

**RSA Identity Governance and Lifecycle
Upgrade and Migration Guide
V7.0.1**



Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

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

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.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the RSA Identity Governance and Lifecycle product and selecting the About menu.

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.

Copyright © 2016 EMC Corporation. All Rights Reserved. Published in the USA.

November 2016

Contents

| | |
|---|-----------|
| Preface | 5 |
| About This Guide | 5 |
| Documentation Set | 5 |
| Support and Service | 5 |
| Chapter 1: Supported Upgrade Scenarios | 6 |
| Chapter 2: Pre-Upgrade Tasks for Migrating Collectors | 7 |
| Changes to Data Collections | 7 |
| About Full Refresh Collections after Migration | 7 |
| Migration Reports | 8 |
| The Migration Report Utility | 10 |
| Download the Migration Report Utility | 10 |
| Install the Migration Reports | 11 |
| Run the Full Migration Report | 13 |
| Run an Individual Migration Report | 14 |
| Chapter 3: Verify Upgrade Prerequisites | 15 |
| Review Public Database Schema and Port Changes Introduced in v7.0.1 | 15 |
| Verify Prerequisites for an RSA Appliance | 16 |
| Verify Prerequisites for a Soft-Appliance Upgrade | 17 |
| Verify Prerequisites for Upgrading on WebSphere | 19 |
| Verify Prerequisites for Upgrading on WebLogic | 20 |
| Additional Prerequisites for WebLogic and WebSphere Application Servers | 21 |
| Chapter 4: Prepare to Upgrade the RSA Identity Governance and Lifecycle Software | 22 |
| Back up the RSA Identity Governance and Lifecycle Application (Appliance and Soft-Appliance Only) | 22 |
| Apply the Latest Operating System and Database Patch Updates | 23 |
| Back Up the RSA-Supplied Database | 24 |
| Back Up the Customer-Supplied Database | 25 |
| Prepare for an Upgrade on WebLogic | 25 |
| Prepare for an Upgrade on WebSphere | 26 |
| Chapter 5: Perform the Upgrade | 27 |
| Upgrade RSA Identity Governance and Lifecycle on an Appliance or Soft-Appliance Server | 27 |
| Download the RSA Identity Governance and Lifecycle Installation Files | 28 |
| Copy the Installation Files to the Installation Host | 29 |
| Run the Installation Script | 30 |
| Verify the Upgrade Succeeded (RSA-Supplied Database) | 31 |
| Import the Database Backup | 32 |
| Verify Data Restoration and Start All Services | 35 |
| Confirm the Setting for the Encryption Key Directory | 35 |
| Re-install Remote Agents | 39 |
| Restore Your Customization Files | 40 |
| Delete the Jboss Folder (When Upgrading From a Pre-v7.0 Product Version) | 41 |

| | |
|---|----|
| Upgrade RSA Identity Governance and Lifecycle on WebSphere Application Server | 41 |
| Deploy the WebSphere Installation EAR Files | 42 |
| Update the Setting for the Encryption Key Directory | 44 |
| Re-install Remote Agents | 48 |
| Upgrade RSA Identity Governance and Lifecycle on WebLogic Application Server | 49 |
| Deploy the WebLogic Installation EAR Files | 50 |
| Update the Setting for the Encryption Key Directory | 52 |
| Re-install Remote Agents | 56 |
| Upgrade AFX | 57 |
| Upgrade AFX If You Have a Pre-6.8.1 Version Installed | 59 |
| Migrate AFX Connectors and Templates from AFX 2.0.x or 2.5.x | 59 |
| Upgrade the AFX Server to Version 7.x | 61 |
| Verify the Upgrade | 62 |

Preface

About This Guide

This guide provides instructions for upgrading RSA Identity Governance and Lifecycle software. It is intended for administrators and other trusted personnel.

Documentation Set

The latest product documentation is always available at <https://community.rsa.com/community/products/governance-and-lifecycle>.

| Document | Description |
|-------------------------------------|---|
| Release Notes | What's new in the release, fixed issues, known issues and workarounds. |
| Installation Guide | Product installation instructions. |
| Upgrade and Migration Guide | Instructions for upgrading your product version and data. |
| Database Setup and Management Guide | Instructions for setting up and managing a customer-supplied Oracle database for RSA Identity Governance and Lifecycle. |
| Online Help | All concepts and instructions you need to configure and use the product. |
| Public Database Schema Reference | The public view of the database schema. |

Support and Service

You can access community and support information on RSA Link at <https://community.rsa.com/community/products/governance-and-lifecycle>. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

You can also access the RSA Identity Governance and Lifecycle community at <https://community.rsa.com/community/products/governance-and-lifecycle/client-partner-community>. This private community is only available to RSA Identity Governance and Lifecycle customers, partners and internal RSA staff.

Chapter 1: Supported Upgrade Scenarios

The following table lists supported upgrade scenarios and the tasks you must perform for each.

| Scenario | Tasks |
|--|---|
| Upgrade from v7.0 to v7.0.1 on all platforms | <ol style="list-style-type: none"> 1. Verify Upgrade Prerequisites 2. Prepare to Upgrade the RSA Identity Governance and Lifecycle Software 3. Upgrade RSA Identity Governance and Lifecycle Software |
| Upgrade from product versions v5.x and v6.x on an appliance or compatible server to v7.0.1 | <ol style="list-style-type: none"> 1. Identifying Collector Changes Using Migration Reports Before Migrating Collectors 2. Verify Prerequisites for an RSA Appliance or Verify Prerequisites for a Soft-Appliance Installation. 3. Prepare to Upgrade the RSA Identity Governance and Lifecycle Software. 4. Upgrade RSA Identity Governance and Lifecycle on an Appliance or Soft Appliance. |
| Upgrade from product versions v5.x or v6.x to v7.0.1 on WebLogic | <ol style="list-style-type: none"> 1. Verify Prerequisites for WebLogic Installation. 2. Back Up the Remote Customer-Supplied Database. 3. Upgrade RSA Identity Governance and Lifecycle on WebLogic Application Server. |
| Upgrade from product versions v5.x or v6.x to v7.0.1 on WebSphere | <ol style="list-style-type: none"> 1. Verify Prerequisites for WebSphere Installation. 2. Back Up the Remote Customer-Supplied Database. 3. Upgrade RSA Identity Governance and Lifecycle on WebSphere Application Server. |
| Upgrade Access Fulfillment Express (AFX) | <ul style="list-style-type: none"> • Upgrade AFX If You Have a Pre-6.8.1 Version Installed. • Upgrade AFX (soft-appliance upgrade scenario) • To initiate the automatic upgrade of AFX during the RSA Identity Governance and Lifecycle upgrade process if AFX is installed on your appliance, see the instructions in Step 3: Run the Installation Script. |

Chapter 2: Pre-Upgrade Tasks for Migrating Collectors

Important: Read this chapter only if you are upgrading from a pre-7.0 version of RSA Identity Governance and Lifecycle.

RSA Identity Governance and Lifecycle v7.0.1 includes changes that affect the collection of data. For example, Identity Data Collectors (IDCs) no longer collect user group information. Before you upgrade, you must ensure that your existing collectors will continue to run and collect the correct data after you upgrade.

Use the Migration Report Utility to generate reports that list issues related to your current configuration and data and help you resolve those issues. RSA strongly recommends that you use these reports before upgrading to RSA Identity Governance and Lifecycle v7.0.1. If you do this prior to upgrading, some data might be rejected during migration and you will have to reconfigure some collectors after upgrading.

Changes to Data Collections

RSA Identity Governance and Lifecycle v7.0.1 includes the following data collection changes:

- Identity Data Collectors no longer collect user groups.
- Duplicate objects are no longer allowed within an application namespace. Previously, duplicate objects were not allowed within a collector, and as a result more than one collector was allowed to collect the same entitlement for an application.
- Primary Data Access Collectors are no longer able to collect duplicate resources based on the Fully Qualified Name.
- Entitlement Data Collectors no longer collect role entitlements. Instead, Role Data Collectors collect all role entitlements.

About Full Refresh Collections after Migration

When you migrate to RSA Identity Governance and Lifecycle v7.0.1 from a pre-7.0 version of the product, note that all of your initial data collections are designated as "full refresh" collections. This means that previously collected data is removed from the system and all data that is collected is new or has changed. All subsequent collections are processed by the delta model.

Migration Reports

After you install and generate the migration reports on your pre-7.0.1 system, you can access the reports from Admin > System > Diagnostics. You can generate all or individual reports that list particular types of issues and the objects affected by those issues. You can download a single HTML version of the reports as you would any other statistics report.

See [The Migration Report Utility](#) and [Download and Configure the Migration Report Utility](#) for more information.

The following table describes each report and provides the high-level steps required to resolve issues.

| Report | Description and Issue Resolution Steps |
|---|--|
| Active IDC Groups | IDCs no longer collect user groups. If any IDCs collect user groups, you must reconfigure them. |
| Collectors Using Identity Collectors for Group Resolution Rules | Because IDCs no longer collect group data, you must edit the collector using the IDC and remove the IDC from the resolution list for groups. If you are reconfiguring ADCs to collect group data, replace the IDC with the ADC that collects the group data. |
| Cyclic Application Roles | <p>Cyclic application roles occur when an application role is collected as an entitlement member of itself, or when the application role is an entitlement in a child role. These cyclic relationships are not supported in v7.0.1.</p> <p>To remove cyclic application roles:</p> <ol style="list-style-type: none"> 1. Edit the collector source data to remove cyclic relationships. 2. Run the collections to remove the cyclic relationships. 3. Rerun the migration report to verify that the cyclic application roles no longer exist. |
| Cyclic Global Roles | <p>Cyclic global roles occur when a role is collected as a member of itself. These cyclic relationships are not supported in v7.0.1.</p> <p>To remove cyclic global roles:</p> <ol style="list-style-type: none"> 1. Edit the collector source data to remove cyclic relationships. 2. Run the collections to remove the cyclic relationships. |

| Report | Description and Issue Resolution Steps |
|-----------------------------------|---|
| | <ol style="list-style-type: none"> Rerun the migration report to verify that the cyclic roles no longer exist. |
| Cyclic Group Memberships | <p>Cyclic group memberships occur when a group is collected as a member of itself. These cyclic relationships are not supported in v7.0.1.</p> <p>To remove cyclic group memberships:</p> <ol style="list-style-type: none"> Edit the collector source data to remove cyclic relationships. Run the collections to remove the cyclic relationships. Rerun the migration report to verify that the cyclic groups no longer exist. |
| Duplicate Objects | <p>Duplicate objects occur when multiple collectors collect the same data for an application.</p> <p>To remove duplicate objects:</p> <ol style="list-style-type: none"> Determine which data collector is incorrectly configured to collect duplicate objects. Edit the data collector so that the query that it uses excludes the duplicate objects. <p>Note: You may need to modify the source data to avoid collecting duplicates.</p> <ol style="list-style-type: none"> Save the changes to the collector. Run the collector. Verify the duplicate objects have been removed by running the migration report again. |
| EDCs Associated to RDCs | EDCs that are configured to process an RDC's entitlements. |
| EDCs Collecting Role Definitions | <p>EDCs no longer collect data associated with roles. Role collectors collect all role definitions.</p> <p>You must reconfigure all EDCs after upgrading to v7.0.1.</p> |
| IDCs Configured to Collect Groups | IDCs no longer collect group data. If any IDCs collect groups, you must reconfigure them. |

| Report | Description and Issue Resolution Steps |
|----------------------------|---|
| Roles Having Group Members | In previous versions, an RDC was associated with a single IDC. Values collected by the RDC were mapped to an attribute in the IDC, which restricted the collection of users to a particular IDC. In RSA Identity Governance and Lifecycle v7.0.1, one or more target IDCs can be configured for the RDC, allowing resolution from multiple IDCs. Each target collector has a user attribute that resolves the collected user. |

The Migration Report Utility

The Migration Report Utility identifies which data and collectors must be modified before the upgrade. The Migration Report Utility file (MigrationReports.zip) contains the following files used to identify installation issues.

| File | Purpose |
|--------------------------------------|--|
| generateMigrationReport.sh | Creates a full migration report similar to a statistics report. |
| insertMigrationReportDefinitions.sh | Creates tabular report definitions for each report listed in the table in "Migration Reports." |
| insertMigrationReportDefinitions.sql | Used by the shell script for creating the tabular report definitions for the individual reports. |
| Pre_Migration_Pkg.pkb | Database package used by the full migration report. |

See [Download and Configure the Migration Report Utility](#) for more information.

Download the Migration Report Utility

Download the Migration Report Utility (MigrationReports.zip) from RSA SecureCare Online, extract the compressed file, and set the correct permissions on the reporting scripts.

Procedure

1. Download the MigrationReports.zip file from from RSA Link at <https://community.rsa.com/community/products/governance-and-lifecycle>.
2. Copy the zip file to the machine hosting the pre-7.0.1 RSA Identity Governance and Lifecycle database.
3. Log on to the database machine as root.

4. Extract the zip file to a temporary directory on the system. For example, on an RSA appliance extract to /tmp/aveksa.
5. Change the permissions on the script files to allow execution privileges. Enter

```
chmod 755 <filename>
```

where *<filename>* is the name of the script.

Install the Migration Reports

If you want to review individual reports for each type of issue that may affect your data, run the `insertMigrationReportDefinitions.sh` script to create the tabular report definitions for the individual migration reports.

Important: If you are upgrading on WebSphere or WebLogic hosted on the AIX, see the Procedure (upgrading on WebLogic or WebSphere hosted on AIX) section below for instructions on how to install the migration reports on those platforms. You cannot run the `insertMigrationReportDefinitions.sh` bash shell script on AIX.

Procedure

1. Log on to the database machine as the oracle user.
Note: Ensure that the file for the script includes execution privileges.
2. Change to the directory containing the extracted Migration Utility scripts. For example, if you have extracted the scripts to /tmp/aveksa, enter

```
cd /tmp/aveksa/MigrationReports
```
3. At the command prompt, enter

```
insertMigrationReportDefinitions.sh
```
4. When prompted, enter the passwords for the AVUSER and the AVDWUSER.
After the script has created the reports, the following message displays:

```
Created required reports with Category Migration
```

Procedure (upgrading on WebLogic or WebSphere hosted on AIX)

Follow these instructions to install migration reports on WebLogic and WebSphere hosted on AIX.

1. cd to the database/Upgrade directory
2. Log on to sqlplus as avuser
3. Run the following commands:

- a. `whenever sqlerror exit 1 rollback`
- b. `whenever oserror exit 2 rollback`
- c. `set serveroutput on size 1000000`
- d. `@./insertMigrationReportDefinitions.sql;`
- e. `commit`

4. Run the following transaction block:

```
BEGIN
FOR rec IN (select 'grant select on ' || TO_CHAR(view_name) || ' to
avdwuser' cmd
from avuser.T_AV_REPORTS
where regexp_like(view_name, '^[vV]_[a-zA-Z0-9_]+$')
and LENGTH(view_name) <= 30 AND REPORT_CATEGORY = 'Migration')
LOOP
EXECUTE IMMEDIATE rec.cmd;
END LOOP;
END;
/
```

5. `commit;`
6. Log out of sqlplus and log in again as avdwuser.

7. Run the following transaction block:

```
BEGIN
FOR rec IN (select 'create or replace synonym ' || TO_CHAR(view_name) ||
' for avuser.' || TO_CHAR(view_name) cmd
from avuser.T_AV_REPORTS
where regexp_like(view_name, '^[vV]_[a-zA-Z0-9_]+$')
and LENGTH(view_name) <= 30 AND REPORT_CATEGORY = 'Migration')
LOOP
EXECUTE IMMEDIATE rec.cmd;
END LOOP;
END;
/
```

8. `commit;`

Run the Full Migration Report

The full migration report includes all migration issues and instructions for resolving them.

Important: If you are upgrading on WebSphere or WebLogic hosted on the AIX, see the Procedure (upgrading on WebLogic or WebSphere hosted on AIX) section below for instructions on running the migration reports on those platforms. You cannot run the `generateMigrationReport.sh` bash shell script on AIX.

Procedure

1. Log on to the database machine as the oracle user.

Note: Make sure that the file for the script includes execution privileges.

2. Go to the directory where you extracted `MigrationReports.zip`. For example:

```
cd /tmp/aveksa/MigrationReports
```

3. At the command prompt, enter

```
generateMigrationReport.sh
```

4. As prompted, provide the password for avuser.
5. View the full migration report in RSA Identity Governance and Lifecycle:
 - a. Log on to the RSA Identity Governance and Lifecycle.
 - b. Click Admin > System > Diagnostic.
 - c. Under Statistics Report in the row containing the report, do one of the following:
 - Download the report by clicking View.
 - Download a ZIP file containing the report by clicking Download.

Procedure (upgrading on WebLogic or WebSphere hosted on AIX)

Follow these instructions to run the `sqlplus` command the `generateMigrationReport.sh` script ultimately calls.

1. `cd` to the database/Upgrade directory.
2. Log on to `sqlplus` as avuser.
3. Run the following commands:
 - a. `whenever sqlerror exit 1 rollback`
 - b. `whenever oserror exit 2 rollback`
 - c. `set serveroutput on size 1000000`

- d. @"/packages/Pre_Migration_Pkg.pkb";
- e. exec Pre_Migration_Pkg.Save_Report;
- f. commit

Run an Individual Migration Report

The individual migration reports list issues within a given category, for example, IDCs configured to collect user groups, and instructions for resolving the issue. For more information, see [Migration Reports](#).

Procedure

1. Log on to RSA Identity Governance and Lifecycle as an administrative.
2. Click Reports > Tabular.
3. In the Grouping drop-down list, select Type.
4. In the table of reports, click Migration (10).
5. Click the name of the report that you want to run.
6. Click Run Report.
7. Save the report results.
8. In the View Report screen do one of the following:
 - Export the results in a particular format:
 - a. Click Export.
 - b. Select the file type in which to save the report results.
 - c. Click OK.
 - Save the results for viewing in the RSA Identity Governance and Lifecycle console:
 - a. Click Save Results.
 - b. Enter a Description for the report results.
 - c. Click OK.

Note: RSA recommends that you perform these steps until the reports indicate no further issues, or until you have saved all of the necessary data.

Chapter 3: Verify Upgrade Prerequisites

Before you upgrade, verify that your current installation satisfies the prerequisites for your installation type:

- [Review Public Database Schema and Port Changes Introduced in v7.0.1](#)
- [Verify Prerequisites for an RSA Appliance](#)
- [Verify Prerequisites for a Soft-Appliance Installation](#)
- [Verify Prerequisites for WebSphere](#)
- [Verify Prerequisites for Weblogic](#)
- [Additional Prerequisites for WebLogic and WebSphere Application Servers](#)

Review Public Database Schema and Port Changes Introduced in v7.0.1

Database Schema Changes

Version 7.0.1 introduces changes to the public database schema. These changes may impact any report configurations that include queries against earlier product version public database schema views.

Deprecated Collectors Table Columns:

- `ROLE_COLLECTOR.USES_IDC_ID`
- `ENTITLEMENT_COLLECTOR.USES_RDC_ID`
- `MULTI_APP_COLLECTOR.USES_RDC_ID`

New Entitlement Relationship Tables:

- `ROLE_COLLECTOR.USES_IDC_ID`
- `ENTITLEMENT_COLLECTOR.USES_RDC_ID`
- `MULTI_APP_COLLECTOR.USES_RDC_ID`
- `BUSINESS_SOURCE`
- `DIRECT_UENTS_WITH_VIOLS`
- `UNIFIED_ENTITLEMENT`

New Users Table:

`USER_DATA_CLEANUP_ITEMS`

Port Changes

Take note of the changes to the ports that use Secure Socket Layer (SSL).

| Version | Changes |
|-------------------|--|
| 7.0.1 and later | Port 8443 connects through SSL. Port 8445 does not work. |
| 6.9.1 and earlier | Port 8443 connects through SSL. Port 8445 connects through non-SSL. |

Verify Prerequisites for an RSA Appliance

Procedure

1. Verify that your appliance is supported for upgrade. RSA supports only RSA- or Aveksa-supplied hardware containing the following model numbers for upgrade.

| Environment | Model Numbers |
|-------------|-------------------------------------|
| Development | Dell R320 |
| Production | Dell R620 Dell R710 Dell R720 |

2. Verify that the appliance runs a supported version of RSA Identity Governance and Lifecycle, v5.x or later. If the appliance runs v4.x and the hardware meets all other requirements, you must install a supported RSA Identity Governance and Lifecycle version before upgrading. For instructions, see the *Installation Guide* for the version you must install.
3. Verify that the appliance runs one of the following 64-bit operating systems. See the *Installation Guide* for instructions if you must install a 64-bit operating system before upgrading.

| Operating System | Patch Level |
|---------------------------------|-------------------------|
| SUSE Linux Enterprise Server 11 | SP3 64-bit |
| Red Hat Enterprise Linux 5 | u8 64-bit u11 64-bit |

4. Verify that the following operating system users and groups for RSA Identity Governance and Lifecycle have the correct ID assignments. If the IDs are incorrect, the upgrade fails and cannot be successfully resumed until the IDs are corrected.

| User | Required UID | Group | Required GID |
|--------|--------------|----------|--------------|
| oracle | 500 | oinstall | 500 |
| admin | 501 | dba | 501 |
| | | datadir | 502 |

5. Verify whether a valid Network Time Protocol (NTP) server is configured for RSA Identity Governance and Lifecycle. You may need to provide the IP address if the installation process cannot find the NTP server currently configured.
6. Verify that operating system /root volume has at least 16 GB of free disk space.

Verify Prerequisites for a Soft-Appliance Upgrade

Procedure

1. Verify that the server where RSA Identity Governance and Lifecycle is installed meets the following requirements.

| Component | Development Environment | Production Environment |
|------------|---|---|
| RAM | 48 GB | 48 GB |
| Processor | Intel E5-2400 Quad Core | Dual Intel E5-2400 Quad Core |
| Disk Space | <ul style="list-style-type: none"> • 450 GB (RAID 1 or RAID 5) • 16 GB minimum for /root volume | <ul style="list-style-type: none"> • 1 TB + (RAID 1 or RAID 5) • 16 GB minimum for /root volume |
| Network | Bond of NICs in active-backup bond mode | |

2. Verify that the installation server runs a supported version of RSA Identity Governance and Lifecycle, v5.x or later. If the appliance runs v4.x and the hardware meets all other requirements, you must install a supported version before upgrading. For instructions, see the *Installation Guide* for the version you must install.
3. Verify that the installation server runs one of the following 64-bit operating systems.

| Operating System | Patch Level |
|---------------------------------|-----------------------|
| SUSE Linux Enterprise Server 11 | SP3 or SP4; 64-bit |
| Red Hat Enterprise Linux 5 | u10 64-bit or greater |

| Operating System | Patch Level |
|----------------------------|----------------------|
| Red Hat Enterprise Linux 6 | u5 64-bit or greater |

Note: RSA Identity Governance and Lifecycle using the RSA-supplied database does not support automatic storage management (ASM).

If the server is not running a supported version of the operating system, you must patch or re-install the OS and re-install RSA Identity Governance and Lifecycle. For instructions, see the *Installation Guide*.

- Verify that the following operating system users and groups for RSA Identity Governance and Lifecycle have the correct ID assignments. If the IDs are incorrect, the upgrade fails and cannot be successfully resumed until the IDs are corrected.

| User | Required UID | Group | Required GID |
|--------|--------------|----------|--------------|
| oracle | 500 | oinstall | 500 |
| admin | 501 | dba | 501 |
| | | datadir | 502 |

- If you use a customer-supplied (remote) database, verify that is running Oracle 12.1.0.2. If it is not, upgrade to Oracle 12.1.0.2 before upgrading RSA Identity Governance and Lifecycle.

Important: If you are upgrading from 6.8.1 or 6.9.1, do the following: back up the database, upgrade to Oracle 12.1.0.2, then restore and migrate the database. See [Back Up the Customer-Supplied Database](#) and [Import Your Customer-Supplied Database Backup and Migrate the Database](#) for instructions. See Oracle documentation for instructions on upgrading the database.

- Verify that required Oracle packages are installed on the same machine as the RSA Identity Governance and Lifecycle software.
 - See the "Package Requirements for Oracle Management Service" section at http://docs.oracle.com/cd/E29505_01/install.1111/e22624/preinstall_req_packages.htm
 - See the "Configuring Operating Systems for Oracle Grid Infrastructure and Oracle RAC" section at <http://docs.oracle.com/database/121/CWLIN/prelinux.htm#CWLIN168>
- Verify whether a valid Network Time Protocol (NTP) server is configured for RSA Identity Governance and Lifecycle. You may need to provide the IP address if the installation process cannot find the NTP server currently configured.

Verify Prerequisites for Upgrading on WebSphere

The WebSphere application server where you plan to upgrade RSA Identity Governance and Lifecycle must meet the following requirements.

| Component | Requirement |
|---|---|
| RSA Identity Governance and Lifecycle Version | V5.x or greater. If you are running V4.x, you must perform a new installation, which you can do as long as the system meets all of the other requirements listed in this table. |
| WebSphere Version | Either of the following: <ul style="list-style-type: none"> • IBM WebSphere Application Server Edition 8.5.5 Fix Pack 2 • IBM WebSphere Application Server Network Deployment Edition 8.5.5 Fix Pack 2 |
| RAM | Development environment: 16 GB Production environment: 32 GB |
| Operating System | An operating system that supports WebSphere |
| Database | An Oracle 12.1.0.2 instance configured to support RSA Identity Governance and Lifecycle. For more information about database requirements, see "Verify Prerequisites for a Customer-Supplied Database" in the <i>Installation Guide</i> . For instructions on configuring the remote, customer-supplied database, see the <i>Database Setup and Management Guide</i> . Important: If you are upgrading from 6.8.1 or 6.9.1, do the following: back up the database, upgrade to Oracle 12.1.0.2, then restore and migrate the database. See Back Up the Customer-Supplied Database and Import Your Customer-Supplied Database Backup and Migrate the Database for instructions. See Oracle documentation for instructions on upgrading the database. |
| Disk Space | 600 MB available for RSA Identity Governance and Lifecycle |
| Java | IBM JDK 1.7 |

Verify Prerequisites for Upgrading on WebLogic

The WebLogic application server where you plan to upgrade RSA Identity Governance and Lifecycle must meet the following requirements.

| Component | Requirement |
|---|---|
| RSA Identity Governance and Lifecycle Version | V5.x or greater. If you are running V4.x, you must perform a new installation, which you can do as long as the system meets all of the other requirements listed in this table. |
| WebLogic Version | 12.1.3 or greater |
| RAM | Development environment: 16 GB Production environment: 32 GB Note: You must allocate at least 4 GB of RAM to the RSA Identity Governance and Lifecycle server. |
| Operating System | An operating system that supports WebLogic |
| Database | An Oracle 12.1.0.2 instance configured to support RSA Identity Governance and Lifecycle. For more information about database requirements, see "Verify Prerequisites for a Customer-Supplied Database" in the <i>Installation Guide</i> . For information about configuring the customer-supplied database, see the <i>Database Setup and Management Guide</i> . Important: If you are upgrading from 6.8.1 or 6.9.1, do the following: back up the database, upgrade to Oracle 12.1.0.2, then restore and migrate the database. See Back Up the Customer-Supplied Database and Import Your Customer-Supplied Database Backup and Migrate the Database for instructions. See Oracle documentation for instructions on upgrading the database. |
| Disk Space | 600 MB available for RSA Identity Governance and Lifecycle |
| Java | Oracle JDK 1.7 |

Additional Prerequisites for WebLogic and WebSphere Application Servers

Procedure

1. If you are upgrading from a pre-v5.0 release, you must add the following new JVM setting resources and uninstall the existing RSA Identity Governance and Lifecycle application before you install the new version. See the *Installation Guide* for more information on configuring the JVM settings:
 - bus member acmMessageTopic
 - acmConnectionFactory
 - jms topic acmMessageTopic.
2. If you are upgrading from a pre-v5.1 release, you must define the ACMProviderUrl variable to configure the communication with RSA Identity Governance and Lifecycle. This is the bootstrap port on WebSphere and the listening port on WebLogic. For instructions on configuring these ports, see the *Installation Guide*.
3. If you are upgrading from a pre-v6.5 release, you must change the following object names in the JDBC data source. For more information, see "Create the JDBC Data Sources" in the WebSphere Installation or WebLogic Installation chapter of the *Installation Guide*.
 - WPDS data source JNDI name
 - WPDS2 data source JNDI names
 - WPDS3 data source JNDI name
 - wpServAutoActSpec name and JNDI name
4. If you are upgrading from a pre-v6.8 release, ensure that the application server instance (or node) JVM heap size for the application server memory has a minimum of 4 GB and the permanent generation heap has a minimum of 512 MB. For more information, see the *Installation Guide*.
5. (WebSphere application server only) If you are upgrading from a pre-v6.5 release, you must add the component-managed authentication setting in the JDBC data source for the following objects.
 - WPDS data source JNDI name
 - WPDS2 data source JNDI name
 - WPDS3 data source JNDI name

For more information, see "Create the JDBC Data Sources" in the WebSphere Installation chapter of the *Installation Guide*.

Chapter 4: Prepare to Upgrade the RSA Identity Governance and Lifecycle Software

Before you upgrade, complete the preparation tasks for your upgrade scenario:

- [Back up RSA Identity Governance and Lifecycle \(Appliance and Soft-Appliance Only\) and Customization Files](#)
- [Apply the Latest Operating System and Database Patch Updates](#)
- [Back Up the RSA-Supplied Database](#)
- [Back Up the Customer-Supplied Database](#)
- [Prepare for an Upgrade on WebLogic](#)
- [Prepare for an Upgrade on WebSphere](#)

Important: Ensure that your environment meets the prerequisites for your upgrade scenario as described in [Verify Upgrade Prerequisites](#) before you prepare for the upgrade.

Back up the RSA Identity Governance and Lifecycle Application (Appliance and Soft-Appliance Only)

Back up RSA Identity Governance and Lifecycle configurations settings so they can be restored if necessary. See "Restore RSA Identity Governance and Lifecycle" in the *Installation Guide* for information on restoring an RSA Identity Governance and Lifecycle software backup.

Also, if you are upgrading from a pre-7.0 version of RSA Identity Governance and Lifecycle, save to a safe location any customization files from `/jboss-4.2.2.GA/server/default/deploy/aveksa.ear/aveksa.war` that you want to restore after the upgrade. As of V7.0, customizations must be applied to the RSA Identity Governance and Lifecycle EAR file and then redeployed into the WildFly application server.

For information on restoring your customization files after the upgrade, see [Restore Your Customization Files](#).

Before You Begin the RSA Identity Governance and Lifecycle Backup

(Optional) Attach and mount an external drive to the installation host as desired for the backup.

Procedure

1. Stop all RSA Identity Governance and Lifecycle services:
 - a. Log in to the installation machine as the 'admin' user.

- b. Enter the following command:

```
sudo service aveksa_server stop
```

2. Stop AFX if it is installed:

```
<path-to-AFX>/afx stop
```

3. Restart the database.

- Shut down the database. Enter:

```
sudo service aveksa_server stopdb
```

- Start the database. Enter:

```
sudo service aveksa_server startdb
```

4. Change to the following directory path:

```
cd /home/oracle/deploy
```

5. Enter the following command:

```
sudo ./acm_backup.sh
```

6. Enter 'yes' to perform the backup operation.

The command creates a file named Backup<*product version*>.tar in the following directory:

```
/home/oracle/AveksaExportImportDir
```

Important: Keep the Backup<product-version>.tar file in a safe place where it can be accessed in case you need to restore.

Apply the Latest Operating System and Database Patch Updates

RSA recommends that you download the Appliance Updater to apply the latest operating system (appliance only) and RSA-supplied database (appliance and soft-appliance installations) patches before you upgrade. The Updater bundles a certified patch set for the RSA-supplied operating system (SUSE or Red Hat) and the RSA-supplied Oracle database. Downloading and running the latest appliance updater closes vulnerabilities and addresses bugs.

On a quarterly basis, RSA bundles patches into a compressed file (rsaimg_updater_<release quarter>_<platform>.tar.bz2) and posts it to RSA Link at

<https://community.rsa.com/community/products/governance-and-lifecycle> for download.

For more information, see the *RSA Identity Governance and Lifecycle Appliance Updater Guide*, also available on RSA Link at <https://community.rsa.com/community/products/governance-and-lifecycle>.

Back Up the RSA-Supplied Database

Note: This task applies only to installations using an RSA-supplied Oracle database. If you use a customer-supplied database, see [Back Up the Customer-Supplied Database](#) for instructions.

This task creates a dump (.dmp) file of the AVUSER schema. The file contains all of the application data and some environment data about a particular system environment.

Procedure

1. Log in to the installation machine as the 'admin' user.
2. Enter the following command:

```
sudo service aveksa_server stop
```
3. Log on to the installation machine as the 'oracle' user.
4. Enter the following command:

(On a soft-appliance host): `/home/oracle/database/DBA/AVDB/scripts/AVDB_Export_AVUSER.sh -t _Backup_Pre_Upgrade -o /home/oracle/upgradbackup`

(On an appliance host): `avdbexport -t _Backup_Pre_Upgrade -o /home/oracle/upgradbackup`

The `-t` option, provides a tag name that is appended to the standard export file name. The script creates an export file named `Export_AVDB_avuser_Backup_Pre_Upgrade.dmp` file in the directory specified by the `-o` option. If `-o` option is not specified, the export file is saved to `/home/oracle/AveksaExportImportDir/`

Note: If you also want to compress the dump file, use the `-g` option.

Note: When using the `-i` option, ensure that the AVUSER and SYS database user passwords are the same. Both users are involved in executing the command. For more information on changing passwords, see "Changing Database User Passwords," in the *Installation Guide*.

5. Copy the .dmp file to an external location (off the appliance).
6. Check the results of the export process in the following log:

```
/home/oracle/AveksaExportImportDir/Export_AVDB_avuser_Backup_Pre_Upgrade.log
```


Back Up the Customer-Supplied Database

Note: If you are upgrading to 7.0.1 from a pre-7.0 version of RSA Identity Governance and Lifecycle, you must back up the database and manually restore it after upgrading. If you are upgrading to 7.0.1 from 7.0, a backup is not required. The upgrade process automatically imports your data.

Before You Begin

- Ensure that the AVEKSA_EXPORTIMPORT_DIRECTORY directory has been created as described in "Set Up the Database" in the *Database Setup and Management Guide*
- Ensure that the database process has Read-Write permissions to the directory.

Procedure

1. Shut down the RSA Identity Governance and Lifecycle server before you export a database.
2. Shut down AFX if it is installed.
3. Run the following command from the database server machine:

```
expdp avuser/<password>@<Oracle_SID> DumpFile=<FileName>.dmp  
Directory=Avekسا_ExportImport_Directory Schemas=avuser  
LogFile=<FileName>.log
```

Where:

`Expdp` is the Oracle data pump utility.

`avuser/<password>` is the connection string.

`DumpFile` is the output file name; here set with a date stamp.

`Directory` is an internal Oracle directory object mapped to a physical UNIX directory. It would typically be the `AvekساExportImportDir` directory created when the customer-provided database was set up.

`Schemas` is the database, `avuser` for example.

`Logfile` is the name of the log file generated for the export.

Prepare for an Upgrade on WebLogic

Complete the following steps before you perform the upgrade.

Procedure

1. Make sure processing tasks are not running on the server:
 - a. Log in to RSA Identity Governance and Lifecycle.
 - b. Go to Admin > Monitoring to determine whether tasks are running.
 - c. Wait until all tasks have completed before proceeding with the upgrade.
2. Stop the RSA Identity Governance and Lifecycle server. See the Installation Guide for your current product version for instructions.
3. Stop AFX if it is installed.
4. Back up the database. See [Back Up the Customer-Supplied Database](#).
5. Upgrade the database to Oracle 12.1.0.2.

Prepare for an Upgrade on WebSphere

Complete the following steps before you perform the upgrade.

Procedure

1. Make sure processing tasks are not running on the server:
 - a. Log in to RSA Identity Governance and Lifecycle.
 - b. Go to Admin > Monitoring to determine whether tasks are running.
 - c. Wait until all tasks have completed before proceeding with the upgrade.
2. Stop the RSA Identity Governance and Lifecycle server. See the Installation Guide for your current product version for instructions.
3. Stop AFX if it is installed.
4. Back up the database. See [Back Up the Customer-Supplied Database](#).
5. Upgrade the database to Oracle 12.1.0.2.

Chapter 5: Perform the Upgrade

The upgrade installs the latest version of RSA Identity Governance and Lifecycle. This chapter assumes that you performed all of the relevant prerequisite verifications and tasks in the previous chapters.

See the section for your upgrade scenario:

- [Upgrade RSA Identity Governance and Lifecycle on an Appliance or Soft-Appliance Server](#)
- [Upgrade RSA Identity Governance and Lifecycle on WebSphere Application Server](#)
- [Upgrade RSA Identity Governance and Lifecycle on WebLogic Application Server](#)
- [Upgrade AFX](#)
- [Upgrade AFX If You Have a Pre-6.8.1 Version Installed](#)

Important: If you plan to upgrade AFX along with RSA Identity Governance and Lifecycle, see [Upgrade AFX](#) for pre- and post-upgrade task instructions.

Upgrade RSA Identity Governance and Lifecycle on an Appliance or Soft-Appliance Server

To complete the upgrade, perform the following steps:

1. [Download the Installation Files](#)
2. [Copy the Downloaded Installation Files to the Installation Host](#)
3. [Run the Installation Script](#)
4. [Verify the Upgrade Succeeded \(RSA-Supplied Database\)](#)
5. [Import the Database Backup](#)
6. [Verify Data Restoration and Start All Services](#)
7. [Confirm the Setting for the Encryption Key Directory](#)
8. [Re-install Remote Agents](#)
9. [Restore Your Customization Files](#)
10. [Delete the Jboss Folder \(When Upgrading From a Pre-v7.0 Product Version\)](#)

Download the RSA Identity Governance and Lifecycle Installation Files

Procedure

1. Download the following installation files:
 - a. Go to [RSA Link](https://community.rsa.com/community/products/governance-and-lifecycle) (https://community.rsa.com/community/products/governance-and-lifecycle), then click Log In and enter your user name and password.
 - b. Click RSA Identity Governance and Lifecycle.
 - c. Click Downloads > RSA Identity Governance and Lifecycle 7.0.1.
 - d. Click on Additional Downloads.
 - e. Click Access Certification Manager.
 - f. Click Download Software (it may take a minute to display the Product List).
 - g. Click RSA Identity Governance and Lifecycle (formerly Aveksa) - Version Upgrades. The Current tab lists the most recent release. The Archive tab lists previous releases.
 - h. Click Access Certification Manager Version 7.0SP1.
 - i. Download the following files:
 - wildfly-8.2.0.Final.tar
 - openjdk17_v001.tar.bz2
 - aveksa-<product-version>.tar.bz2
 - j. If you are using a customer-supplied database, download these files:
 - instantclient-basiclite-linux.x64-12.1.0.2.0.zip
 - instantclient-sqlplus-linux.x64-12.1.0.2.0.zip
2. If you are using an RSA-supplied database, go back one screen, select Hardware Appliance Version 7.0SP1, then download these files:
 - linuxamd64_12102_database_1of2.zip
 - linuxamd64_12102_database_2of2.zip
 - linuxamd64_12102_grid_1of2.zip
 - linuxamd64_12102_grid_2of2.zip
 - oracle_12.1.0.2_patches_v001.zip
 - asmlib-008_x64.tar.bz2

- `cvupack_Linux_x86_64.zip`
 - `redhat-release-6Server-1.noarch.rpm` (Download only for a Soft Appliance running Red Hat Enterprise Linux 6)
3. Download the appliance updater file for your installation.

| Operating System | Appliance Updater |
|--|---|
| RSA appliance running SUSE Enterprise Linux Server 11 SP3 or a soft-appliance server with an RSA-supplied database | <code>rsaimg_updater_2016Q2_SLES11_12C.tar.bz2</code> |
| RSA appliance running Red Hat Enterprise Linux 5 | <code>rsaimg_updater_2016Q2_RHEL5_12C.tar.bz2</code> |

Copy the Installation Files to the Installation Host

Procedure

1. Log in to the host as root.
2. Create a directory for the packages:


```
mkdir -p /tmp/aveksa/packages
```

Note: If the `/tmp/aveksa/packages` directory already exists, delete any files in the directory.
3. Copy the downloaded installation package files to the `/tmp/aveksa/packages` directory.
4. Verify that the compressed package files you downloaded were not corrupted during the file transfer. Run the following commands in the `/tmp/aveksa/packages` directory:

- `tar -jtvf` on all downloaded `.tar.bz2` files. For example:


```
tar -jtvf asmlib-008_x64.tar.bz2
```
- `unzip -t` on all downloaded `.zip` files. For example:


```
unzip -t linuxamd64_12102_database_1of2.zip
```

The commands list the packages and indicate if errors were detected.

5. Delete the following directory if it exists on the appliance:

```
/tmp/aveksa/staging
```

6. Expand the Aveksa package in a new staging directory:

```
mkdir -p /tmp/aveksa/staging
cd /tmp/aveksa/staging
tar -jxvf /tmp/aveksa/packages/aveksa-<product-version>.tar.bz2
```

Run the Installation Script

Expect the upgrade procedure to consume 60 to 90 minutes.

The installation script performs checks for the following installation requirements:

- Memory
- Operating system packages
- Network settings
- User and group settings
- System configurations

The script displays information about the checks, and it indicates if a requirement is not met. After you resolve the requirement, you can run the script again.

Procedure

1. Log in to the installation host as an administrator with 'root' privileges.
2. Run the upgrade script:

```
cd /tmp/aveksa/staging
./install.sh
```

Note: If the Access Fulfillment Express (AFX) module is installed on the RSA appliance where you are upgrading RSA Identity Governance and Lifecycle and you want to upgrade that AFX module, enter `install.sh -afx`. To upgrade AFX For all other RSA Identity Governance and Lifecycle deployment scenarios, you must perform the steps covered in [Upgrading AFX](#) or [Upgrade AFX If You Have a Pre-6.8.1 Version Installed](#).

3. Read and accept the license agreement.

A series of prompts and other information particular to your installation appears.

4. Enter "yes" at the following prompt:

```
Do you wish to install this version of RSA Identity Governance and
Lifecycle (yes or no)?
```

The installation begins. A summary displays information about the location of the installation and package files, and whether the Oracle database is a customer-supplied (remote) database. The default values on an RSA Identity Governance and Lifecycle appliance are:

```
Location of installation files: /tmp/aveksa/staging
Location of package files: /tmp/aveksa/packages
Use remote Oracle server: N
```

If you answered "Y" (Yes), the script displays the database connection information.

Note: If you created the database instance with non-default names for the database users, you must use the same usernames and passwords when prompted.

5. If the summary of install information is correct, enter "yes" at the following prompt:

```
Does this match your current install information (yes or no)?
```

If you enter "no," you are prompted to provide the correct information.
6. If you want to allow the installation to change the kernel settings, answer yes at the following prompt:

```
Do you want to run kernel settings change script now (yes or no)?
```

If you want to run the script yourself, answer no; the installation ends. You must then run the kernel settings change script (`/tmp/modify_kernel_settings.sh`), before running the installation script again.
7. If you backed up the database, enter `BACKUP-OFFSITE-VERIFIED` at the prompt. Otherwise, stop the installation, perform a backup, and run the installation script again.
8. If you are upgrading from v7.0.0 to v7.0.1, enter Y at the following prompts:

```
An existing database was found. Do you want to keep the database instance [Y] ?
```

```
Migration is necessary when upgrading. Do you want to migrate the database [Y] ?
```

The script indicates when the upgrade has completed. To see what actions the installer performed during the upgrade, review the install log (`/tmp/aveksa-install.log`).

Verify the Upgrade Succeeded (RSA-Supplied Database)

Verify that the upgrade succeeded before you restore the database.

Procedure

1. Start all RSA Identity Governance and Lifecycle services:
 - a. Log in to the installation machine as the 'admin' user.
 - b. Enter the following command:

```
sudo service aveksa_server start
```
2. Log in to RSA Identity Governance and Lifecycle as AveksaAdmin (using the default password: aveksa123).

Note: If you chose not to migrate the database, when you start RSA Identity Governance and Lifecycle for the first time after upgrading, the Initialization Status indicates that the database schema is out-of-date. At the prompt, enter the following password: `AuthorizeMigration`. The startup process performs a migration of the database, which updates the schema.

Note: If stored data must be re-encrypted because a key rollover was done, the Initialization Status indicates the startup process will re-encrypt the data. When the process is complete, you must restart RSA Identity Governance and Lifecycle.

3. Log out from RSA Identity Governance and Lifecycle. If you can log in, your upgrade succeeded.

Import the Database Backup

This task restores the database you backed up before the upgrade. Perform the appropriate task for your database:

- [Import Your RSA-Supplied Database Backup and Migrate the Database](#)
- [Import Your Customer-Supplied Database Backup and Migrate the Database](#)

Import the RSA-Supplied Database Backup and Migrate the Database

You perform the import procedure for the RSA Identity Governance and Lifecycle Oracle database using the `/home/oracle/database/DBA/AVDB/scripts/AVDB_Import_AVUSER.sh` script alias, `avdbimport`, provided with the installation. The script uses the Oracle `impdp` utility to import the dump.

Procedure

1. Log in to the installation machine as the oracle user.

2. Stop services:

```
service aveksa_server stop
```

3. Restart the database:

```
service aveksa_server stopdb  
service aveksa_server startdb
```

4. As the 'oracle' user, enter

```
avdbimport <Options> <Dump_File_Name>
```

Command options:

| Option | Use |
|--------|---|
| -t | Use with the tag name if the exported dump file was saved with a tag name. |
| -i | Use with the input directory name if the exported dump file was saved to an output directory other than the default <code>/home/oracle/AveksaExportImportDir/</code> directory. Note: When using the <code>-i</code> option, ensure that the AVUSER and SYS database user passwords are the same. Both users are involved in executing the command. For more information, see "Changing Database User Passwords" in the <i>Installation Guide</i> |
| -g | Use to uncompress the dump file if the <code>-g</code> option was used to compress the exported dump file. |

5. Start services:

```
service aveksa_server start
```

6. Check the import results in the `Import_AVDB_avuser.log`. By default, the log file is in the following location:

```
/home/oracle/AveksaExportImportDir/Import_AVDB_avuser.log
```

If you used the `-i` option to import the dump file, the log file is in the input directory.

This is the log for the Oracle `impdp` import utility command. You can check the import progress using the `tail -f` command on the log file.

```
/home/oracle/database/DBA/AVDB/logs/
```

The directory contains the log files for the import script that list all completed tasks. A log file name in this directory is based on the Oracle Service name and/or Schema Owner if defined, `Import_${ORACLE_SERVICE_NAME}_${SCHEMA_OWNER}_History.log` for example:

```
Import_AVDB_avuser_History.log
```

7. Migrate the database:

a. Log in to the installation machine as the 'admin' user.

b. Stop services:

```
service aveksa_server stop
```

c. Run the migration command:

```
sudo /home/oracle/deploy/migrate.sh
```

Potential Benign Error Messages When Importing an RSA-Supplied Database

You might encounter the following error messages during the database import. These messages are benign and do not indicate a problem with the import:

- `ORA-06564: object AVEKSA_DATA_DIRECTORY does not exist.`

This directory is not in product releases greater than v6.5. Data dumps imported from older versions invoke this error because the directory is no longer created.

- `ORA-39082: Object type TRIGGER:"AVUSER"."TRIG_AV_JOB_STATS_EMAIL_AI" created with compilation warnings.`

The UTL_MAIL package is not installed in v7.0.1. This trigger is removed after database migration.

- `ORA-31685: Object type MATERIALIZED_VIEW:"AVUSER"."MV_SYSTEMAPPSSUMMARY" failed due to insufficient privileges.`

V7.0.1 does not allow you to create materialized views. The view is removed during database migration.

- `ORA-39082: Object type PACKAGE_BODY:"AVUSER"."AV_JOBSTATS_PKG" created with compilation warnings.`

V7.0.1 does not allow you to see the dba_extents table. The stored procedure that references this table is removed during database migration.

- `ORA-39082: Object type PACKAGE_BODY:"AVUSER"."??????_PKG" created with compilation warnings.`

The schema or security privileges have changed. All stored procedure packages are updated during database migration.

Import the Customer-Supplied Database Backup and Migrate the Database

After the upgrade, import the database on the database server machine using Oracle's impdp data pump utility. It uses a .dmp file of the AVUSER schema created from the export process.

Note: This section assumes you are capable of using an SQL utility (Oracle SQL Developer for example) to issue commands to the database.

Prerequisite

Ensure that the AVEKSA_EXPORTIMPORT_DIRECTORY directory has been created as described in "Set Up the Database" in the *Database Setup and Management Guide* and the database process has Read-Write permissions to the directory.

Procedure

1. Shut down RSA Identity Governance and Lifecycle.
2. Remove the avuser user from the database:

```
drop user AVUSER cascade;
```

3. Create the avuser user:

```
Create USER AVUSER identified by <password> profile ACMPROFILE;
```

```
ALTER USER AVUSER DEFAULT TABLESPACE DATA_1M TEMPORARY TABLESPACE TEMP;
```

4. Specify avuser privilege grants as described in "Configure the User Schema Privilege Grants" in the *Database Setup and Management Guide*.

5. Import the schema/data:

```
impdp avuser/<password>@<Oracle_SID> DumpFile=<SomeFileName>.dmp  
Directory=Avekسا_ExportImport_Directory Schemas=avuser  
LogFile=<SomeFileName>.log
```

6. If the database does not require migration, run these commands as avuser to refresh database statistics:

```
EXEC DBMS_STATS.GATHER_SCHEMA_STATS ('AVUSER') ;  
EXEC DATABASE_STATISTICS.AFTER_IMPORT;
```

If the database requires migration, you are prompted to migrate the database when you open RSA Identity Governance and Lifecycle.

7. Restart RSA Identity Governance and Lifecycle.

Verify Data Restoration and Start All Services

Perform this task to verify that data has been restored successfully and that you can start all services.

Procedure

1. Start all RSA Identity Governance and Lifecycle services:
 - a. Log in to the installation machine as the 'admin' user.
 - b. Enter the following command:

```
sudo service aveksa_server start
```
2. Log into RSA Identity Governance and Lifecycle as AveksaAdmin and verify that you have successfully imported your data.
3. If AFX is installed, start it.
4. Log out from RSA Identity Governance and Lifecycle.

Confirm the Setting for the Encryption Key Directory

The Key Encryption Key (KEK) is the key used to encrypt all other encryption keys. After installation (or upgrade), on first startup of RSA Identity Governance and Lifecycle, a unique KEK is created and stored in the encryption key directory. The default location of the directory is /home/oracle/security. If the default directory is not available or you want to set a different directory, you must create the directory, and then specify the location in a Java system variable.

Procedure

1. Log in as root.
2. Make sure you have a directory for storing the encryption key. For security purposes, the directory should have the following settings:
 - If the directory already exists, set its permissions to 700 (rwx-----) and make sure that the directory is owned by the same user under which RSA Identity Governance and Lifecycle is running.
 - If the directory does not exist, the parent directory must be writable for the user under which RSA Identity Governance and Lifecycle is running. In this case, RSA Identity Governance and Lifecycle will create the directory with the correct permissions.
 - For a cluster, this same directory also needs to exist on each of the nodes.
3. Confirm that the Java system property "rsavialg.security.keydir" is set to the appropriate directory. Use the steps for your platform in the following table to confirm or add the setting.

| Platform: | Instructions: |
|------------|---|
| Standalone | <p>The property is in aveksa-standalone-full.xml (/home/oracle/wildfly/standalone/configuration/aveksa-standalone-full.xml):</p> <pre><system-properties> <property name="rsavialg.security.keydir" value="/home/oracle/security"/> </system-properties></pre> <p>The default value for the directory is "/home/oracle/security" Change this to the directory where you will store the encryption key.</p> |
| Cluster | <p>On the Domain Controller, the property is in domain.xml (/home/oracle/wildfly/domain/configuration/domain.xml). Set the following values:</p> <pre><system-properties> <property name="rsavialg.security.keydir" value="/home/oracle/security"/> </system-properties></pre> <p>The default value for the directory is "/home/oracle/security" You should change this to the directory where you will store the encryption key</p> <p>The setting on the domain controller will be propagated to the other nodes in the cluster. Make sure you have the same encryption key directory on each of the nodes.</p> |

4. Create a secure backup process to back up the keys in the encryption key directory. RSA Identity Governance and Lifecycle generates these keys and stores them only in the designated directory.

Important: If the keys are lost, any data encrypted with those keys will be irrecoverable. The backup process should ensure that the keys are not compromised during the backup or after they are in the backup location.

Note: Anytime that you change the value of the Java system property after the keys have already been created (meaning after you configured the property and brought the system up), you must bring down the system and move the keys to the new location before bringing up the system again.

Using Non-restrictive Mode for the Encryption Key Directory

RSA recommends restricting access to the encryption key directory as stated in the previous section. If your installation cannot restrict the directory to the application owner and permissions as stated, you can implement a non-restrictive mode by using a Java system property named: `rsavialg.security.strict.permissions.disabled`.

When "`rsavialg.security.strict.permissions.disabled`" is set to be "true", restrictions on who owns the encryption key directory and what permissions are set on the directory are more flexible, but there are still requirements for permissions as described below.

Procedure

1. Add the "`rsavialg.security.strict.permissions.disabled`" property to system properties and set the value to "true" as shown for the platform type:

| Platform: | Instructions: |
|------------|--|
| Standalone | <p>The property is in <code>aveksa-standalone-full.xml</code> (<code>/home/oracle/wildfly/standalone/configuration/aveksa-standalone-full.xml</code>):</p> <pre><system-properties> <property name="rsavialg.security.keydir" value="/home/oracle/security"/> <property name="rsavialg.security.strict.permissions.disabled" value="true"/> </system-properties></pre> |
| Cluster | <p>On the Domain Controller, the property is in <code>domain.xml</code> (<code>/home/oracle/wildfly/domain/configuration/domain.xml</code>). Set the following values:</p> <pre><system-properties> <property name="rsavialg.security.keydir" value="/home/oracle/security"/> <property name="rsavialg.security.strict.permissions.disabled" value="true"/> </system-properties></pre> |

2. Change the "`rsavialg.security.keydir`" property to the directory you want to use.

- If the directory already exists, set its permissions such that the user (owner of the process under which RSA Identity Governance and Lifecycle is running) has “rwx” access into this directory. The owner of the directory need not be the same as the owner of the application process, but the owner of the application process must be able to read and write into this directory. This means “rwx” permissions have to be set for the appropriate file permission field (owner, group, all) , which will allow the application process full access.
- If the directory does not exist, it is recommended that you create it. Set up the permissions on the directory as specified in the previous item.
- If the directory does not exist and you do not create it, the application will attempt to create the directory on first startup using default permissions and the directory will be owned by the same user as the application process.

Note: Any time the value of the "rsavialg.security.strict.permissions.disabled" property is set or changed, the application server should be restarted.

Note: If "rsavialg.security.strict.permissions.disabled" is set to “false” or you remove this property, then standard “restrictive” handling for this directory will be used. If you had previously set up the directory for “non-restrictive” handling and switch to “restrictive” you must ensure this directory is set up given the requirements outlined in “Confirm the Setting for the Encryption Key Directory” (see above).

Error Messages

The following table lists error messages that might display (in the AveksaServer.log) after you configure the encryption key directory. The table lists default directory paths for the master encryption key directory (/home/oracle/security) and its parent directory (/home/oracle). The suggested actions are performed on the RSA Identity Governance and Lifecycle host.

| Message | Description | Action |
|--|---|---|
| KEK_ERROR_PARENT_DIRECTORY_DOES_NOT_EXIST | The parent directory /home/oracle for the specified encryption key storage directory /home/oracle/security does not exist. | Create the directory structure, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_PARENT_DIRECTORY_IS_NOT_WRITABLE | The parent directory /home/oracle for the specified encryption key storage directory /home/oracle/security is not writable. | Change permissions on the specified encryption key directory to allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_PARENT_IS_ | The parent /etc/hosts for the specified encryption key storage directory | Specify a directory path for the encryption key directory. |

| Message | Description | Action |
|---|--|---|
| A_FILE | /etc/hosts/security is a file, not a directory. | |
| KEK_ERROR_FILE_ALREADY_EXISTS | A file already exists with the same path as the specified encryption key storage directory /etc/hosts. | Specify a directory location, not a file location. |
| KEK_ERROR_COULD_NOT_CREATE_DIRECTORY | Could not create the encryption key storage directory /home/oracle. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_DIRECTORY_IS_NOT_WRITABLE | The encryption key storage directory /home/oracle is not writable. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_DIRECTORY_DOES_NOT_EXIST | The encryption key storage directory /home/oracle does not exist. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_INVALID_DIRECTORY_PERMISSIONS | The encryption key storage directory /home/oracle must have rwx----- (700) permissions. Please refer to the installation documentation for a system property that can be set to remove this restriction. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. Alternatively, you can set a system property to remove this restriction. See "Using Non-restrictive Mode for the Encryption Key Directory" in the previous section. |

Re-install Remote Agents

Remote agents are installed on the systems from which you collect data, for example, your Microsoft Exchange server. After upgrading to v7.0.1, you must re-install any remote agents that you are using for collections. This allows the agents to use the updated cryptographic capabilities.

Before you start

In RSA Identity Governance and Lifecycle, go to Collectors > Agents. If the agent is not running, then you must re-install.

Procedure

1. Connect to the host where the agent is installed, and then stop the agent:
 - On Linux: `service aveksa_agent stop`
 - On Windows, use the Windows Services Control Panel applet to stop the service.
2. Back up the previous version of the agent. Connect to the host where the agent is installed and copy the files to another location.

Note: The default agent, AveksaAgent, is installed in the AveksaAgent directory on the remote system.
3. Remove the agent by deleting the files from the agent directory.
4. Get the updated agent files by downloading the new archive file from the agent detail page.
 - a. Log on to the appliance where RSA Identity Governance and Lifecycle is installed, click Collectors > Agents, then select an agent.
 - b. Click Download Agent.
5. Copy the agent archive file from the download directory. Connect to the agent host and copy the archive file to the agent directory.
6. Unzip the agent file, AveksaAgent.zip for example.
7. Start the agent service as follows:
 - On Linux: `service aveksa_agent start`
 - On Windows, use the Windows Services Control Panel applet to start the service.
8. To verify that RSA Identity Governance and Lifecycle can connect to the agent, click Collectors > Agents. The status for "Is Running" should be Yes.

Restore Your Customization Files

This section describes how to restore your customization files after the upgrade that you may have saved from the your pre-7.0 version of RSA Identity Governance and Lifecycle. Customizations must be applied to the RSA Identity Governance and Lifecycle application EAR file and redeployed into the WildFly application server.

Procedure

1. Log on to your installation appliance or server as the oracle user.
2. Go to the following directory:


```
cd /home/oracle/deploy
```

3. Enter the following command:

```
customizeACM.sh -c
```

4. Answer "Yes" to expand the EAR.

5. Upload the customization files you saved before the upgrade to the following directory:

```
/tmp/customizeACM
```

6. Go to the following directory:

```
cd /home/oracle/deploy
```

7. Repack the EAR with your customization files by running the following command:

```
customizeACM.sh -d
```

Delete the Jboss Folder (When Upgrading From a Pre-v7.0 Product Version)

This task is required when you are upgrading from a pre-V7.0 version of RSA Identity Governance and Lifecycle. With the the WildFly application server, you do not require the Jboss folder or its contents from the previous product version.

Procedure

1. Log on to the installation machine as root user.
2. Change to /home/oracle.
3. Delete the jboss folder. Enter

```
rm -rf jboss
```

Upgrade RSA Identity Governance and Lifecycle on WebSphere Application Server

To complete the upgrade, perform the following steps:

1. [Deploy the WebSphere Installation EAR Files](#)
2. [Update the Setting for the Encryption Key Directory](#)
3. [Re-install Remote Agents](#)

Before you begin

In a clustered environment, consider the following:

- The deployment process requires a single connection to the database for setup and migration. Therefore, a single node only must be used during the process. Ensure that only one server instance is running and connected to the database instance. Shut down AFX if it is installed.
- After node is updated, verify that you can start RSA Identity Governance and Lifecycle and start the other nodes. For instructions managing RSA Identity Governance and Lifecycle instance nodes in the cluster, see the Help topic, "Manage Server Cluster Nodes."

Deploy the WebSphere Installation EAR Files

This section describes how to upgrade the Aveksa EAR and deploy the aveksaWFArchitect.ear file for the Workflow Architect. The Workflow Architect is used in RSA Identity Governance and Lifecycle to view and edit workflows.

Procedure

1. Download the following upgrade file to the WebSphere host:
 - a. Go to [RSA Link](https://community.rsa.com/community/products/governance-and-lifecycle) (<https://community.rsa.com/community/products/governance-and-lifecycle>), then click Log In and enter your user name and password.
 - b. Click RSA Identity Governance and Lifecycle.
 - c. Click Downloads > RSA Identity Governance and Lifecycle 7.0.1.
 - d. Click on Additional Downloads.
 - e. Click Access Certification Manager.
 - f. Click Download Software (it may take a minute to display the Product List).
 - g. Click RSA Identity Governance and Lifecycle (formerly Aveksa) - Version Upgrades. The Current tab lists the most recent release. The Archive tab lists previous releases.
 - h. Click Access Certification Manager Version 7.0SP1.
 - i. Download the following files:
 - ACM-WebSphere-<product version>.tar
2. Untar the file. Enter

```
tar xvf ACM-WebSphere <product version>.tar
```

This creates a directory named ACM-WebSphere-<version> that contains the EAR files for deployment.
3. Apply any customization changes to the EAR files if required. See "Modifying the RSA Identity Governance and Lifecycle Enterprise Archive" in the *Installation Guide* for more information.

4. Upgrade the Aveksa EAR.
 - a. From the Applications menu, click Application Types > WebSphere Enterprise Applications
 - b. Select the application and click the Update button to upload the updated EAR or WAR.
 - c. Select Replace the entire application and select the path to the replacement ACM EAR file to upload and specify the context, 'aveksa.' Continue through the wizard (choose Fast Path).
 - d. Finish installing the EAR, which may take several minutes.
 - e. Save changes to the master configuration.
5. Deploy the Workflow Architect EAR.
 - a. From Applications menu, click Application Types > Websphere Enterprise Applications, and then click Install. Continue through the wizard (choose Fast Path).
 - b. Browse to the aveksaWFArchitect.ear file in the ACM-WebSphere-<version>. The installation process continues through several pages. Accept default values where not indicated otherwise.
 - c. (Clustered environment only) Select Map Modules to Servers: Select all the modules, select the correct scope from the list of Clusters and Servers, and then click Apply. The server associated with the module should be listed as the cluster. Click Next.
 - d. In the Map Virtual Hosts for Web Modules screen, click Next.
 - e. Finish installing the EAR, which may take several minutes.
 - f. Save changes to the master configuration.
6. Restart the WebSphere application server.
7. Start the RSA Identity Governance and Lifecycle application on the single designated deployment node only in a clustered environment.
8. Log on to RSA Identity Governance and Lifecycle to verify a successful upgrade.
9. If you see the Initialization Status prompt, one or both of these cases apply:
 - The database schema is out-of-date. At the prompt, enter the password: AuthorizeMigration. The startup process migrates the database, which updates the schema.
 - Stored data needs to be re-encrypted because a key rollover was done. The startup process re-encrypts the data.

Note: If the Initialization Status displays an "Unable to check Database" error, you must restart the WebSphere server.

- Restart the RSA Identity Governance and Lifecycle application, and also restart AFX if it is installed.

Note: If the installation fails, RSA recommends that you first uninstall RSA Identity Governance and Lifecycle, restart your application server and reinstall RSA Identity Governance and Lifecycle.

Update the Setting for the Encryption Key Directory

The Key Encryption Key (KEK), is the key used to encrypt all other encryption keys. The upgrade creates a unique KEK and stores it in the encryption key directory. The default location of the directory is `/home/oracle/security`. If the default directory is not available or you want to set a different directory, you must create the directory, and then specify the location in a Java system variable.

Procedure

- Log in to the WebSphere host as administrator with root privileges.
- Make sure you have a directory for storing the key encryption key. For security purposes, the directory should have the following settings:
 - If the directory already exists, set write permissions to 700 (`rwX-----`) for the user under which RSA Identity Governance and Lifecycle is running.
 - If the directory does not exist, the parent directory must be writable for the user under which RSA Identity Governance and Lifecycle is running. In this case, RSA Identity Governance and Lifecycle will create the directory with the correct permissions.
- Set the Java system property `"rsavialg.security.keydir"` to the directory where the encryption key is stored. Perform these steps in the Admin console for WebSphere:
 - To select the server, click `Servers > Server types > WebSphere application servers > Select server`.
 - Choose the server used for RSA Identity Governance and Lifecycle.
 - Under the Configuration tab, select `Server Infrastructure > Java and Process Management > Process Definition`.
 - Under Additional Properties, select `Java Virtual Machine > Custom Properties`.
 - Select New, then enter:
Name: `rsavialg.security.keydir`
Value: `<directory path for master encryption key>`
For example, in a standalone environment:

```
rsavialg.security.keydir=<directory path for the encryption key>
```

For example, in a cluster environment:

```
rsavialg.security.keydir=<server and directory path for the master encryption key>, where server is the hostname of a common network path that is accessible from all nodes. (You could also set this up on each node by defining a local directory path on each node.)
```

4. Create a secure backup process to back up the keys that are in the encryption key directory. RSA Identity Governance and Lifecycle generates these keys and stores them only in the designated directory.

Important: If the keys are lost, any data encrypted with those keys will be irrecoverable. The backup process should ensure that the keys are not compromised, or otherwise exposed, during the backup or after they are in the backup location.

Note: Anytime that you change the value of the Java system property after the keys have already been created (meaning after you configured the property and brought the system up), you must bring down the system and move the keys to the new location before bringing up the system again.

Using Non-restrictive Mode for the Encryption Key Directory

RSA recommends restricting access to the encryption key directory as stated in the previous section. If your installation cannot restrict the directory to the application owner and permissions as stated, you can implement a non-restrictive mode by using a Java system property named: `rsavialg.security.strict.permissions.disabled`.

When "`rsavialg.security.strict.permissions.disabled`" is set to be "true", restrictions on who owns the encryption key directory and what permissions are set on the directory are more flexible, but there are still requirements for permissions as described below.

Procedure

1. In the Admin console, add a java system property named "`rsavialg.security.strict.permissions.disabled`" property and set the value to "true" as shown for the platform type:
 1. To select the server, click Servers > Server types > WebSphere application servers > Select server.
 2. Choose the server used for RSA Identity Governance and Lifecycle.
 3. Under the Configuration tab, select Server Infrastructure > Java and Process Management > Process Definition.
 4. Under Additional Properties, select Java Virtual Machine > Custom Properties.

5. Select New, then enter:

Name: `rsavialg.security.strict.permissions.disabled`

Value: `true`

2. Change the `"rsavialg.security.keydir"` property to the directory you want to use.

If the directory already exists, set its permissions such that the user (owner of the process under which RSA Identity Governance and Lifecycle is running) has “`rwX`” access into this directory. The owner of the directory need not be the same as the owner of the application process, but the owner of the application process must be able to read and write into this directory. This means “`rwX`” permissions have to be set for the appropriate file permission field (owner, group, all) , which will allow the application process full access.

If the directory does not exist, it is recommended that you create it. Set up the permissions on the directory as specified in the previous item.

If the directory does not exist and you do not create it, the application will attempt to create the directory on first startup using default permissions and the directory will be owned by the same user as the application process.

Note: Any time the value of the `"rsavialg.security.strict.permissions.disabled"` property is set or changed, the application server should be restarted.

Note: If `"rsavialg.security.strict.permissions.disabled"` is set to “`false`” or you remove this property, then standard “`restrictive`” handling for this directory will be used. If you had previously set up the directory for “`non-restrictive`” handling and switch to “`restrictive`” you must ensure this directory is set up given the requirements outlined in “`Confirm the Setting for the Encryption Key Directory`” (see above).

Error Messages

The following table lists error messages that might display after you configure the encryption key directory. The table lists default directory paths for the encryption key directory (`/home/oracle/security`) and its parent directory (`/home/oracle`). The suggested actions are performed on the RSA Identity Governance and Lifecycle host.

| Message | Description | Action |
|--|--|--|
| <code>KEK_ERROR_PARENT_DIRECTORY_DOES_NOT_EXIST</code> | The parent directory <code>/home/oracle</code> for the specified encryption key directory <code>/home/oracle/security</code> does not exist. | Create the directory structure, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key |

| Message | Description | Action |
|--|---|---|
| | | directory again. |
| KEK_ERROR_PARENT_DIRECTORY_IS_NOT_WRITABLE | The parent directory /home/oracle for the specified encryption key directory /home/oracle/security is not writable. | Change permissions on the specified encryption key directory to allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_PARENT_IS_A_FILE | The parent /etc/hosts for the specified encryption key directory /etc/hosts/security is a file, not a directory. | Specify a directory path for the encryption key directory. |
| KEK_ERROR_FILE_ALREADY_EXISTS | A file already exists with the same path as the specified encryption key directory /etc/hosts. | Specify a directory location, not a file location. |
| KEK_ERROR_COULD_NOT_CREATE_DIRECTORY | Could not create the encryption key directory /home/oracle. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_DIRECTORY_IS_NOT_WRITABLE | The encryption key directory /home/oracle is not writable. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_DIRECTORY_DOES_NOT_EXIST | The encryption key directory /home/oracle does not exist. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read |

| Message | Description | Action |
|---|--|---|
| | | from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_INVALID_DIRECTORY_PERMISSIONS | The encryption key directory /home/oracle must have rwx----- (700) permissions. Please refer to the installation documentation for a system property that can be set to remove this restriction. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. Alternatively, you can set a system property to remove this restriction. See "Using Non-restrictive Mode for the Encryption Key Directory" in the previous section. |

Re-install Remote Agents

Remote agents are installed on the systems from which you collect data, for example, your Microsoft Exchange server. After upgrading to v7.0.1, you must re-install any remote agents that you are using for collections. This allows the agents to use the updated cryptographic capabilities.

Before you start

In RSA Identity Governance and Lifecycle, go to Collectors > Agents. If the agent is not running, then you must re-install.

Procedure

1. Connect to the host where the agent is installed, and then stop the agent:
 - On Linux: `service aveksa_agent stop`
 - On Windows, use the Windows Services Control Panel applet to stop the service.
2. Back up the previous version of the agent. Connect to the host where the agent is installed and copy the files to another location.

Note: The default agent, AveksaAgent, is installed in the AveksaAgent directory on the remote system.

3. Remove the agent by deleting the files from the agent directory.
4. Get the updated agent files by downloading the new archive file from the agent detail page.
 - a. Log on to the appliance where RSA Identity Governance and Lifecycle is installed, click Collectors > Agents, then select an agent.
 - b. Click Download Agent.
5. Copy the agent archive file from the download directory. Connect to the agent host and copy the archive file to the agent directory.
6. Unzip the agent file, AveksaAgent.zip for example.
7. Start the agent service as follows:
 - On Linux: `service aveksa_agent start`
 - On Windows, use the Windows Services Control Panel applet to start the service.
8. To verify that RSA Identity Governance and Lifecycle can connect to the agent, click Collectors > Agents. The status for "Is Running" should be Yes.

Upgrade RSA Identity Governance and Lifecycle on WebLogic Application Server

To complete the upgrade, perform the following steps:

1. [Deploy the WebLogic Installation EAR Files](#)
2. [Update the Setting for the Encryption Key Directory](#)
3. [Re-install Remote Agents](#)

Before you begin

In a clustered environment, consider the following:

- The deployment process requires a single connection to the database for setup and migration. Therefore, a single node only must be used during the process. Ensure that only one server instance is running and connected to the database instance. Shut down AFX if it is installed.

- After node is updated, verify that you can start RSA Identity Governance and Lifecycle and start the other nodes. For instructions managing RSA Identity Governance and Lifecycle instance nodes in the cluster, see the Help topic, "Manage Server Cluster Nodes."

Deploy the WebLogic Installation EAR Files

This section describes how to upgrade the Aveksa EAR and deploy the aveksaWFArchitect.ear file for the Workflow Architect. The Workflow Architect is used in RSA Identity Governance and Lifecycle to view and edit workflows.

Procedure

1. Download the following upgrade file to the WebLogic host:
 - a. Go to [RSA Link](https://community.rsa.com/community/products/governance-and-lifecycle) (https://community.rsa.com/community/products/governance-and-lifecycle), then click Log In and enter your user name and password.
 - b. Click RSA Identity Governance and Lifecycle.
 - c. Click Downloads > RSA Identity Governance and Lifecycle 7.0.1.
 - d. Click on Additional Downloads.
 - e. Click Access Certification Manager.
 - f. Click Download Software (it may take a minute to display the Product List).
 - g. Click RSA Identity Governance and Lifecycle (formerly Aveksa) - Version Upgrades. The Current tab lists the most recent release. The Archive tab lists previous releases.
 - h. Click Access Certification Manager Version 7.0SP1.
 - i. Download the following files:
 - ACM-WebLogic-<product version>.tar
2. Untar the file. Enter

```
tar xvf ACM-WebLogic <product version>.tar
```

This creates a directory named ACM-WebLogic-<version> that contains the EAR files for deployment.
3. Apply any customization changes to the upgrade EAR files if required. For more information, see "Modifying the RSA Identity Governance and Lifecycle Enterprise Archive" in the *Installation Guide.V7.0.1*

4. Upgrade the Aveksa EAR :
 - a. From the WebLogic Administrative Console, click Deployments > aveksa > Delete.
 - b. Click Deployments > Install.
 - c. Browse to aveksa.ear. For example: ACM-WebLogic_<version>/aveksa.ear. The path might be different for a customized aveksa.ear.
 - d. Choose Install this deployment as an application.
 - e. Set Name to aveksa.
 - f. Choose Copy this application to every target for me under Source accessibility. Continue to the next page.
 - g. Under Additional configuration choose: No, I will review the configuration later.
5. Deploy the Workflow Architect ear:
 - a. Select Deployments > Install.
 - b. Browse to aveksaWFArchitect.ear. For example: ACM-WebLogic /aveksaWFArchitect.ear. The path may differ for a patch.
 - c. Install this deployment as an application.
 - d. Select deployment targets: the server for a standalone server environment or the cluster for a clustered environment.
 - e. Choose Copy this application to "every target for me" under Source accessibility.
 - f. In Additional configuration choose: No, I will review the configuration later.
 - g. Click Finish.
6. Restart the WebLogic application server.
7. Start the RSA Identity Governance and Lifecycle application on the single designated deployment node only in a clustered environment.
8. Log on to RSA Identity Governance and Lifecycle to verify a successful upgrade..
9. If you see the Initialization Status prompt when you start RSA Identity Governance and Lifecycle, one or both of these cases apply:
 - The database schema is out-of-date. At the prompt, enter the following password:
"AuthorizeMigration." The startup process migrates the database, which updates the schema.

- Stored data needs to be re-encrypted because a key rollover was done. The startup process re-encrypts the data.

Note: If the Initialization Status displays an "Unable to check Database" error, you must restart the WebLogic server.

10. Restart the RSA Identity Governance and Lifecycle application.

Note: If the installation fails, RSA recommends that you first uninstall RSA Identity Governance and Lifecycle, restart your application server and reinstall RSA Identity Governance and Lifecycle.

Update the Setting for the Encryption Key Directory

The Key Encryption Key (KEK) is the key used to encrypt all other encryption keys. The upgrade creates a unique KEK and stores it in the encryption key directory. The default location of the directory is /home/oracle/security. If the default directory is not available or you want to set a different directory, you must create the directory manually, and then specify the location using a Java system variable.

Procedure

1. Log in to the WebLogic host as administrator with root privileges.
2. Make sure you have a directory for storing the key encryption key. For security purposes, the directory should have the following settings:
 - If the directory already exists, set its permissions to 700 (rwx-----) and make sure that the directory is owned by the same user under which RSA Identity Governance and Lifecycle is running.
 - If the directory does not exist, the parent directory must be writable for the user under which RSA Identity Governance and Lifecycle is running. In this case, RSA Identity Governance and Lifecycle will create the directory with the correct permissions.
3. Set the Java system property "rsavialg.security.keydir" to the directory where the encryption key is stored.
4. There are two ways to set JVM arguments in WebLogic installations. These methods might not map to your environment if you use custom scripts for starting a WebLogic application server instance. See your WebLogic administrator to configure the JVM setting for your environment.

- Edit the WebLogic Domain startup environment script. This is typically done on a standalone system and is required if using the AdminServer as the instance where you are deploying RSA Identity Governance and Lifecycle.

Edit the `setDomainEnv.sh` file for the domain in which you will be deploying the RSA Identity Governance and Lifecycle application.

For example, from `$WEBLOGIC_HOME/user_projects/domains/<domain_name>/bin`, add the following settings to the beginning of the `setDomainEnv` script, where `WL_HOME` is set.

```
JAVA_OPTIONS="$JAVA_OPTIONS -Drsavialg.security.keydir=<directory path for the encryption key>"
```

```
export JAVA_OPTIONS
```

For example, in a standalone environment:

```
JAVA_OPTIONS="$JAVA_OPTIONS  
-Drsavialg.security.keydir="/wls/masterkeystorage"
```

For example, in a cluster environment:

```
JAVA_OPTIONS="$JAVA_OPTIONS -  
Drsavialg.security.keydir="/wls/masterkeystorage"
```

- Use the Administration Console to specify JVM arguments for a server instance. This is typically used if your servers are managed through NodeManager.

From the Administration Console:

1. Click Environment > Servers > Select server.
2. Click Configuration tab > Server Start tab.
3. Add the startup setting `-Drsavialg.security.keydir=<directory path for the encryption key>` to the Arguments field .

Using Non-restrictive Mode for the Encryption Key Directory

RSA recommends restricting access to the encryption key directory as stated in the previous section. If your installation cannot restrict the directory to the application owner and permissions as stated, you can implement a non-restrictive mode by using a Java system property named: `rsavialg.security.strict.permissions.disabled` .

When `"rsavialg.security.strict.permissions.disabled"` is set to be “true”, restrictions on who owns the encryption key directory and what permissions are set on the directory are more flexible, but there are still requirements for permissions as described below.

Procedure

1. Add a java system property named "rsavialg.security.strict.permissions.disabled" property and set the value to "true" as shown for the platform type:

There are two ways to set JVM arguments in WebLogic installations. These methods might not map to your environment if you use custom scripts for starting a WebLogic application server instance. See your WebLogic administrator to configure the JVM setting for your environment.

- Edit the WebLogic Domain startup environment script. This is typically done on a standalone system and is required if using the AdminServer as the instance where you are deploying RSA Identity Governance and Lifecycle.

Edit the setDomainEnv.sh file for the domain in which you will be deploying the RSA Identity Governance and Lifecycle application.

For example, from \$WEBLOGIC_HOME/user_projects/domains/<domain_name>/bin, add the following settings to the beginning of the setDomainEnv script, where WL_HOME is set.

```
JAVA_OPTIONS="$JAVA_OPTIONS -Drsavialg.security.strict.permissions.disabled=true"
export JAVA_OPTIONS
```

For example, in a standalone environment:

```
JAVA_OPTIONS="$JAVA_OPTIONS
-Drsavialg.security.strict.permissions.disabled="true"
```

For example, in a cluster environment:

```
JAVA_OPTIONS="$JAVA_OPTIONS -
Drsavialg.security.strict.permissions.disabled="true"
```

- Use the Administration Console to specify JVM arguments for a server instance. This is typically used if your servers are managed through NodeManager.

From the Administration Console:

1. Click Environment > Servers > Select server.
2. Click Configuration tab > Server Start tab.
3. Add the startup setting -Drsavialg.security.strict.permissions.disabled=true to the Arguments field .

2. Change the "rsavialg.security.keydir" property to the directory you want to use.

If the directory already exists, set its permissions such that the user (owner of the process under which RSA Identity Governance and Lifecycle is running) has “rwx” access into this directory. The owner of the directory need not be the same as the owner of the application process, but the owner of the application process must be able to read and write into this directory. This means “rwx” permissions have to be set for the appropriate file permission field (owner, group, all) , which will allow the application process full access.

If the directory does not exist, it is recommended that you create it. Set up the permissions on the directory as specified in the previous item.

If the directory does not exist and you do not create it, the application will attempt to create the directory on first startup using default permissions and the directory will be owned by the same user as the application process.

Note: Any time the value of the "rsavialg.security.strict.permissions.disabled" property is set or changed, the application server should be restarted.

Note: If "rsavialg.security.strict.permissions.disabled" is set to “false” or you remove this property, then standard “restrictive” handling for this directory will be used. If you had previously set up the directory for “non-restrictive” handling and switch to “restrictive” you must ensure this directory is set up given the requirements outlined in “Confirm the Setting for the Encryption Key Directory” (see above).

Error Messages

The following table lists the error messages that might display after you configure the encryption key directory. The table lists default directory paths for the encryption key directory (/home/oracle/security) and its parent directory (/home/oracle). The suggested actions are performed on the RSA Identity Governance and Lifecycle host.

| Message | Description | Action |
|--|---|---|
| KEK_ERROR_PARENT_DIRECTORY_DOES_NOT_EXIST | The parent directory /home/oracle for the specified encryption key directory /home/oracle/security does not exist. | Create the directory structure, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_PARENT_DIRECTORY_IS_NOT_WRITABLE | The parent directory /home/oracle for the specified encryption key directory /home/oracle/security is not writable. | Change permissions on the specified encryption key directory to allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_PARENT_IS_ | The parent /etc/hosts for the specified encryption key directory | Specify a directory path for the encryption key directory. |

| Message | Description | Action |
|---|--|---|
| A_FILE | /etc/hosts/security is a file, not a directory. | |
| KEK_ERROR_FILE_ALREADY_EXISTS | A file already exists with the same path as the specified encryption key directory /etc/hosts. | Specify a directory location, not a file location. |
| KEK_ERROR_COULD_NOT_CREATE_DIRECTORY | Could not create the encryption keydirectory /home/oracle. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_DIRECTORY_IS_NOT_WRITABLE | The encryption key directory /home/oracle is not writable. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. |
| KEK_ERROR_DIRECTORY_DOES_NOT_EXIST | The encryption key directory /home/oracle does not exist. | Create the directory, set permissions to allow RSA Identity Governance and Lifecycle to read from and write to the directory, and specify the encryption key directory again. |
| KEK_ERROR_INVALID_DIRECTORY_PERMISSIONS | The encryption key directory /home/oracle must have rwx----- (700) permissions. Please refer to the installation documentation for a system property that can be set to remove this restriction. | Verify that directory permissions allow RSA Identity Governance and Lifecycle to write to the directory. Alternatively, you can set a system property to remove this restriction. See "Using Non-restrictive Mode for the Encryption Key Directory" in the previous section. |

Re-install Remote Agents

Remote agents are installed on the systems from which you collect data, for example, your Microsoft Exchange server. After upgrading to v7.0.1, you must re-install any remote agents that you are using for collections. This allows the agents to use the updated cryptographic capabilities.

Before you start

In RSA Identity Governance and Lifecycle, go to Collectors > Agents. If the agent is not running, then you must re-install.

Procedure

1. Connect to the host where the agent is installed, and then stop the agent:
 - On Linux: `service aveksa_agent stop`
 - On Windows, use the Windows Services Control Panel applet to stop the service.
2. Back up the previous version of the agent. Connect to the host where the agent is installed and copy the files to another location.

Note: The default agent, AveksaAgent, is installed in the AveksaAgent directory on the remote system.
3. Remove the agent by deleting the files from the agent directory.
4. Get the updated agent files by downloading the new archive file from the agent detail page.
 - a. Log on to the appliance where RSA Identity Governance and Lifecycle is installed, click Collectors > Agents, then select an agent.
 - b. Click Download Agent.
5. Copy the agent archive file from the download directory. Connect to the agent host and copy the archive file to the agent directory.
6. Unzip the agent file, AveksaAgent.zip for example.
7. Start the agent service as follows:
 - On Linux: `service aveksa_agent start`
 - On Windows, use the Windows Services Control Panel applet to start the service.
8. To verify that RSA Identity Governance and Lifecycle can connect to the agent, click Collectors > Agents. The status for "Is Running" should be Yes.

Upgrade AFX

When AFX is also installed on your appliance, RSA Identity Governance and Lifecycle automatically upgrades AFX whenever you upgrade RSA Identity Governance and Lifecycle using the `-afx` option with `install.sh` (`install.sh -afx`). Otherwise, you are required to complete the tasks in this section to successfully upgrade AFX in other RSA Identity Governance and Lifecycle deployment scenarios.

Perform the tasks in this section only if you are upgrading from v6.8.1 or later. If you are upgrading from a pre-v6.8.1 version of RSA Identity Governance and Lifecycle, see [Upgrade AFX If You Have a Pre-6.8.1 Version Installed](#) for instructions.

Before you begin

Perform the following before you upgrade AFX

- Stop all AFX servers.
Example 1: `/home/afxuser/AFX/afx stop`
Example 2: `/home/oracle/AFX/afx stop`
- Upgrade RSA Identity Governance and Lifecycle.

Procedure

1. Start all AFX servers:
 - a. Connect to the AFX server machine using the “afx account.”
 - b. Start AFX using the “afx” admin script located in the top level AFX installation directory:
`<path-to-AFX>/afx start`
Example 1: `/home/afxuser/AFX/afx start`
Example 2: `/home/oracle/AFX/afx start`
2. Monitor the upgrade status.
 - To confirm the upgrade is in progress, see the `/home/oracle/AFX/esb/logs/AFX-INIT.log` file. Look for the "Initiating server upgrade" entry.
 - To view upgrade steps that have been completed and to confirm that the upgrade was successful, see the `/home/oracle/AFXServer-upgrade/afx-server-upgrade-<timestamp>.log` file. Look for the "Success" entry.
3. Download the AFX connectors and templates package for the RSA Identity Governance and Lifecycle product upgrade or patch version from RSA Link.
For example: `AFX-<product version>-Standard-Connectors.zip`
4. Log in to RSA Identity Governance and Lifecycle and do the following.
 - a. From AFX > Import, select the package and import all files in the package.
 - b. From AFX > Connector Templates, verify that your template versions match the RSA Identity Governance and Lifecycle product version you installed.
 - c. From AFX > Connectors, verify that the status of your connectors is "Running."

For more information on working with AFX, see online Help.

Upgrade AFX If You Have a Pre-6.8.1 Version Installed

This section describes how to upgrade your existing AFX installation to version 7.x. This process consists of the following tasks:

- [Migrate AFX Connectors and Templates from AFX 2.0.x or 2.5.x](#)
- [Upgrade the AFX Server to Version 7.x](#)

Migrate AFX Connectors and Templates from AFX 2.0.x or 2.5.x

All AFX 7.x (and 2.9.x) data, including connector templates and connector files, are stored in the RSA Identity Governance and Lifecycle database. Data from versions 2.0.x and 2.5.x was stored on the AFX server machine. To load connectors and templates from these versions into the RSA Identity Governance and Lifecycle database, do the following:

1. [Run the AFX Connector Converter Utility.](#)
2. [Import the Connector and the Connector Template Packages Archives into RSA Identity Governance and Lifecycle v7.x.](#)

Run the AFX Connector Converter Utility

The Connector Package File Migration utility generates a new connector package zip file that contains the connectors and a template zip file that contains the templates. You can then import the zip files into the RSA Identity Governance and Lifecycle database.

Procedure

1. Connect to your AFX server machine as root user.
2. Stop the AFX Server if it is running.
3. Back up the existing AFX installation by copying the current AFX install directory and all of its contents. For example, if your current AFX installation is located at /opt/AFX:

```
cp -rpf /opt/AFX /opt/AFX-backup
```
4. Choose a download directory on the AFX server machine (/tmp for example).
5. Download AFX-`<product-version>`-Connector-Converter.zip from the packages directory for this RSA Identity Governance and Lifecycle release version.
6. Change to the download directory and expand the connector converter zip file:

```
cd /tmp
```
7. Unzip AFX-`<product-version>`-Connector-Converter.zip.
This creates an AFXConverter directory that includes all of the components required to run the utility.

8. Change to the AFXConverter directory and run the utility with required inputs provided for the Mule installation directory and output destination directory. The name of the Mule installation directory depends on the AFX version that is currently installed. For example, if AFX is installed in /opt/AFX and output is to be saved to /tmp/AFXConverter/output:

- For AFX 2.0.x installations:

```
cd /tmp/AFXConverter
./afx_connector_converter.sh /opt/AFX/mule-ee-3.2.1
/tmp/AFXConverter/output
```

- For AFX 2.5.x installations:

```
cd /tmp/AFXConverter
./afx_connector_converter.sh /opt/AFX/mule /tmp/AFXConverter/output
```

9. After the utility has completed, find the following files in the output directory and copy them to a system from which you can access the RSA Identity Governance and Lifecycle application via a web browser:

- /tmp/AFXConverter/output/AFXConnectorTypePackages.zip (contains connector templates and supporting files)
- /tmp/AFXConverter/output/AFXConnectorPackages.zip (contains connectors and supporting files)

Import the Connector and the Connector Template Packages Archives into RSA Identity Governance and Lifecycle v7.x

After you complete the steps in [Run the AFX Connector Converter Utility](#) to generate the packages archive of your previous release, import the archive into to RSA Identity Governance and Lifecycle 7.x.

Procedure

1. Log on to RSA Identity Governance and Lifecycle as an administrator user, AvekseAdmin for example.
2. Click AFX > Import.
The Import Connector Package page appears.
3. Click Browse, select the AFXConnectorTypePackages.zip file, select Select All Items and then click Next to import it.
4. Click Browse, select the AFXConnectorPackages.zip file, select and then click Next to import it.

The connector template and connector packages are loaded into the RSA Identity Governance and Lifecycle database.

5. After you have imported the packages archives, you must download and import the AFX 7.x connector packages included in the RSA Identity Governance and Lifecycle release. This step is required to migrate your connectors and templates to ensure compatibility with an AFX 7.x server installation. See "Install the AFX Connector Packages" in the *Installation Guide*.

Important: For security reasons, values for password settings are not included in the connector packages generated by the converter utility and thus are not populated for the connectors that were imported/migrated. You must edit each connector and update the value for any password setting after you install the connector packages.

Upgrade the AFX Server to Version 7.x

This section describes how to upgrade the AFX server to version 7.x. To upgrade your AFX server, you must first uninstall the existing AFX server version and then install version 7.x.

Procedure

1. Connect to the AFX server machine as root user.
2. Stop the AFX server if it is running.
3. Back up your existing AFX installation by copying the current AFX install directory and all contents. For example, if your current AFX installation is located at /opt/AFX:

```
cp -rpf /opt/AFX /opt/AFX-backup
```
4. Remove your existing AFX deployment:
 - If upgrading from a pre-2.8.1 version, perform the uninstall procedure documented in the *Access Fulfillment Express Guide* for the AFX server version you have currently installed. See the "Uninstall the AFX Server" section.
 - If upgrading from a 2.8.x version or greater, disable AFX from Admin > System > Settings. For more information, see *Specifying System Settings* in Help.
5. Delete the existing AFX install directory and all of its contents. For example, if your current AFX installation is located in /opt/AFX:

```
rm -rf /opt/AFX
```
6. Disconnect from the AFX server machine and follow the steps in "Installing the AFX Server" in the *Installation Guide* to install AFX Server version 7.x.

Verify the Upgrade

Services are automatically restarted after you upgrade RSA Identity Governance and Lifecycle. You are not required to start services manually.

Procedure

1. Check the upgrade log files (/tmp/aveksa-install.log) to ensure there are no problems indicated by a “Step failed” message.

The installation process involves installation of several components. Log output varies depending on whether you performed a new or upgrade installation. “Step failed” messages indicate where the problem occurred.

You can ignore the following output from the Oracle installer:

```
CRS-4000: Command Start failed, or completed with errors.  
PRCR-1079 : Failed to start resource ora.asm  
[WARNING] [INS-41812] OSDBA and OSASM are the same OS group.  
ORA-01078: failure in processing system parameter
```

Note: For more information on system-generated error messages, see the "Troubleshooting" appendix in the *Installation Guide*.

2. Log on to RSA Identity Governance and Lifecycle and complete the following tasks:
 - Verify various screens to ensure they are functioning properly.
 - Run various tasks, such as collections, reviews, reports, and rules.