Purpose

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

Supported Software

- *RSA Identity Management and Governance 6.8.1 and later*
- *RSA Via Lifecycle and Governance 7.0.0 and later*
- *RSA Identity Governance and Lifecycle 7.0.1 and later*
- *Application: IBM Tivoli Directory Server 6.1 and later*

Identity Data Collector

Prerequisites

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 IBM Tivoli 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 IBM Tivoli Directory 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.

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	IBM Tivoli Directory Server Identity Data Collector
Description	IBM Tivoli Directory Server Identity Data Collector
Data Source Type	IBM Tivoli Directory Server
Agent	AveksaAgent

Directory	Directory name under which Data Collector is being created e.g. IBM Tivoli Directory
Status	Active
Copy from	N/A
Scheduled	N/A

Connection Configuration

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 non-SSL port: 389 and SSL port: 636)>
Bind DN	<The DN of the ITDS 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.
Disable Paging	<Want to enable paging or not (Default: false)>
Page Size	<Page Size must not exceed MaxPageSize attribute in IBM Tivoli Directory Server. (Default: 1000)>
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	<Whether Certificate validation should be skipped or not. (Default: false)> WARNING: NOT RECOMMENDED as it skips certificate chain validation
Select Certificate	<Lists down the certificates fetched from the server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from IBM Tivoli Directory Server 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

The following table lists the parameters for the select types of identity data to collect.

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 Attribute to User Attributes” screen, while creating the Collector.

Field Name	Value
User Base DN	<Base DN of the ITDS user from where user identities are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
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 filter e.g. (objectclass=inetorgperson) , (&(objectclass=OrclUser)(objectclass=OrclUserV2)) etc.>
User ID	<Any unique value for the users. (Default: 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>
Is Terminated	<Is terminated attribute of the user>
Last Name	<sn attribute of the user>
Termination Date	<Termination date of the user>
Title	<title attribute of the user e.g. title, dn etc.>
Unique Id	<uid attribute of the user>

Account Data Collector

Prerequisites

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

- IBM Tivoli Directory Server (ITDS)

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	IBM Tivoli Directory Server Account Data Collector
Description	IBM Tivoli Directory Server's Account Data Collector
Data Source Type	Ldap
Agent	AveksaAgent
Directory	Directory name under which Account Data Collector is being created e.g. ITDS, Ldap Directory etc. While creating directory, make sure that radio buttons 'Allow Account Disabling' and 'Allow Account Locking' should be clicked to option 'Yes'
Status	Active
Copy from	N/A
Scheduled	N/A

Connection Configuration

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.

Field Name	Value
Host	<Host name or IP address of the server>
Port	<Port number of the server (Default non-SSL port: 389 and SSL port: 636)>
Bind DN	<The DN of the ITDS 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.
Disable Paging	<Want to enable paging or not (Default: false)>
Page Size	<Page Size must not exceed MaxPageSize attribute in IBM Tivoli Directory Server. (Default: 1000)>
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	<Whether Certificate validation should be skipped or not. (Default:

Validation	false)> WARNING: NOT RECOMMENDED as it skips certificate chain validation
Select Certificate	<Lists down the certificates fetched from the server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from IBM Tivoli Directory Server in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server

Select types of account data to collect

The following table lists the parameters for the select types of identity data to collect.

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)>

Mapping for account and user account attributes

The following table lists the parameters on the “Mapping for account and user account attributes” screen.

Field Name	**Value**
Account Base DN	<Base DN of the ITDS account from where accounts are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
Account Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>

Account Search filter	<Searches the accounts based on the provided filter (for e.g. (objectClass=inetOrgPerson))>
Account ID	<Any unique value for the accounts. (Default: cn)>
Account Disabled	ibm-pwdAccountLocked
Account Locked	ibm-pwdAccountLocked
External id	Dn
User ID	<Any unique value for the users. (Default: dn)>

Mapping for Group attributes

The following table lists the parameters on the "Mapping for group attributes" screen.

Field Name	**Value**
Group Base DN	<Base DN for group starting from where groups are to be collected. (for e.g.: ou=TestGroups,dc=aveksa,dc=com)>
Group Search Scope	<Define the search scope for collection. (for e.g., 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)>

External Id	distinguishedName
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.

Field Name	**Value**
Target Collector	<Any created LDAP IDC. (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.

Field Name	**Value**
Target Collector	<ITDS Account Data Collector>
Account Attribute	< External id >

Edit Sub-Group Resolution Rules

The following table lists the parameters on the "Edit subgroup resolution rules" screen.

Field Name	**Value**
Target Collector	<ITDS Account Data Collector>
Group Attribute	< External id >

Entitlement Data Collector

Prerequisites

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

- IBM Tivoli Directory Server (ITDS)

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	IBM Tivoli Directory Server Entitlement Data Collector
Description	IBM Tivoli Directory Server's Entitlement Data Collector
Data Source Type	Ldap
Agent	AveksaAgent
Directory	Directory name under which Entitlement Data Collector is being created e.g. ITDS, Ldap Directory etc. While creating directory, make sure that radio buttons 'Allow Account Disabling' and 'Allow Account Locking' should be clicked to option 'Yes'
Status	Active
Copy from	N/A
Scheduled	N/A

Connection Configuration

The following table lists the parameters displayed on the "Configuration Information" screen during collector creation.

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

Field Name	Value
Host	<Host name or IP address of the server>
Port	<Port number of the server (Default non-SSL port: 389 and SSL port: 636)>
Bind DN	<The DN of the ITDS 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.
Disable Paging	<Want to enable paging or not (Default: false)>
Page Size	<Page Size must not exceed MaxPageSize attribute in IBM Tivoli Directory Server. (Default: 1000)>
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	<Whether Certificate validation should be skipped or not. (Default: false)> WARNING: NOT RECOMMENDED as it skips certificate chain validation
Select Certificate	<Lists down the certificates fetched from the server. Selected certificate will be appeared in PEM format in Certificate field>
Certificate	<Certificate retrieved from IBM Tivoli Directory Server in PEM format> Note: Keep this field blank if one wants to use default truststore of JVM or Server

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 ITDS user from where users are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
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 filter (for 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. (for e.g.: ou=TestGroups,dc=aveksa,dc=com)>
Group Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (Default: (objectclass= groupofNames))>
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 ITDS account starting from where accounts are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
Account Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter>(for 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. (for e.g.: ou=TestGroups,dc=aveksa,dc=com)>
Group Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>
Group Search filter	<Searches the groups based on the provided filter. (Default: (objectclass=groupofNames))>
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 ITDS user from where users are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
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 filter>(for 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 ITDS account starting from where accounts are to be collected. (for e.g.: ou=TestUsers,dc=aveksa,dc=com)>
Account Search Scope	<Define the search scope for collection. (for e.g., sub-tree or one level)>
Account Search filter	<Searches the accounts based on the provided filter>(for 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