RSA Professional Services

RSA Identity Governance and Lifecycle

Deployment Recommend Practices
Upgrade & Migration for 7.1.1

Version: 1.0
Issue Date: April 16, 2019

Table of Contents

Revision History

Rev:	Date:	Author(s):	Description
1.0	April 16, 2019	Paul Soczka	Initial Create

RSA G&L Acronyms and Terminology

Please refer to the below list of acronyms which are used widely within the RSA teams.

Abbreviation	Term	Description
G&L / IGL	RSA Identity Governance and Lifecycle	RSA Identity Governance and Lifecycle Product
ACL	Access Control List	Data source containing all account and entitlement details
A&D	Architecture and Design	Term used when defining and outlining the summary and implementation of RSA G&L.
AD	Active Directory	Application used to manage users. Often used to collect identities from and to authenticate users.
ACM	Access Certification Manager	The reviews module. This module must be enabled in order to see the reviews menu. Note: In the past it denoted Aveksa Compliance Manager – the old name for the platform.
AFX	Automated Fulfillment Express	Add-on module that uses XML messaging to fulfill changes at their source.
ARM	Access Request Manager	Add-on module used to enable a self-service portal. Allows users to request access changes for themselves and/or other users.
BOE	Basis of Estimate	Costing for delivery of a project broken down by job type e.g. architect, deliver or consultant
BRM	Business Role Manager	Add-on module used to enable roles-based access controls.
DAG	Data Access Governance	Add-on module used to collect report on, and review unstructured data.
DSE	Dedicated Support Engineer	An individual assigned to a project to provide enhanced support
FF	Fixed Fee	Contract term where the amount of payment does not depend on the amount of resources or time expended.
IAM	Identity and Access Management	The larger umbrella of RSA products which RSA G&L is a member along with members of the Access Platform.
JML	Joiners – Movers – Leavers	Term used to describe when people join a company, change jobs within a company, or leave a company.
LOE	Level Of Estimate	Initial estimation for delivery time per project
MAL	MyAccessLive	Hosted version of RSA G&L platform
PCF	Project Completion Form	Required by RSA to acknowledge completion of a Milestone or the project entirely.
PM	Project Manager	RSA G&L Project Manager
POC	Proof of Concept	A demonstration in principle with the purpose to verify that a concept or theory has the potential of being used.
PS	Professional Services	RSA Professional Services team
RBAC	Role Based Access Control	Defines access to source entitlements via roles
SoD	Segregation of Duties	Term used to describe two sets of entitlements that a single user should never have together a.k.a Separation of Duties
SCOL	Secure Care Online	Online secure portal providing access to a support knowledgebase, current platform patches, bug fixes, to sign up for notifications, your support cases and more.
SOW	Statement of Work	A formal document that defines the activities, deliverables, and timeline a vendor must execute in performance of specified work for a client.
SSM	Solution Success Manager	The RSA Solution Success Manager - formally a Solution Principle (SP)
T&M	Time & Materials	Contract term where the client agrees to pay the contractor based upon the time and resources expended.
XML	Extensible Markup Language	Used to define a data structure

RSA Identity G&L Community

Use the RSA G&L Community to ask questions, interact with your peers, suggest ideas and find out about new releases. The community is 100% free to use for our clients and we strongly recommend you join today!

Whether you are a brand-new customer of RSA G&L, or have been using the product for years, we believe that you'll find this private community to be very valuable. The RSA G&L Community is a private community and is only available to RSA G&L clients, partners and internal RSA staff.

RSA Community: https://community.rsa.com/
More information about RSA Link can be found here: https://community.rsa.com/docs/DOC-58573

Direct link to the RSA IGL Community Link:
https://community.rsa.com/community/products/governance-and-lifecycle

COMMUNITY ACCESS PROCEDURE:

1. Community Homepage: https://community.rsa.com/

2. Register an account on the RSA Community: https://community.rsa.com/register

Once you have registered, your customer ID will give you access to all the private (client only) areas of RSA Link community.

OTHER USEFUL RSA IGL LINK COMMUNITIES:

- Client and partner community: click here
- RSA IGL Ideas, for enhancement requests and suggestions: click here
- RSA IGL Recommended Practices: click here
- RSA IGL Blueprints: click here
- RSA IGL Connector and Collector guides: click here
- RSA IGL University: click here

Global RSA G&L Contact Mailbox

If you have any questions, please contact the following mailbox:

rsa.identity.ps.global.mailbox@rsa.com

1. INTRODUCTION

1.1. Document Scope

This document has been created to provide the recommended practices **when upgrading from RSA IGL 7.0 to 7.1/7.1.1** by completing following activities:

- Pre-Migration reports
  - Analysis of results
  - Identifying issues
  - Resolving 7.1.x migration items
- Database Backup
- Database Restore
- Upgrades
- Migrations

The aim of this document is to get very prescriptive around how to perform an upgrade and be successful on the RSA Identity Governance and Lifecycle (RSA Identity G&L) journey to v7.1.x. RSA wants to share this with partners and customers as well, so we are all doing the same thing.

One of the goals is to ensure that customer/partner resources are fixing and resolving all items (ex: custom work), to mitigate issues downstream when moving from v7->v8. Removal of "custom" work is a top priority and getting to do more things "out-of-the-box" (OOTB) is a must.

1.2. Intended Audience

This guide has been created for both clients and partners.

2. EXECUTIVE SUMMARY

Managing your environment should always follow industry standard practices, along with your internal company policies on this matter. RSA Provides detailed guides found on RSA link (https://community.rsa.com/) around all topics covered here and this document should be used as a supplementary source of information to these standards and will help as a guiding framework when using the RSA Identity G&L product.

The notes in this guide should always be carefully followed and if any further assistance is needed, please seek help on the community or from the RSA Professional Services Team, who can fully assist with all these tasks and have paid offerings (SKUs) to deliver on everything documented here, if you do not wish to complete this on your own.

RSA is here to help if required and we have specific SKU'ed offering for upgrade and migration planning. RSA PS can analyze the existing version and produce not only recommendations for upgrade, but also provide you with recommendations on changing any WF/ARM/AFX/BRM if need be. RSA PS is also here to offer assistance if you wish to change your overall architecture. For example:

- Moving from appliances to your own infrastructure (WebLogic/WebSphere)
- Moving to a remote DB
- Moving to a separate AFX server
- Clustering for load balancing

3. REFERENCE DOCUMENTS

Please always refer to the product guides found in the official documentation for complete details, as posted to the RSA Link community.

1. Browse to: https://community.rsa.com/
2. Select your application (Products/application)
3. Select the "Documentation" link
4. Pick your product version for RSA Identity Governance and Lifecycle
5. Download all available documents for your product version
6. Please carefully read below documents of version to upgrade to:
    - Release Notes for all major versions between source and target version
    - Platform Support Matrix
    - Install Guide
    - Upgrade and Migration Guide
    - Appliance Updater Guide
    - Database Setup and Management Guide

4. NOTES AND ADVISORIES

Various items to take note of before using this guide:

- RSA Identity G&L Versions used in this guide are version 7.0.x to v7.1.x.
- This document covers the details of the approaches where RSA Identity G&L application on a server is upgraded to latest version.
- This guide should be used to deploy a solution in a Development environment first and fully tested out before migrating to any other environments.
- Please seek help from the RSA Community or RSA directly if you are unsure.

5. PLANNING THE UPGRADE

This section briefs the considerations to be made while choosing the appropriate approach for upgrade and information on where to look for relevant documentation.

5.1. Why should you upgrade?

Upgrading to the latest version and patch is always recommended, as it includes latest fixes/ features currently available in the product. Apart from giving the benefit of newly introduced or improved features, this also can save you a lot of time in the future, as potential issues you might face, could always be fixed in a newer version.

5.2. Upgrade basics

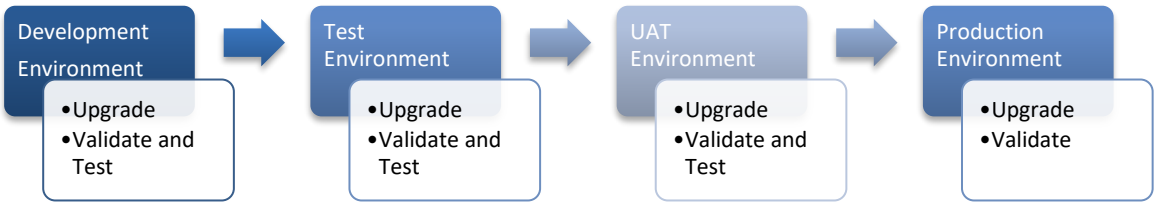
Choose target product version

Decide the product version you will upgrade to. Refer to the release notes of version you are planning to upgrade to, as well as release notes of all intermediate base versions to understand what is new in that release, what are fixed issues, what are known issues. This helps to identify if your environment is ready to be upgraded to new version.

Applying latest patch after completing the upgrade is always recommended, as it includes latest fixes/ features currently available in the product.

Phased approach

Each of the lower (Non-Production) environments must be upgraded and validated following the recommended approach before beginning upgrade of Production environment.



6. PRE-UPGRADE ACTIVITES

6.1. Pre-Migration Reports

RSA provides a migration utility which enables you to generate reports that list issues with your current configuration and provide guidance on how to resolve those issues. You must use the migration utility to assess the impact to your system and, if necessary, modify collectors and data before you perform an upgrade. Although this is a must for upgrades from pre 7.0 versions, these can be used for any other upgrades.

The tools you need to identify issues with your installation are available in the Migration Report Utility file (MigrationReports.zip), which contains the following files:

- generateMigrationReport.sh is a shell script that creates a full migration report similar to an ASR report.
- insertMigrationReportDefinitions.sh is a shell script that creates tabular report definitions for each report listed in the table in "Migration Reports."
- insertMigrationReportDefinitions.sql is an SQL script used by the shell script for creating the tabular report definitions for the individual reports.
- Pre_Migration_Pkg.pkb is a database package that is used by the full migration report

6.2. Verify Prerequisites

Verify that your current environment satisfies the prerequisites for your install type which are listed below and perform necessary changes to meet those. This includes verifying sizing and architecture, as when you upgrade to a new version you might need to increase and change various settings, such as CPU. The product documentation clearly states the recommended configuration settings which should be applied, so a comparison should be done before you start.

Verify system prerequisites:

Please refer to Platform Support Matrix, "**Installation Prerequisites" / "Upgrade Prerequisites**" section of Install Guide, Upgrade and Migration guide of the corresponding version to get details of these.

- Verify Prerequisites for an RSA Appliance
- Verify Prerequisites for a Soft-Appliance Installation
- Verify Prerequisites for WebSphere
- Verify Prerequisites for WebLogic

Verify database prerequisites:

This step is applicable for Soft-Appliance installs with remote database and for WebLogic/WebSphere installs where you use a customer-supplied (remote) database. Verify Prerequisites for Customer Supplied Database as per Database Setup and Management guide

6.3. Prepare validation checklist

Prepare the checklist of items specific to your environment which need to be validated post upgrade. These validations and tests can be run in development environment to make sure use cases are working fine post upgrade.

Refer to release notes of version you are planning to upgrade and any intermediate base versions to understand what is new, what are fixed issues, what are known issues and prepare a list of configurations which may get affected with upgrade. Post-upgrade validation checklist must cover validation those.

Along with these, include tests related to below configurations in validation checklist.

- Identity collectors and unification (important due to collection changes introduced in v7.x and if any custom post processors are in scope)
- Other collectors (important due to collection changes introduced in v7.x and if any custom post processors are in scope)
- Authentication sources
- User interface changes (important if any custom logo, customer strings file, dash board images are in scope)
- Role data collectors if applicable (important due to collection changes introduced in v7.x)
- Change request generation
- Approval and Fulfillment workflow processing (consider workflows with any custom java nodes)
- AFX connectors
- Custom Reports
- Review generation
- Scheduled jobs such as scripts configured in crontab
- Other custom changes

6.4. Identify custom changes present

Apart from the changes in latest product versions that may affect the migration, there might be other custom configurations specific to the environment which will need to be updated or re-applied post migration.

1. Any "custom" work that has been completed outside of the UI will not be exported and will be over-written during an upgrade. These items and the process behind them must be documented and saved, so that they can be re-applied once the upgrade is completed.
   Custom work also includes any database changes such as post processors, tables, indexes, functions, views which are not part of standard product schema and were created explicitly for custom requirements.

   You may use the attached sheet to list down all the custom changes in scope at your environment. Please refer to Appendix II for more details on how to identify and backup such customizations.

Pre- Upgrade Custom Changes Check List		
Possible custom changes to be documented or saved before upgrade	**Is applicable (Y/N)**	**Details such as file names**
Save copy of coverage file and/or alternate manager file		
Save copy of custom images		
Save copy of custom dashboard Images		
Save copy of custom JSP pages		
Save copy of custom customer strings file		
Save copy of custom security files		
Save copy of custom connector templates required		
Save copy of required collector, connector or other external JARs		
Save copy of Java node related files - .Jar, .Class, .Properties etc.		
Save copy of custom Plug-in related files		
Save copy of custom scripts used		
Save copy of custom AFX connector related files		
Save copy of custom AFX connector template		
Document custom post-processor changes in scope		
Document custom functions, views, tables, indexes in scope		
Document custom cron tab changes in scope		
Document AFX suffix mapping file		
Document Remote AFX Agent related changes in scope		
Document any other custom changes		

6.5. Download required product software

Below are the steps to download required product software:

1. Login to: https://community.rsa.com/
2. Select RSA Identity Governance and Lifecycle.
3. Click Downloads > RSA Identity Governance and Lifecycle <Target Version>.
4. Click on Additional Downloads.
5. Click Access Certification Manager.
6. Click Download Software (it may take a minute to display the Product List).
7. Click RSA Identity Governance and Lifecycle (formerly Aveksa) - Version Upgrades.
8. The Current tab lists the most recent release. The Archive tab lists previous releases.
9. Download the installers for the required version.
10. Download the AFX connector templates of version if AFX is in scope
11. Copy the Downloaded Installation Files to the Installation Host

Please refer to Product Upgrade and Migration Guide for details of files to be downloaded and steps to copy the downloaded installation files to the installation host.

6.6. Setup other required software

The following software are required for us to deploy, install and configure RSA Identity G&L within your environment and so is required on any computers being used by the team both internally and externally.

Please review the below list of software to ensure installation of these will not breach any company policies. This access is required for all onsite RSA consultants and internal RSA G&L team using the product. A suitable alternative solution will need to be agreed if the below cannot be installed.

Software	Use
Putty	Open source terminal emulator supporting SCP, SSH, Telnet and raw socket connection.
FTP Client (e.g. FileZilla or WinSCP)	Cross-platform FTP application, used to transfer RSA G&L installation files from local to remote machine.
Query Analyser (Squirrel SQL Client, Toad, SQL Developer)	SQL database administration tool used to write and test SQL before applying to RSA G&L
SOAP UI	Required if any web service development is needed.
Firefox/Chrome	A second browser allows 2 concurrent sessions and is useful for testing purposes
Microsoft Office	Required for creating documentation – run books, presentations, etc.
LDAP Browser (e.g. Apache Directory Studio)	Used as an Active Directory browser

6.7. Plan the Schedule and Prepare communication plan

Plan the estimated start and end date and time of upgrade process. Consider the existing schedules of collectors and rules while deciding the start time. System will not be available to process the requests and other scheduled jobs during the upgrade process.

Prepare the communication plan on who must be notified during upgrade. It is recommended to include both IT Team and business team who are affected by this upgrade and downtime of the service.

Communicate the planned downtime details to the monitoring team, if the server is being monitored by any tool which may trigger incidents during downtime.

You may use below attached document as checklist of high level activities during upgrade.

Upgrade Checklist.docx

7. UPGRADE APPROACHES

There are three approaches for upgrade:

1. **In-place upgrade**: Upgrade existing environment and migrate database
2. **Database export/import**: Export/Import database into a fresh environment
3. **Config-only metadata exports**: Perform a migration of the configuration only

7.1. In-Place Upgrade

This section is about how you upgrade your current environment itself to new version of RSA Identity G&L on a second server and migrate all data.

It is critical to refer to the Product Upgrade and Installation guides specific for the target version being upgraded to for current information.

Advantages:

1. Both Data and Configuration of the existing environment(s) is retained post-upgrade.
2. No additional server / environments are required as upgrade being performed on same environment, assuming the source environment matches current product version server requirements.
3. Oracle version will be automatically upgraded to the target release version through the appliance updater (as needed).
4. WildFly version will be automatically upgraded to the target release version through the appliance updater (as needed).
5. This approach can be used in conjunction with the new Archiving capabilities to reduce the size of the database.

Drawbacks:

1. Performing database migration will also bring in any existing data issues from old database and may affect data integrity in new environment as well.
2. Importing database will increase size of the initial database in the new 7.x environment while part of existing data might be unwanted deleted or unreferenced objects.

   The SQL queries below can be utilized to identify counts of Objects (deleted vs non-deleted), count of deleted unreferenced groups, deleted unreferenced entitlements, deleted unreferenced app-roles, deleted unreferenced resources, deleted unreferenced roles, deleted unreferenced accounts. This information can be useful to identify the amount of data which need not to be carried forward to new environment post upgrade.

3. Product customizations existing in current solution will be brought forward automatically unless identified in the pre-migration activities and remediated. Unresolved product Customizations may break in current version of the product.
4. If the current environment is undersized based on current product requirements, the existing servers will need to be re-sized accordingly prior to performing a product upgrade.
5. WebSphere Only: minimum product version has been updated to v8.5.5.9.
6. This approach requires downtime during upgrade.

7.2. Database export/import

This section is about how you install new version of RSA Identity G&L on a second server and migrate all your data to this new version.

Advantage:

1. Both Data and Configurations of existing environment is retained and will be accessible from new environment.
2. New target environment(s) can be re-sized to meet current customer and product needs and current version of IGL deployed with latest patches.
3. No production down-time. Once the new environment is online and tested, DNS entries can be re-pointed to the new environment
4. Legacy (current) environment can remain online for:
    a. Fall back purposes
    b. Legacy audit needs prior to go-live

Drawbacks:

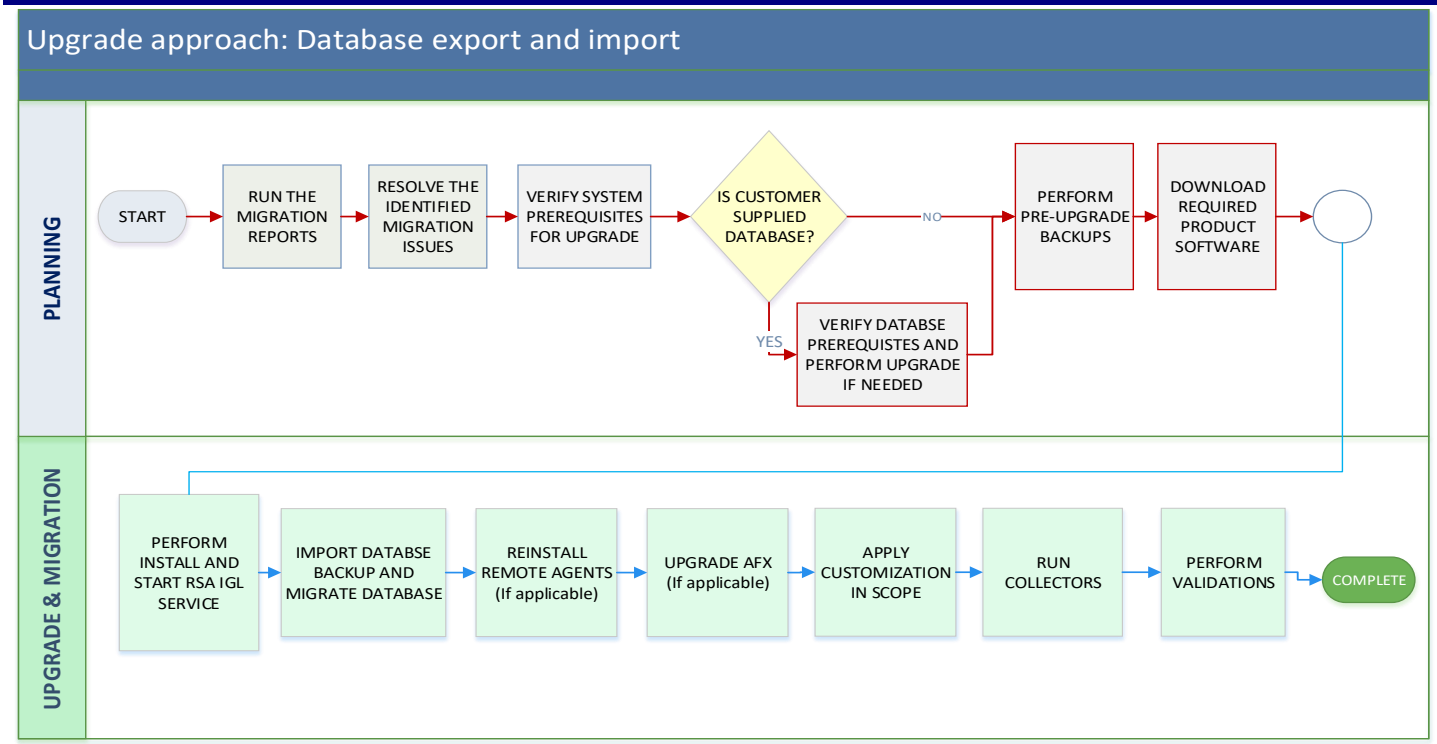
1. Performing database migration will also bring in any existing data issues from old database and may affect data integrity in new environment as well.
2. Importing database will increase size of the initial database in the new 7.x environment while part of the existing data might be unwanted deleted or unreferenced objects.

    Below SQL queries can be utilized to identify counts of Objects (deleted vs non-deleted), count of deleted unreferenced groups, deleted unreferenced entitlements, deleted unreferenced app-roles, deleted unreferenced resources, deleted unreferenced roles, deleted unreferenced accounts. This information can be useful to identify the amount of data which need not to be carried forward to new environment post upgrade.

3. This approach requires an additional (Secondary) environment to be available for performing upgrade.
4. Product DB customizations existing in current solution will be brought forward automatically unless identified in the pre-migration activities and remediated. Unresolved product Customizations may break in current version of the product.
5. WebSphere Only: minimum product version has been updated to v8.5.5.9.

Any changes required to make the application (which is now hosted on new server) accessible by users must be performed post upgrade.

Old environment must be considered as Read-Only and no additional changes must be allowed to be performed on old environment as databases will not be synchronized post upgrade and migration


Upgrade approach: Database export and import
PLANNING
START
RUN THE MIGRATION REPORTS
RESOLVE THE IDENTIFIED MIGRATION ISSUES
VERIFY SYSTEM PREREQUISITES FOR UPGRADE
IS CUSTOMER SUPPLIED DATABASE?
NO
YES
VERIFY DATABSE PREREQUISTES AND PERFORM UPGRADE IF NEEDED
PERFORM PRE-UPGRADE BACKUPS
DOWNLOAD REQUIRED PRODUCT SOFTWARE
UPGRADE & MIGRATION
PERFORM INSTALL AND START RSA IGL SERVICE
IMPORT DATABSE BACKUP AND MIGRATE DATABASE
REINSTALL REMOTE AGENTS (If applicable)
UPGRADE AFX (If applicable)
APPLY CUSTOMIZATION IN SCOPE
RUN COLLECTORS
PERFORM VALIDATIONS
COMPLETE

7.3. Config-only Metadata Exports

This section is about how you install new version of RSA Identity G&L on a second server and import all your configurations to this new version.

Advantages:

1. Performing a config-only upgrade helps in better data integrity in the new environment as any known data issues are not carried forward from old database.
2. This also results in improved performance as size of the initial database in the new 7.x environment will be considerably reduced.

   Below SQL queries can be utilized to identify counts of Objects (deleted vs non-deleted) and count of deleted unreferenced groups, deleted unreferenced entitlements, deleted unreferenced app-roles, deleted unreferenced resources, deleted unreferenced roles and deleted unreferenced accounts. This information can be useful to identify the amount of data which need not to be carried forward to new environment post upgrade.

3. Historical audit data on the (now) deprecated source system can be archived and will be available for any audit data retrieval for as long as archive is maintained.

Drawbacks:

1. Since only configuration items are carried forward into the new (upgraded) environment, certain data elements are not carried forward (as of 7.1.1):
   a. Local Entitlements
   b. Manually Mapped Account associations
   c. Challenge / Response questions and answer pairs
2. As of 7.1.1, changes have been made to improve external WebService calls into RSA IGL security. Tokens must now be used (vs. IP white listing only) for many of the WebService Calls today. This is a change from 7.1, and prior, versions of IGL where IP white listing was needed only and may have a down-stream impact to external processes which leverage these and may need to be updated to include the additional calls to get, and use, WebService tokens.
   a. has impact on JSP pages
   b. has an impact on JAR's
   c. has an impact on Driver's
   d. has an impact on images/security context files

Process:

RSA Identity G&L MetaData exports are for a specific product version, and for the same product version only. To avoid any compatibility issues, we must setup system of same version before generating export of metadata for version to upgrade to.

To achieve this, MetaData exports will need to be first imported into an environment (Temporary Destination Server) where the patch level of the Temporary Destination Server is the same as the source system. Once imported, the Temporary Destination Server can then be safely upgraded/patched to the desired 7.x version of G&L. After this process has completed, the Temporary Destination Server can then be used as the 7.x solution going forward, or the now upgraded 7.x metadata can be exported and imported to the final target destination server, configuration can be verified and collections can be re-run to re-build the data model to be current.

Any changes required to make the application (which is now hosted on new server) accessible by users must be performed post upgrade.

Old environment must be considered as Read-Only and no additional changes must be allowed to be performed on old environment as databases will not be synchronized post upgrade and migration.

Data availability

- Historical data for below will not be available post upgrade from new environment.
  But these can be maintained as part of archive database and limited access can be granted for audit and administrator purposes.
  - Change request history
  - Review history
  - Data run history
  - Workflow history
  - Historical Violations
  - Exceptions
- User data will be collected during first collection post upgrade as per availability in identity source.
  In case of certain identity sources, source such as feed file only contains active user data, hence running configured IDCs will only collect active user data.
  In order to retain information of terminated users (with Is_Deleted=1), who were identified as terminated in previous runs, after upgrade we need to first collect such users as one time activity.
  This will collect such deleted and hence terminated users as terminated users in target environment on first unification. This temporary IDC will be deleted and these users will be identified as deleted on subsequent unification runs.
- Account, App-Role, Entitlement, Role data will be collected during first collection post upgrade.
- Applicable violations will reappear on SoD rule processing in target environment. But exception details will need to be documented and backed up from source environment prior to upgrade and reapplied post upgrade.
- Existing open reviews or change requests can be allowed to continue on old environment and close per their configured schedules. Any new ones, needing to be opened after the go-live date of the new 7.x solution will be generated on the new system.

Alternatively, a Database Export/Import migration approach may be done first into the target 7.1.1 environment. This will upgrade both data and configurations to the latest version of RSA IGL. From there, metadata export/import approach can then be leveraged. This approach is useful when an intermediate environment is not available within a customers environment.

APPENDIX

I. Upgrade activities checklist

You may use below attached document as checklist of activities during upgrade.

Upgrade Checklist.docx

II. Customization backup and restore steps

You may use below attached document as reference while performing backup and restoration of customizations.

RSA Identity GL - Customization Back up

III. Deleted Users IDC creation steps and considerations

User data will be collected during first collection post upgrade as per availability in identity source.
In case of certain identity sources, source such as feed file only contains active user data, hence running configured IDCs will only collect active user data.

In order to retain information of terminated users (with Is_Deleted=1), who were identified as terminated in previous runs, after upgrade we need to first collect such users as one time activity using a Deleted Users IDC.
This step is important to retain any account-user mappings for such users which otherwise result in orphans and also to identify rehires.
This IDC will collect such deleted and hence terminated users from source environment as terminated users in target environment on first unification. This temporary IDC can then be deleted and these users will be identified as deleted on subsequent unification runs.

Steps to create and run Deleted users IDC:

1. Create Directory named 'Deleted users'
2. Create IDC under 'Deleted users' directory with below query.
   You may create Database type of collector pointing to source environment's database or export the query results as csv and collect from csv.
   Please make sure to perform activity this immediately before running other configured IDCs so that data being collected is accurate.
   User Data Query:
   select user_id,unique_id,first_name,last_name,email_address,department,termination_date, 1 as is_terminated,column1,columnN from pv_users where is_terminated='True' and deletion_date is not null
   Here replace column1,column with any other additional column details to be collected as per your environment's user attributes
3. Map above fields with corresponding user attributes
4. Navigate to Unification configuration > Participating collectors > Deleted User Temp IDC is set with 'Yes' for 'Create Users'.
5. Run this collector and unification.

6. Verify the applicable users are collected as terminated users with appropriate termination date as in source environment.
7. Inactivate and delete this collector.

Important Notes:

1. 'Termination Date' will be same on both source and target environments for these users
2. 'First seen on' date for these users will be the date when the Deleted Users IDC was run and will not be same as 'First seen on' date on source environment.
3. 'Deletion Date' on target environment will be the date when unification was run after the above IDC was deleted. So 'Deletion Date' will not be same on both source and target environments.
4. We are collecting these users under a new directory 'Deleted users' and hence user's directory in source environment and target environment will be different.

--- END OF DOCUMENT ---