RSA Identity Governance and Lifecycle Collector Data Sheet for IBM Notes

Version 1.3 | Jan 2018

Contents

Purpose **4**

Supported Software **4**

Prerequisites **4**

JBoss *4*

WildFly *4*

WebSphere *5*

WebLogic *6*

Enable SSL for DIIOP on IBM Notes Server *7*

Identity Data Collector **7**

Configuration *7*

Collector Description *7*

Configuration Information *8*

Map Collector Attributes to User Attributes *8*

Account Data Collector **10**

Configuration *10*

Collector Description *10*

Configuration Information *10*

Map Collector Attributes to Account Attributes *11*

Map Collector Attributes to Account Mapping Attributes *12*

Map Collector Attributes to Group Attributes *12*

Edit User Resolution Rules *12*

Edit Member Account Resolution Rules *12*

Edit Sub-Group Resolution Rules *13*

Edit Group Owner Resolution Rules *13*

Entitlement Data Collector **13**

Set up Custom Attribute *14*

Configuration *14*

Collector Description *14*

Configuration Information *15*

Group Evaluation *16*

Account Evaluation *16*

Revision History

Revision Number	**Description**
Version 1.0	IBM Notes Collector
Version 1.1	Added the DIIOP SSL configuration details
Version 1.2	Changed name from Lotus Notes to IBM Notes
Version 1.3	Changed Old RSA Logo and minor modifications.

Purpose

This data sheet provides the configuration information required to create a new collector.

Supported Software

RSA Identity Governance and Lifecycle **Version*:*** *6.8.1, 6.9.1 and above*

Application: *IBM Notes Domino 8.5 and 9.0.1 (Support for SSL is from Domino server version 9.0.1 Fix Pack 5)*

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

Prerequisites

IBMNotes Client API(s) need to be used which require an authenticated session. An Administrator account should be created on IBMNotes, which is a member of LocalDomainAdmins group, and this will be used for communicating with the IBMNotes server.

JBoss

1. Create a "lib" directory under
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/LotusNotesIdentityCollector1
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/LotusNotesAccountCollector1
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/LotusNotesEntitlementCollector1

2. Copy the NCSO.jar from their IBM Notes installation into the "lib" directories created above. The NCSO.jar should reside in <your_domino_installation>\data\domino\java
3. Restart ACM.

Note that the above steps have to be repeated after upgrading or hotfixing ACM as the Collectors directory will be overridden.

Without performing the above steps, the IBM Notes Collectors will fail with a "java.lang.NoClassDefFoundError" when they are run. However, other modules in ACM won't be affected if the NCSO.jar is absent.

WildFly

On an RSA Identity Governance and LifeCycle appliance or software appliance running v7.0 or later, you must use the customizeACM.sh tool to extract the aveksa.ear file, customize it and repackage it. The following procedure requires that you know how to use the customizeACM.sh tool. For more information, see "Customize RSA Identity Governance and LifeCycle" in the *Installation Guide*.

Customize RSA Identity Governance and LifeCycle

You can customize RSA Identity Governance and LifeCycle by modifying the aveksa.ear file located in /home/oracle/archive.

RSA provides a utility (customizeACM.sh in /home/oracle/deploy) that allows you to conveniently extract aveksa.ear file and rebuild a customized version.

Procedure

1. Log on to the appliance as the admin user via ssh tool. e.g. Putty
2. Verify that RSA Identity Governance and LifeCycle is running. Enter 'sudo service aveksa_server status' command.
   For running server, message displayed is: Aveksa Compliance Manager Server is running
   If the message indicates that the server is not running, enter 'sudo service aveksa_server start'.
3. Change to the oracle user. Enter 'su – oracle'
4. Go to /home/oracle/deploy.
5. Run the customizeACM.sh script to extract the .ear file, specifying the location of .ear file that you want to modify. Enter 'customizeACM.sh -c <path to the ear file>'
   Content of the .ear file will be extracted to a directory at the given location: /tmp/customizeACM/.

Note: If you do not specify the path to the .ear file, the script prompts you to use the currently deployed .ear file. If you want to use the currently deployed .ear, enter 'yes'. If you do not want to use the currently deployed .ear, enter 'no'.
e.g customizeACM.sh –c

6. Go to /tmp/customizeACM/ and modify the extracted files.
   Create a "lib" directory under
   /tmp/customizeACM/aveksa.war/LotusNotesIdentityCollector1/
   /tmp/customizeACM/aveksa.war/LotusNotesAccountCollector1
   /tmp/customizeACM/aveksa.war/LotusNotesEntitlementCollector1

7. Copy NCSO.jar from the IBM Notes installation into the "lib" directories created above. The NCSO.jar should reside in <your_domino_installation>\data\domino\java

8. When you finish modifying the files, run the customizeACM.sh script again to rebuild the .ear file. Go to /home/oracle/deploy, enter 'customizeACM.sh -d'
   The script performs the following tasks:
   - Archives the new .ear file to the following location, appending a time and date stamp to the name: /home/oracle/archive.
   - Deploys the new customized .ear file.

Note: No need to Restart ACM or AFX

WebSphere

- Copy the NCSO.jar from their IBM Notes installation into the "lib" directories created above. The NCSO.jar should reside in <your_domino_installation>\data\domino\java
- Restart the WebSphere Application Server:
- /opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<HostName>Node01Cell/aveksa.ear/aveksa.war/LotusNotesIdentityCollector1/lib/ (For Identity Collector)

- /opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<HostName>Node01Cell/aveksa.ear/aveksa.war/LotusNotesAccountCollector1/lib/ (For Account Collector)
- /opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<HostName>Node01Cell/aveksa.ear/aveksa.war/LotusNotesEntitlementCollector1/lib/ (For Entitlement Collector)
- Restart Server

WebLogic

Copy NCSO.jar files to following location and restart the server:

Location for aveksa.ear: /home/oracle/ACM-WebLogic

- Create a new folder: mkdir /tmp/aveksa.ear
- Unzip aveksa.ear to /home/oracle/ACM-WebLogic
  E.g. unzip -q -X /home/oracle/ACM-WebLogic/aveksa.ear -d /tmp/aveksa.ear
- Rename existing aveksa.ear file to aveksa.ear.old in /home/oracle/ACM-WebLogic/
  E.g. mv /home/oracle/ACM-WebLogic/aveksa.ear /home/oracle/ACM-WebLogic/aveksa.ear.old
- Copy NCSO.jar file to /tmp/aveksa.ear/aveksa.war/LotusNotesIdentityCollector1/lib/ (For Identity Collector)
- Copy NCSO.jar file to /tmp/aveksa.ear/aveksa.war/LotusNotesAccountCollector1/lib/ (For Account Collector)
- Copy NCSO.jar file to /tmp/aveksa.ear/aveksa.war/LotusNotesEntitlementCollector1/lib/ (For Entitlement Collector)
- Repackage aveksa.ear: Note you are creating the ear file in a new location /home/oracle/ACM-WebLogic
- cd /tmp/aveksa.ear
- zip -q -r -u /home/oracle/ACM-WebLogic/aveksa.ear *

Now deploy new ear file.

- Login to weblogic console:
  e.g http://<server_hostname>:7001/console
- Go to Deployment > Server
- Select aveksa.ear and click on Update button
- Select path /home/oracle/ACM-WebLogic and select aveksa.ear
- Click Next and then Finish it

Restart the WebLogic Server.

Without performing the above steps, the IBM Notes Collectors will fail with a "java.lang.NoClassDefFoundError" when they are run. However, other modules won't be affected if the NCSO.jar is absent.

Enable SSL for DIIOP on IBM Notes Server.

1. In the Server document, under the server's Domino Directory, go to the Ports tab -> Internet Ports tab -> DIIOP tab. Ensure that the SSL port number is correct and enabled. It defaults to 63149.
2. In the configuration of the Server document, go to Web -> Internet Sites -> Add Internet for the IIOP site and specify the kyr file (certificate file). Copy the certificate file to the RSA server machine.
3. In the Server tab of the server's Domino Directory, go to server tasks, and make sure that the DIIOP server task is present, which listens to the request on port 63149 and port 63148 (if non-SSL is enabled).

Note: Support for SSL is from Domino server versions 9.0.1 Fix Pack 5 and higher.

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	IBMNotes IDC
Description	IBMNotes Identity Data Collector
Data Source Type	IBMNotes
Agent	AveksaAgent
Business Source	Any Created Directory: e.g. IBM Notes Directory
Status	Active
Copy from	Select any existing IBMNotes IDC to copy configuration details

Scheduled	Default: No

Configuration Information

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

Field Name	**Value**
Domino Server Host	Host-Name or IP Address of machine running IBM Domino server
Domino Server DIIOP Port	Port on which DIIOP (Domino Internet Inter-ORB Protocol) service is listening. Default: 63148 (Non-SSL) and 63149 (SSL)
Administrator Hierarchical Name	Username of administrator e.g. CN=Dev Notes/O=AVEKSA ,where 'Dev Notes' is admin user with organization 'AVEKSA'
Administrator Password	Password of administrator user
Use SSL for DIIOP	Choose whether to use Secure Sockets Layer (SSL) to connect. If this is selected, RSA server uses the DIIOP SSL protocol to connect to the IBM Notes Domino server. If selected, you must provide the Keystore path and Keystore password.
Keystore Path	Enter the complete path of the Keystore file. For example, *C: \\workspace\\LotusNotesClient\\certs\\trust.jks*
Keystore Password	Enter the password for Keystore file specified in the Keystore Path field.
User Database	Name of the Notes directory database that contains user information. Default: names.nsf
User View	Name of the View within the directory database that contains entries for users to collect. Default: ($People)

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**
First Name	FirstName
Last Name	LastName
Email Address	MailAddress
User ID	ShortName

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	IBMNotes ADC
Description	IBMNotes Account Data Collector
Data Source Type	IBMNotes
Agent	AveksaAgent
Business Source	Any Created Directory: e.g. IBMNotes
Status	Active
Copy from	Select any existing IBMNotes ADC to copy configuration details
Scheduled	Default: No

Configuration Information

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

Field Name	Value
Domino Server Host	Host-Name or IP Address of machine running IBM Domino server
Domino Server DIIOP	Port on which DIIOP (Domino Internet Inter-ORB Protocol) service is listening. Default:

Port	63148>
Administrator Hierarchical Name	Username of administrator e.g. CN=Dev Notes/O=AVEKSA ,where 'Dev Notes' is admin user with organization 'AVEKSA'
Administrator Password	Password of administrator user
Use SSL for DIIOP	Select whether to use Secure Sockets Layer (SSL) to connect If this is selected, the RSA server uses the DIIOP SSL protocol to connect to the IBM Notes Domino server. If selected, you must provide the Keystore path and Keystore password.
Keystore Path	Enter the complete path of the Keystore file. For example: *C: \\workspace\\LotusNotesClient\\certs\\trust.jks*
Keystore Password	Enter the password for Keystore file specified in the Keystore Path field.
Account Database	Name of the Notes directory database that contains account information. Default: names.nsf
Account View	Name of the View within the directory database that contains entries for accounts to collect. Default: ($People)
Group Database	The name of the Notes directory database that contains group information. Default: names.nsf
Group View	The name of the View within the directory database that contains entries for groups to collect. Default: Groups

Map Collector Attributes to 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 Disabled	IS_DISABLED
Account Locked	IS_LOCKED

Map Collector Attributes to Account Mapping Attributes

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

Field Name	**Value**
User Reference	ShortName

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**
Owner	ListOwner

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	Associate an already created IDC; Default value is Users
User Attribute	By 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	Associate an already created 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	Associate an already created Account Data Collector
Group Attribute	Name

Edit Group Owner Resolution Rules

Note: This resolution wizard is enabled only on having group Owner configured on the *Map Collector Attributes to Group Attributes*

The following table lists the parameters on the “Edit Group Owner Resolution Rules” screen, while creating the collector.

Field Name	Value
Target Collector	Associate an already created IDC; Default value is Users
Group Attribute	First Name

Entitlement Data Collector

Set up Custom Attribute

You must create custom attributes that will collect these additional values from the IBM Notes databases into product.

To create a custom attribute, go to Admin > Attributes >Resource:

1. Click Edit.
2. Click Add Attribute.

Use the table below to configure the attributes for IBM Notes Entitlement Data Collector.

Resource Attribute	**Collector Attribute**
< Custom attribute created for Application Title >	Title
<Custom attribute created for ReplicaID>	ReplicaID

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	IBMNotes EDC
Description	IBMNotes Entitlement Data Collector
Data Source Type	IBMNotes
Agent	AveksaAgent
Business Source	Any Created Directory: e.g. IBMNotes

Status	Active
Copy from	Select any existing IBMNotes EDC to copy configuration details
Scheduled	Default: No

Configuration Information

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

Field Name	**Value**
Domino Server Host	Host-Name or IP Address of machine running IBM Domino server
Domino Server DIIOP Port	Port on which DIIOP (Domino Internet Inter-ORB Protocol) service is listening. Default: 63148
Administrator Hierarchical Name	User-name of administrator e.g. CN=Dev Notes/O=AVEKSA ,where 'Dev Notes' is admin user with organization 'AVEKSA'
Administrator Password	Password of administrator user
Use SSL for DIIOP	Select whether to use Secure Sockets Layer (SSL) to connect If this is selected, the RSA server uses the DIIOP SSL protocol to connect to the IBM Notes Domino server. If selected, you must provide the Keystore path and Keystore password.
Keystore Path	Enter the complete path of the Keystore file. For example: *C: \\workspace\\LotusNotesClient\\certs\\trust.jks*
Keystore Password	Enter the password for the Keystore file specified in the Keystore Path field.
Catalog Database	The name of the catalog database that contains entries to collect. Default: catalog.nsf

Catalog View	The name of the View within the catalog database that contains entries to collect. Default: Applications\by Title

Group Evaluation

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

Field Name	**Value**
Associated Collector	Associate an already created Account Data Collector
Group Value Evaluates to	Name

Account Evaluation

The following table lists the parameters on the “Account Evaluation” screen, while creating the collector.

Field Name	**Value**
Associated Account Collector	Associate an already created Account Data Collector
Account Value Evaluates to	Account Name

Copyrights

Trademarks