile.*

Ensure that an Oracle Directory Server 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 Identity 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 Directory Server Identity Data Collector
Description	Oracle Directory Server’s Identity Data Collector
Data Source Type	LDAP
Agent	AveksaAgent or any other collector agent
Directory	Select existing directory or create new one for collector association
Status	Active
Copy from	Select existing Oracle Directory Server Identity Collector to copy its configuration details
Scheduled	Select “yes” if you want to schedule it

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 theOracle Directory Server 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 Directory Server 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 Active 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 Server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from ODS 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 ODS user from where user identities are to be collected. (for e.g.: OU=xx,DC=xx,DC=xx)>
User Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>
User Search filter	<Searches the users based on the provided>
User ID	<Any unique value for the users.>
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>
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 Directory Server Account Data Collector
Description	Oracle Directory Server's Account Data Collector
Data Source Type	LDAP
Agent	AveksaAgent or any other collector agent
Directory	Select existing directory or create new one for collector association
Status	Active
Copy from	Select existing Oracle Directory Server Account Collector to copy its configuration details
Scheduled	Select "yes" if you want to schedule it

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 Directory Server 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 IBM Tivoli 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 Active 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 ODS Server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from ODS in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server
Ignore Referral	<Whether Referral should be ignored or not. If referral is ignored and if a subtree search is performed, the search will return all objects within the specified domain that meet the search criteria. The search will also return referrals to any subordinate domains that are direct descendants of the directory server domain. If referrals are not ignored and if a subtree

	search is performed, the underlying LDAP API will automatically attempt to bind to any referrals and add the search results to the result set>

Select Types of Account Data to Collect

Select checkbox for Account, User Account Mapping and Groups for collection.

Field Name	Value
Accounts	<Enable the check-box to collect accounts. (Default: false)>
User Account Mappings	<Enable the check-box to collect user account mappings. (Default: false)>
Groups	<Enable the check-box to collect groups. (Default: false)>

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

Map Collector Attributes to User Account Attributes

The following table lists the parameters on the “Map for Account and User Account Attributes” screen, while creating the Collector.

Field Name	Value
Account Base DN	<Base DN of the ODS account from where accounts are to be collected. (for e.g.: CN=Users,dc=aveksadev,dc=com)>
Account Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter> (e.g. (objectClass=inetOrgPerson))
Account ID	<Any unique value for the accounts. (Default: cn)>
User ID	<Any unique value for the users. (Default: cn)>

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> (e.g.: OU=TestGroups,o=ods)
Group Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (e.g : (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)>
Owner	<Attribute to map to the group owner>

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)>

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	<Oracle Directory Server 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	<Oracle Directory Server 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 Directory Server Entitlement Data Collector
Description	Oracle Directory Server’s Entitlement Data Collector
Data Source Type	LDAP
Agent	AveksaAgent or any other collector agent
Directory	Select existing directory or create new one for collector association
Status	Active
Copy from	Select existing Oracle Directory Server Entitlement Collector to copy its configuration details
Scheduled	Select “yes” if you want to schedule it

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 Directory Server 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 IBM Tivoli 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 Active 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 ODS Server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from ODS in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server.
Ignore Referral	<Whether Referral should be ignored or not. If referral is ignored and if a subtree search is performed, the search will return all objects within the specified domain that meet the search criteria. The search will also return referrals to any subordinate domains that are direct descendants of the directory server domain. If referrals are not ignored and if a subtree

	search is performed, the underlying LDAP API will automatically attempt to bind to any referrals and add the search results to the result set>

Select Types of Entitlement Data to Collect

Case 1: Select 'Users' & Enable 'Collect Groups as Application Roles'

User Data Attribute Modeling Options

Field Name	Value
User Base DN	<Base DN of the ODS user from where users are to be collected. (e.g.: CN=Users,dc=aveksadev,dc=com)>
User Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
User Search filter	<Searches the users based on the provided filter>(e.g = (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>

Collect attribute name values as resource-action pairs

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as resource

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as application role

Field Name	Value
Attributes To Extract	<List of attributes to extract>

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

Mapping for group attributes

Field Name	Value
Group Base DN	<Base DN for group starting from where groups are to be collected. (e.g.: OU=TestGroups,o=oid)>
Group Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (e.g. : (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

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

Case 2: Select ‘Accounts’ & Enable ‘Collect Groups as Application Roles’

Account Data Attribute Modeling Options

Field Name	Value
Account Base DN	<Base DN of the OID account starting from where accounts are to be collected. (e.g.: OU=xx,dc=xx,dc=xx)>
Account Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter>(e.g = (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>

Collect attribute name values as resource-action pairs

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as resource

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as application role

Field Name	Value

Attributes To Extract	<List of attributes to extract>

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

Mapping for group attributes

Field Name	Value
Group Base DN	<Base DN for group starting from where groups are to be collected. (e.g.: cn=testGroups,dc=aveksa1,dc=local)>
Group Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (e.g. : (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)>

Account Evaluation

Field Name	Value
Associated Account Collector	<Created LDAP Account Collector>
Account value evaluates to	<Account Name>

Case 3: Select 'Users' and Disable 'Collect Groups as Application Roles'

User Data Attribute Modeling Options

Field Name	Value
User Base DN	<Base DN of the ODS user from where users are to be collected. (e.g.: CN=Users,dc=aveksadev,dc=com)>
User Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
User Search filter	<Searches the users based on the provided filter> (e.g. : (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>

Collect attribute name values as resource-action pairs

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as resource

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as application role

Field Name	Value
Attributes To Extract	<List of attributes to extract>

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

Entitled User Evaluation

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

Case 4: Select 'Accounts' and Disable 'Collect Groups as Application Roles'

Account Data Attribute Modeling Options

Field Name	Value
Account Base DN	<Base DN of the ODS account starting from where accounts are to be collected. (e.g.: OU=xx,dc=xx,dc=xx)>
Account Search Scope	<Define the search scope for collection. (e.g., sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter>(e.g. : (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>

Collect attribute name values as resource-action pairs

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as resource

Field Name	Value
Attributes To Extract	<List of attributes to extract>

Collect attribute value as application role

Field Name	Value
Attributes To Extract	<List of attributes to extract>

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

Account Evaluation

Field Name	Value
Associated Account Collector	<Created LDAP Account Collector>
Account value evaluates to	<Account Name>

COPYRIGHTS

TRADEMARKS