RSA Identity Governance and Lifecycle Data Sheet
for
IBM Tivoli Directory Server Connector

Version 1.1 | March 2017

Contents

Revision History

Revision Number	Description
Version 1.0	IBM ITDS
Version 1.1	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle ITDS Connector

PURPOSE

This data sheet provides the configuration information required to create a new connector for IBM Tivoli Directory Server.

SUPPORTED SOFTWARE

RSA Identity Governance and Lifecycle Version: 6.8.1 and above.

Application: IBM Tivoli Directory Server (ITDS) 6.1 and later.

PREREQUISITES

IBM Tivoli Directory Server should be installed and configured properly.

SSL communication

For SSL communication, installing required certificates is must.

IBM Tivoli Directory Server (ITDS) and certificate authority (CA) certificates (only if required) should be added to the appropriate keystores. Follow the steps mentioned below for adding certificates to the keystores of WebSphere, WebLogic and WildFly application servers:

WebSphere Application Server:

1. Log in to WebSphere Administrative console (http://<HOST_NAME>:9060/ibm/console/login.do)
2. In left panel, expand 'Security' menu.
3. Click 'SSL certificate' and 'key management' link.
4. Click 'Manage endpoint security configurations' link under 'Configuration Settings'.
5. Select 'Outbound' properties for the appropriate node.
6. Click appropriate node link to get the properties.
7. Under 'Related Items', click 'Key stores and certificates' and click the 'NodeDefaultTrustStore' key store.
8. Under 'Additional Properties', click 'Signer certificates' and then click 'Retrieve from Port'.
9. In the 'Host' field, enter 'host name', enter 'SSL port(default-636)' in the 'Port' field, and '<alias_name>' in the 'Alias' field.
10. Click 'Retrieve Signer Information'.
11. Verify that the certificate information is for the trusted certificate.
12. Click 'Apply' and 'Save'.
13. Login into WebSphere machine using SSH (example: putty).
14. On command prompt, run: /home/oracle/AFX/afx stop.
15. On command prompt, run: /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1.

16. On command prompt, run: /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1.
17. On command prompt, run: /home/oracle/AFX/afx start.

WebLogic Application Server:

1. Download/Retrieve IBM ITDS and CA (only if required) SSL certificates in PEM format and save them at location /home/oracle.
2. Log in to WebLogic Administrative console. (http://<HOST_NAME>.aveksa.local:7001/console/login/LoginForm.jsp)
3. Click 'Servers' link in 'Environment' section under 'Domain Configurations'.
4. Click 'aveksaServer' link.
5. Go to 'SSL' tab.
6. Click 'Advanced' link.
7. Select 'HostName Verification = None'.
8. Save the settings.
9. Login into WebLogic machine using SSH (example: putty).
10. Change directory: cd /home/oracle/
11. Add the saved certificate and CA (only if required) certificates in server.keystore by using keytool
    Run: keytool -import -file <cert.pem> -alias <cert_alias> -keystore server.keystore
12. Restart SSL on WebLogic Server as mentioned below.
13. Go to Servers -> controls tab.
14. Select/check aveksaServer (admin) and then click Restart SSL.
15. Restart the Server. Go to /home/oracle/AFX/afx stop.
    Run:/home/oracle/wls/12.1.3.0/user_projects/domains/aveksaDomain/bin/stopWebLogic.sh.
    Run:/home/oracle/wls/12.1.3.0/user_projects/domains/aveksaDomain/bin/startWebLogic.sh.
    /home/oracle/AFX/afx start.

WildFly Application Server:

1. Download/retrieve IBM ITDS and CA (only if required) SSL certificates in PEM format and save them.
2. cd <$JAVA_HOME>/jre/lib/security.
3. Add certificates in cacerts by using keytool
   keytool -import -file <cert.pem> -alias <cert_alias> -keystore cacerts

   Password for keystore (unless you have made any changes): changeit

   Run: keytool -import -file <certificate_path> -alias <certificate_alias> -keystore cacerts
4. Restart Server :
   Run:
   afx stop

acm stop
acm start
afx start

Manage Endpoint Credentials Using a Password Vault

To use a third-party password vault to manage the 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 ITDS password from the vault. See the RSA Identity Governance and Lifecycle Help for more information about creating a password vault profile.
3. Ensure that an ITDS 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 connector with a static password.

Configuration

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

General

The following table lists the parameters on the "General" screen, while creating the connector.

Field Name	Value
Name	IBM Tivoli Directory Server Connector
Description	IBM Tivoli Directory Server's Connector
Server	**AFX Server**
Connector Template	*IBM Tivoli's Directory Server*
State	**Test**

Export As Template	Provide any name to export connector configuration as connector template

Settings

The following table lists the parameters on the "Settings" screen, while creating the connector.

Field Name	Value
Host	<Host name or IP address to the server>
Port	<Port Number of the server> (Default non-SSL port: 389 and SSL port: 636)
Use Secure Connection	<Check the checkbox to enable secure connection> (Default is false)
Login Distinguished Name	<Distinguished Name to Login to the server>
Static Password	Select this option, if you want to provide the password statically/manually. Fill in the value of password for the ITDS administrator user 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 connector deployment and connection tests.
Timeout(seconds)	<Timeout for operations>(Default is 10)
Account DN Prefix	<Prefix for Account Distinguished Name>(Default is CN)
Account DN Suffix	<Suffix for Account Distinguished Name>
Group DN Prefix	<Prefix for Group Distinguished Name>(Default is CN)

Group DN Suffix	<Suffix for Group Distinguished Name>
DN Suffix Mappings	<Suffix Mappings for Distinguished Name>
Object classes to create account	<List of object classes to create Account (UserObjectClasses)> e.g. 'top','person','organizationalPerson','inetOrgPerson'
Object classes to create group	<List of object classes to create group (GroupObjectClasses)> e.g. 'top','groupOfNames'
User membership attribute for group	<User membership attribute for Group>(Default is member)
Use full DN for user membership attribute value	<Wants to use full DN for User membership attribute value on Group object or not> (Default is true)

Capabilities

The following commands are supported by the RSA Identity Governance and Lifecycle IBM ITDS connector:

- Create an Account on a server
- Delete an Account from a server
- Reset an Account's password
- Add Account to Group
- Remove Account From Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account

- Unlock an Account
- Create a Group
- Delete a Group
- Update a Group

Create an Account

The following table lists the parameters on the "CreateAccount" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${AccountTemplate.AccountName}
Description	Full DN of account or login name

Field Name	**Value**

Parameter Name	CN
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Common Name
Mapping	${AccountTemplate.CN}
Description	Name that represents an object. It is used to perform searches

Field Name	**Value**
Parameter Name	sn
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Last Name

Mapping	${User.Last_Name}
Description	Surname of a person

Field Name	**Value**
Parameter Name	givenName
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	First Name
Mapping	${User.First_Name}
Description	given name of a person

Field Name	**Value**
Parameter Name	mail
Type	STRING

Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Email address
Mapping	${User.Email_Address}
Description	simple SMTP address of a person

Field Name	**Value**
Parameter Name	Password
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**Yes**
Display Name	Initial password to set
Mapping	${AccountTemplate.Password}
Description	password which is required for login

Delete an Account from a server

The following table lists the parameters on the "Delete Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Reset an Account's Password

The following table lists the parameters on the "Reset Password" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-

Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	Password
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**Yes**
Display Name	Password
Mapping	No mapping
Description	New password to reset an old password

Add Account to Group

The following table lists the parameters on the "Add an Account to Group" screen.

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account DN or Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Field Name	Value
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**

Display Name	Group DN or Group Name
Mapping	${Group.Name}
Description	Full DN of group or group name

Remove Account from Group

The following table lists the parameters on the "Remove Account from Group" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account DN or Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	Group

Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Group DN or Group Name
Mapping	${Group.Name}
Description	Full DN of group or group name

Enable Account

The following table lists the parameters on the "Enable an Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}

Description	Full DN of account or login name

Disable Account

The following table lists the parameters on the "Disable an Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Update Account

The following table lists the parameters on the "Update an Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING

Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Move Account

The following table lists the parameters on the "Move Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account DN or Account Name
Mapping	${Account.Name}
Description	Full DN of Account or login name

Field Name	Value
Parameter Name	NewParentDN
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	New Parent's DN
Mapping	No mapping
Description	DN of new account base or organizational unit

Lock an Account

The following table lists the parameters on the "Lock an Account" screen.

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**

Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Unlock an Account

The following table lists the parameters on the "Unlock an Account" screen.

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Account Name
Mapping	${Account.Name}
Description	Full DN of account or login name

Create a group

The following table lists the parameters on the "Create Group" screen.

Field Name	Value
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Group Name
Mapping	
Description	Full DN of group

Field Name	Value
Parameter Name	CN
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**

Display Name	Common Name
Mapping	No mapping
Description	Name that represents an object. It is used to perform searches

Field Name	**Value**
Parameter Name	Member
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Member account Name
Mapping	No mapping
Description	Full DN of account

Delete a group

The following table lists the parameters on the "Delete Group" screen.

Field Name	**Value**
Parameter Name	Group

Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Group Name
Mapping	${Group.Name}
Description	Full DN of group

Update a group

The following table lists the parameters on the "Update a Group" screen.

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	Group Name
Mapping	${Group.Name}

Description	Full DN of group

TROUBLESHOOTING

This section describes common errors when configuring the RSA Identity Governance and Lifecycle components for IBM ITDS and solutions.

- Dynamic password is used on Connector Settings page and the connector is not getting deployed with error displayed as: Password Vault Error.

  This may happen if there is an error in retrieving the password using the mentioned profile. You need to check if the values provided in the profile for password retrieval are valid and adequate permissions are present on the vault for fetching the password.

Copyrights

Trademarks