RSA Identity Management and Governance

Solutions Integration Guide

Collection and Governance of RSA Archer GRC Accounts, Groups and Roles

Contact Information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers: www.emc.com/domains/rsa/index.htm.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person. No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

December 2014

Contents

Introduction

This guide explains the export and collection of accounts, groups and roles from RSA Archer GRC into the RSA Identity Management and Governance Platform (RSA IMG) (formerly known as Aveksa). After collection, this information is available for Access Governance processes within RSA IMG – such as reporting, reviewing and requesting access.

This initial implementation leverages CSV extracts from the RSA Archer GRC environment collected into the RSA IMG environment. Downstream provisioning tasks (fulfillment) that are generated from the RSA IMG environment are currently manual, until an automated connection connector is developed in the future.

Supported Platform Versions

RSA Archer GRC:

- Version 5.5 SP2

RSA IMG (formerly known as Aveksa):

- Version 6.8.1 and later

Audience

The following is the target audience for this guide:

- **RSA Archer GRC Administrator** or appropriate user with application rights to perform the export of the RSA Archer GRC data (running the specific report).

- **RSA IMG Administrator** or appropriate user with application rights to copy the report results (.csv files) to the RSA IMG server and the rights to create and modify the “Archer” Account and Entitlement collectors.

This guide assumes that the administrators of the both RSA Archer GRC and RSA IMG fully understand their configurations and detailed steps for both running reports (on RSA Archer GRC) and configuring the collectors, reports, reviews, and so forth (on RSA IMG).

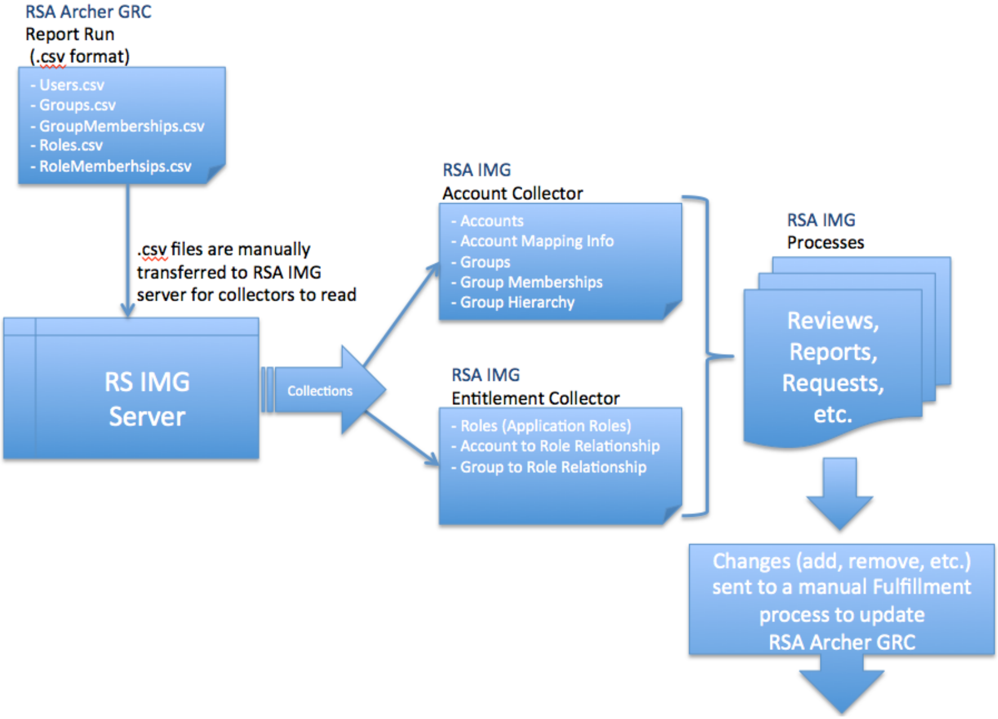
Collecting RSA Archer GRC Accounts, Groups and Roles into RSA IMG

Integrate the RSA Archer GRC and RSA IMG Systems

Overall Integration Flow

This is the overall data flow of this data collection process. This process entails some manual activities. Automated and direct data connections that will evolve over time and be released in future versions. The goal of this integration to provide a facility for obtaining data from the RSA Archer GRC platform and being able to collect that information into the RSA IMG platform for Governance purposes, such as Reporting, Access Reviews/Certifications and Access Requests.

This section outlines the high-level process and integration steps between the RSA Archer GRC and the RSA IMG platforms for exporting and importing accounts, groups and roles data.



The report process from RSA Archer GRC creates a set of CSV files (as a single ZIP file); this file is downloaded, extracted and transferred to the RSA IMG platform for the collectors to access. Once these files are collected, the information is available in the RSA IMG platform.

The resulting ZIP file contains the following CSV files:

- **Users.csv.** Contains the current set of RSA Archer GRC users and associated attribute information, which is imported as accounts into the RSA IMG platform.
- **Groups.csv**. Contains the current listing of groups and group metadata from RSA Archer GRC.
- **GroupMembership.csv**. Contains group membership and group hierarchy relationships from RSA Archer GRC.
- **Roles.csv**. Contains the current listing of application roles from RSA Archer GRC.
- **RoleMembership.csv**. Contains the current relationship of users and groups to RSA Archer GRC application roles.

The export process creates the CSV files, and then compresses them into a single ZIP file that you can download.

Important: You must ensure that you have proper permissions to export account data. You must also have set up your email address as the default email in your contact information to receive notification that the export process has completed successfully.

RSA Archer GRC Access Control Report - Extract Process

You must export the information from RSA Archer GRC as a set of CSV files that will be imported by the RSA IMG platform.

Export Account Access Control Data

Procedure

1. In RSA Archer GRC, go to the Access Control Reports page:
   a. Click Navigation Menu > Administrators > Access Control.
   b. Click View Access Control Reports.
2. Click Export Account Data.
3. Perform one of the following:
   a. Click OK to continue and complete the data extract.
   b. Click Cancel to cancel the export process.
4. Follow your process for downloading the report AccountDataExport.zip file. The zip file contains the following CSV files:
   - Groups.csv
   - GroupMemberships.csv
   - Roles.csv
   - RoleMemberships.csv
   - Users.csv

Extracting and Transferring Report CSV Files to the RSA IMG Platform

The extraction and transfer of the AccountDataExport.zip file is specific to each organization’s implementation. Extract and transfer the file to a location accessible by the RSA IMG platform. Most organizations have a CSV repository location that their current RSA IMG implementation utilizes.

RSA IMG Application and Collection Process

The Account and Entitlement Data collectors for the RSA Archer GRC information must be configured to collect from the RSA Archer GRC report CSV extracts. The actual implementation and configuration of the collectors varies from implementation to implementation.

Example collection queries are provided in the Data Export Structure and Sample Collector Queries section. You need to review the data in the CSV extracts and determine if any specific or additional information is required for the collection mapping processes in your environment.

You need to review and potentially modify the example queries to match your organizational and data requirements. The person configuring the collectors must have a solid understanding of the deployment requirements and associated deployment data model (for accounts, groups and entitlements) for configuring these collectors.

RSA Archer GRC Application Scope

The RSA IMG Platform must have a Business Source to represent the information collected from the RSA Archer GRC platform; this is typically an Application that is named RSA Archer GRC.

See the *RSA IMG Administrator’s Guide* for more information on creating and setting up an Application.

Account Data Collector (ADC)

The “RSA Archer GRC” Account Data collector (in RSA IMG) will be collecting accounts, account mappings, groups and group membership/hierarchy (sub-groups).

The collector must be configured to collect the data (including data for any custom attributes) based on the deployment requirements.

See the *RSA IMG Administrator’s Guide* for more information on creating and setting up an Account Data Collector.

Entitlement Data Collector (EDC)

Once the RSA Archer GRC data is collected into the RSA IMG Platform, it is available for access review/certification and for setting up the access request processes

See the *RSA IMG Administrator’s Guide* for information on creating and setting up an Entitlement Data Collector.

Data Export Structure and Sample Collector Queries

RSA Archer GRC Data Export Elements

The tables in this section outline the attributes that are contained in the RSA Archer GRC Access Report.

All the information that is exported from RSA Archer GRC may not have a corresponding RSA IMG attribute for import. As each implementation is different and may already have custom attributes defined, review the structure and data included in the exports and complete one of the following options:

Map RSA Archer GRC export data attribute to existing OOTB attribute or existing custom attribute schema in the associated collector or collectors (Account or Entitlement).

Add additional Account / Group / Role custom attribute to collect respective RSA Archer GRC data element / attribute in the associated collector or collectors (Account or Entitlement).

Do not import or leverage the data element / attribute from the RSA Archer GRC export files.

Users.csv

Attribute	OOTB IMG Acct Attribute Mapping Suggestion	Comments
UserId	Account ID/Name	
FirstName		
LastName		
UserName		
UserDomain		
LastUpdated		Presented in Zulu time
Address		
Company		
Title		
DefaultEmail		
DefaultEmailType		
Email2		
Email2Type		
Email3		
Email3Type		
Email4		
Email4Type		
Email5		
Email5Type		
Phone1		

Attribute	OOTB IMG Acct Attribute Mapping Suggestion	Comments
Phone1Type		
Phone2		
Phone2Type		
Phone3		
Phone3Type		
Phone4		
Phone4Type		
Phone5		
Phone5Type		
AccountStatus		
LastLoginDate	Last Login	Zulu time
ForcePasswordChange		

Groups.csv

Attribute	OOTB IMG Group Attribute Mapping Suggesion	Comments
GroupId		
Name	Group ID/Name	
DisplayName		
Description		
LastUpdated		Presented in Zulu time
LdapDistinguishedName		

GroupMemberships.csv

Attribute		Comments
GroupId		
UserId		
ParentGroupId		

Roles.csv

Attribute	OOTB IMG Application Role Attribute Mapping Suggestion	
RoleId		
Name	Application Role ID/Name	
Alias		
Description		
LastUpdated		Zulu time
AssignByDefault		

RoleMemberships.csv

Attribute		Comments
RoleId		
GroupId		
UserId		

Sample Collection Queries

This section includes sample SQL queries that you can use in the configuration of the associated Account and Entitlement data collectors (ADC & EDCs). Each deployment may be different based on the current RSA IMG implementation, integration and business requirements. Configuration of the collector will be according to the current implementation requirements.

There are some data elements/attributes that map to existing OOTB attributes and potentially custom attributes that have already been defined in the current implementation. There may also be cases where data is needed from the RSA Archer GRC Platform but no attribute exists (either OOTB or a currently defined custom attribute). In these cases you must create a custom attribute and update the query/collector to appropriately collect and populate the information.

These collector queries are provided as a framework to collect and import this information into the RSA IMG Platform. Review the configuration of the collectors and modify the configuration according to implementation and business requirements.

Basic RSA IMG Collector Connection Information

Put the CSV files contained in zip file extract in the /home/oracle/ftp/archer path to align with the configuration URL of the ADC & EDC collectors, or an appropriate location based on your implementation architecture. If the location of the files is different, update the collector URL accordingly.

Note: For the JDBC URL for the CSV database (HXTT) driver the following two parameters are needed for the collection of these files:

_CSV_Header=true : as the CSV files contain a header row

_CSV_Quoter=” : as the CSV files have fields surrounded by quotes. This is important as some of the data (i.e.: descriptions) may contain line breaks

For example:

Attribute	Setting
DB Type	CSV
Driver Class	com.hxtt.sql.TextDriver
URL	jdbc:csv:////home/oracle/ftp/archer/?_CSV_Header=true;_CSV_Quoter=";tmpdir=/tmp

Accounts Data Query

```
select distinct
 UserID,
 FirstName || ' ' || LastName as AccountFullName,
 UserName as DomainAccount,
 UserDomain,
 Title,
 (case
   when (DefaultEmailType = 'Business') then DefaultEmail
   when (Email2Type = 'Business') then Email2
   when (Email3Type = 'Business') then Email3
   when (Email4Type = 'Business') then Email4
   when (Email5Type = 'Business') then Email5
  end ) BusinessEMail,
(case
   when (Phone1Type = 'Business') then Phone1
   when (Phone2Type = 'Business') then Phone2
   when (Phone3Type = 'Business') then Phone3
   when (Phone4Type = 'Business') then Phone4
   when (Phone5Type = 'Business') then Phone5
  end ) BusinessPhone,
 AccountStatus,
 date_add(left(lastlogindate, len(lastlogindate) -1), interval
-5 hour) as ESTLastLogin
from users
```

Note: Review this query and modify it for your implementation based on the data elements you chose to collect for the accounts and any data desired to collect into custom attributes.

The Date values exported from RSA Archer GRC are represented in Zulu time; the implementation and desired time zone offset may be different for each implementation and the query should be adjusted accordingly. The query above removes the Z from the timestamp and then sets the time to EST.

The Email and Phone values collected look for those that are marked as Business from within RSA Archer GRC; the users from within RSA Archer GRC may choose to associate the Type for any of the values.

User Account Mappings Data Query

```
select distinct
 UserName as DomainAccount,
 UserName as UserMapping
from users
```

Note: Review this query and modify it based on the deployment requirements for account to user mapping.

Group Data Query

```
select distinct
 Name as Group,
 DisplayName
from groups
```

Account Membership Query

```
select distinct
 grpmem.GroupId,
 grp.Name as Group,
 grpmem.UserId,
 accts.UserName as DomainAccount
from GroupMemberships grpmem
 left join Groups grp
  on grpmem.GroupId = grp.GroupId
 left join Users accts
  on grpmem.UserId = accts.UserId
```

Subgroup Membership Query

```
select distinct
 GroupID as subgroupId,
 groups.Name as SubGrpName,
 ParentGroupId as parentId,
 parentGroups.Name as Group
from GroupMemberships gh
  left join Groups
  on gh.GroupId = Groups.GroupId
  left join Groups ParentGroups
  on gh.ParentGroupId = ParentGroups.GroupId
where ParentId is not null
```

Application Role Query

```
select distinct
 RoleId,
 Name as AppRole
from Roles
```

Application Roles for Groups Query

```
select distinct
 rm.roleid,
 rm.groupid,
 roles.name as AppRole,
 Groups.name as Account
from RoleMemberships rm
 left join Roles
  on rm.roleID = roles.roleID
 left join Groups
  on rm.GroupID = Groups.GroupID
 where rm.groupid is not null
```

Application Roles for Accounts Query

```
select distinct
 rm.roleid,
 rm.userid,
 roles.name as AppRole,
 users.username as Account
from RoleMemberships rm
 left join Roles
  on rm.roleID = roles.roleID
 left join Users
  on rm.UserID = Users.UserID
 where rm.userid is not null
```