Migrating ESM Resources From Oracle to CORR-Engine

ESM 5.5 P1 to ESM 6.5c SP1

April 21, 2014

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
4/21/2014	ESM with CORR-Engine 6.5c SP1	Describes how to migrate ESM Resources from ESM 5.5 P1 to ESM 6.5c SP1

Contents

Migrating ESM Resources From Oracle to CORR-Engine

This document tells you how to migrate the ESM resources from ESM 5.5 to ESM 6.5c SP1.

The goal of this migration is to help you migrate your content from the Oracle database to CORR-Engine.

Migration Overview

The migration path suported for this release is from ESM 5.5 Patch 1 (or greater) to ESM 6.5c SP1.

To migrate Oracle-based ESM 5.5 Patch 1 resources, follow these two steps, in order:

1 Install ESM 6.5c SP1 on a machine other than your ESM 5.5 Patch 1 machine. Refer to the ESM 6.5c SP1 Installation and Configuration Guide for instructions.

2 Migrate resources from the ESM 5.5 Patch 1 installation to the freshly-installed ESM 6.5c SP1 on which the resources have not been altered or added.

Important! Any resources changed or added after installation along with their associations with any events are wiped out when migrating the resources. This document will assist you in this step.

What is and is Not Migrated

Consider the following before you migrate:

- Migration of content is only supported to a **freshly** installed ESM 6.5c SP1 installation.
- The following are **not** migrated:
  - Event data
  - Case event data
  - Trend data - Trend tables are not migrated as part of data migration tool as these tables can have large amount of data. Trend tables are recreated on the system when the trend runs first time based on the schedule. Wait for the first scheduled run of a trend before running a query on the trend.
  - Domain fields - These fields migrate, but actions on the data won't work because the Domains feature is not supported on the CORR-Engine. Rule actions won't fire on domain fields and channels with domain fields won't have values.
  - Imported KB articles - These reside on the file system and are outside the database, so they are not migrated.

Migration Log Files

The migration tool creates the `ResourceMigration.log` file, which logs the actual schema and data transfer process. The file is located in

`/opt/arcsight/resourcemigration/logs/ResourceMigration.log`.

The `ResourceMigration.log` file is overwritten each time you run the migration tool.

The upgrade wizard, which is part of the migration process, creates two log files, `server.upgrade.log` and `server.upgrade.std.log`, located in `/opt/arcsight/manager/logs/upgrade`.

These logs are helpful for troubleshooting, if you run into issues while running the tool.

Excluding Resources from Being Migrated

> **Caution** MySQL 5.1 supports 1024 partitions. If a table you are migrating has more than 1024 partitions, the migration fails and you get an error that too many partitions were defined. To resolve this issue, exclude tables that have over 1024 partitions by adding the table name to the `SqlQueryPattern.xml` file located in `/opt/arcsight/resourcemigration/config` directory.

When migrating your resources from Oracle to CORR-Engine, there may be some tables in your Oracle database that you may not want to transfer. You can configure the tool to exclude such tables. The `<pattern>` tag in the `/opt/arcsight/resourcemigration/config/SqlQueryPattern.xml` file defines which tables get migrated. Should you need to modify this tag to either include additional tables or exclude tables that are already included, the migration tool provides means to exclude an Oracle table during transfer. For details, contact HP by sending an email to arstresourcemigrationtool@hp.com *before* you do so.

Before Running the Migration Tool

Important! Keep in mind that both source (ESM with Oracle) and destination (ESM with CORR- Engine) must be installed in the same mode (FIPS mode or default mode) and they must use the same authentication parameters (Password Based or SSL, etc.).

Have the source and destination environments ready by following the steps below.

Source machine (where Oracle is installed):

- Shut down the Manager and ArcSight Web.

  On Unix machines:

  Run the following command to stop ArcSight Web:

  `/etc/init.d/arcsight_web stop`

  Run the following command while logged in as the **superuser** in order to stop the ArcSight Manager:

  `/etc/init.d/arcsight_manager stop`

  On Windows:

  When not running as a service, press Ctrl-C in the command window where the ArcSight Manager or ArcSight Web is running.

- **Important!** Make sure that Oracle is up and running.

- Edit the `<ORACLE_HOME>/network/admin/sqlnet.ora` file to add your destination machine's IP address to the `TCP.INVITED_NODES` field.

- Restart the TNS listener by running the following command on Unix machines:

  `/etc/init.d/tnslistener restart`

On Windows, you must stop and then start the TNS Listener service.

■ Some tables are dynamically created (for instance Active List, Session List, and Trends). The column names for such tables depend on input from you. Make sure that your tablenames in Oracle do not contain any special characters. Special characters are not permitted for table names in MySQL, because table names are mapped to actual file names in the operating system. So any character (or even character sequence) that is not permitted in the operating system's file system can not be used in a table name.

■ Make sure that you have the location of the Firefox browser listed in your path environment variable.

■ Make sure archived report definitions are not saved in the database. If reports are saved in the database, download the BLOB files for them to the system file, and then remove them from database before you run the resource migration.

■ The size of BLOB/CLOB objects such as reports, or configuration files or any other BLOB/CLOB files saved in database, must not exceed 125 MB. If they do, copy them to your file system and removed them from the database before you begin the migration process. To see the size of such objects:

a Find all the tables in 'arcsight' schema.

b Select all the tables that have blob columns.

c Find the length of each blob column in each table.

Refer to the Oracle documents for details on the above steps.

■ The Resource Validation command `resvalidate` will list any invalid resources, such as resources that depend on another resource that is no longer present. This list has two uses: it identifies ones you may want to fix and it is a baseline report so you can find resources that were invalidated by the migration.

a Run the `resvalidate` command the first time with `-persist true` (the default) to validate and fix invalid resources. There is a chance that some invalid resources could be missed the first time.

```
arcsight resvalidate
```

b Then run the resvalidate script a second time with '-persist false' to generate an accurate report:

```
arcsight resvalidate -persist false
```

(You should always run the `resvalidate` command a twice, in this way.)

Destination machine (ESM 6.5c SP1):

■ Your machine must have at least 500 MB of free space.

■ Make sure that the destination system can access the Oracle database on the source system.

■ If you have a very large number of resources, the default 6 GB of heap size on the Manager may not be sufficient to handle the load. To work around this issue, set ARCSIGHT_JVM_OPTIONS environment variable to the desired heap size before you run the migration tool. For instance,

```
ARCSIGHT_JVM_OPTIONS="-Xms4096m –Xmx8192m".
```

■ Your destination machine should have a **freshly installed** ESM 6.5c SP1, where no live events have been processed or other resources created. The resource migration overwrites all data on the destination system. In other words, all resources created on the destination system before migration will be lost.

- If you have large Active Lists and Session Lists (entries in millions) that need to be migrated, you must add the following properties in /opt/arcsight/manager/config/server.properties on the **destination** machine in order to avoid data loss:

  ```
  sessionlist.max_capacity=<max_entry_in_SessionList>

  activelist.max_capacity=<max_entry_in_ActiveList>
  ```

- Shut down the ArcSight Manager and ArcSight Web.

Case Customization

If you have done any case customizations on the source ESM system, contact HP by sending an email to arstresourcemigrationtool@hp.com before proceeding with the resource migration.

Running the Tool

New in ESM 6.5c SP1, the arcsight_services command should no longer be run as /sbin/service arcsight_services. It should now be run as /etc/init.d/arcsight_services.

The Migration Tool must be run on the **destination** machine.

1 Log in as user "arcsight" on your destination system that has ESM 6.5c SP1 installed on it.

2 Stop ArcSight Web by running:

   ```
   /etc/init.d/arcsight_services stop arcsight_web
   ```

3 Stop the ArcSight Manager by running:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

4 Download the following file on your destination machine:
   ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin

   where x.x.x stands for the migration tool version number.

5 Give file ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin execute permission. To do so, enter:

   ```
   chmod +x ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin
   ```

6 Run the downloaded file. You can run it in GUI mode or console mode. If you do not have X Windows installed, it automatically runs in console mode.

   ```
   ./ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin
   ```

7 Follow the prompts on the screens.

8 After the installation completes, open this file:
   /opt/arcsight/resourcemigration/config/Config.databases.properties.

9 Edit the properties as follows and save the file:

> **Note**
> You only need to change the credentials to the source and destination systems and source database instance name if it is other than "arcsight". Accept the default values for the remaining properties.

```
sourceServerName=<IP address or hostname of the machine that has
Oracle on it>
```

```
sourceSchema=<Oracle database instance name>
```

```
sourcePortNumber=1521
```

```
sourceUserName=<"oracle" user's username (usually "arcsight")>
```

```
*sourcePassword=
```

* Delete the default text in the file and leave this property blank.

```
targetServerName=127.0.0.1
```

> **Caution**
> Do not change the IP for the `targetServerName` field. By default, it is set to 127.0.0.1.

```
targetSchema=arcsight
targetPortNumber=3306
targetUserName=arcsight
**targetPassword=
```

** Delete the default text in the file and leave this property blank.

```
validation=Yes
transferData=Yes
preSql=Yes
postSql=Yes
disableKeys=Yes
parallel=Yes
maxLobSize=125 MB<max size of record in any MySQL table>
skipDDLSpecialChars=Yes
useFreeMemOnly=Yes
```

10 Verify that Logger, MySQL and postgresql are up by running:

```
/etc/init.d/arcsight_services status all
```

If they are not running, be sure to start them.

To start the postgresql, run:

```
/etc/init.d/arcsight_services start postgresql
```

To start MySQL, run:

```
/etc/init.d/arcsight_services start mysqld
```

To start the Logger services, run:

```
/etc/init.d/arcsight_services start logger_httpd
/etc/init.d/arcsight_services start logger_servers
/etc/init.d/arcsight_services start logger_web
```

11 If running, stop the following components:

◆ ArcSight Web

```
/etc/init.d/arcsight_services stop arcsight_web
```

◆ ArcSight Manager

```
/etc/init.d/arcsight_services stop manager
```

> **!**
> **Caution**
>
> **Important! --** If you run the migration from a remote system connected to the appliance, have X-Windows running on your remote system and use ssh -X to run the migration.

12 Run the Resource Migration tool:

a The tool checks to make sure that the version of the database schema on your source machine is listed in the `/opt/arcsight/resourcemigration/config/Version.properties` file. It compares only the major, minor, and service pack version of the version number. For example, if the version number is 5.5.0.xxxx.x, it will compare only 5.5.0 and ignore the rest.

b From the `bin` directory of the Resource Migration tool (by default `/opt/arcsight/resourcemigration/bin`), run the following:

```
./arcsight_resourcemigration.sh
```

13 Check the `ResourceMigration.log` file. If you find any errors listed, resolve them before proceeding. If you are unable to fix an issue, contact HP for help by sending an email to arstresourcemigrationtool@hp.com. Then, follow Step 12 again.

14 Verify that the migration was successful by checking two things:

◆ The Upgrade Wizard's report located in `/opt/arcsight/manager/upgrade/out/<date-time>/summary.html`

◆ The wizard's log in `/opt/arcsight/manager/logs/upgrade`.

15 Start the Manager by running:

```
/etc/init.d/arcsight_services start manager
```

16 Start ArcSight Web by running:

```
/etc/init.d/arcsight_services start arcsight_web
```

Resource Migration in a Hierarchical Setup

A hierarchical setup is where data from one or more source ArcSight Managers is forwarded to a central, destination ArcSight Manager.

To migrate resources in a hierarchical setup, first migrate the resources on the upper-most level Managers one at a time. For each Manager, follow the directions in all the sections above. The next step is to migrate the resources on all ArcSight Managers at the next-level down in the hierarchy until all Managers at each level of the hierarchy have been upgraded.

Troubleshooting

Here are some tips for troubleshooting the following issues.

■ **Errors when running the migration tool**

If there are errors when running the migration tool, the tool terminates. If you encountered the error while running the wizard, check the log file for the wizard. Try to fix the issue, then rerun the wizard.

If you encountered the error during the actual resource migration (after you run `./arcsight_resourcemigration.sh` command), find the problem in the log file (`ResourceMigration.log`), try to fix it, and then rerun the `arcsight_resourcemigration.sh` command.

If you are unable to fix the issue, contact HP for help with it by sending an email to arstresourcemigrationtool@hp.com.

■ **Error when running the content upgrade**

The resource migration tool first migrates your resources and then upgrades the content.

Look for the line, "`Data migration tool ends`" in the `ResourceMigration.log` file. That means your resources have been migrated successfully and the content upgrade has begun. If there is an error while upgrading your content, run the Content (Core and Foundation packages) upgrade (**while logged in as "arcsight" user**) from the Manager's `bin` directory (`/opt/arcsight/manager/bin`) on the destination machine to bring the schema and the standard content up to ESM 6.5c SP1 requirements:

```
./arcsight upgrade manager -m -i silent -f /dev/null
```

■ **Trends-related error message**

Immediately after resource migration, if you view the Trend, you see the following error:

```
Persistence Exception. Unable to execute query.Table Trend***
doesn't exist.
```

This is because the trend data does not get migrated and there is no trend data available immediately after the resource migration. Once the trend runs, it backfills the data, this issue is automatically resolved, and trends work normally.

■ **Out of memory errors when migrating resources**

This can happen when you have a very large number of resources and the default 6 GB of heap size is insufficient to handle the load. To work around this issue, set ARCSIGHT_JVM_OPTIONS environment variable to the desired heap size, then run the tool again. For instance,

```
ARCSIGHT_JVM_OPTIONS="-Xms4096m –Xmx8192m".
```

Post-Migration Issues

■ After the resource migration completes, the latitude values for `ARC_LOCATION` get truncated and appear as a double value in MySQL. The in-memory value may not match the value in the database, especially if some of these values get stored in Active Lists and Session Lists.

■ The Reference ID for a resource changes after the resource migration, so if any resource (for example, Filters) refers to another resource by its Reference ID, the referring resource needs to be manually updated to use the new Reference ID.

- Make sure to re-register your remotely installed connectors with the Manager.

- The Resource Validation report generated at the end of the upgrade process may have some invalid resources. As a workaround, run the resource validation script manually after the upgrade finishes:

    a Run the `resvalidate` command the first time with `-persist true` (the default) to validate and fix invalid resources. There is a chance that some invalid resources could be missed the first time.

    ```
    arcsight resvalidate
    ```

    b Then run the resvalidate script a second time with '-persist false' to generate an accurate report:

    ```
    arcsight resvalidate -persist false
    ```

    Look for any resources that were valid on the source system before the migration, but are invalid now. One possible reason for an invalid resource is that a dependent resource is missing. You can often restore the missing resource by installing the package that contains it. If you do not want that package installed you can uninstall it again, and the missing resource remains and the invalid resource remains valid.

- Once you have completed resource migration, review the enabled Pattern Discovery schedules and disable or reduce any unneeded schedules. This frees system resources and can help yield a higher EPS rate.

- There are two packages that are present in the migration-destination system that are not installed by default.

    All Packages/ArcSight Administration/ArcSight Admin DB CORR
    All Packages/ArcSight Administration/ArcSight Search Filters

    To use these packages, install them manually.

- File resources are not always handled properly during the ESM migration. This results in unassigned file resources after the migration. For example, the .art files are created as new file resources in ESM 6.5c SP1, and the resources get new version IDs during the migration. The original files are stored in the Files resource under the Unassigned folder. To work around this issue, you can safely delete the unassigned .art files after migration because they are duplicates.

Uninstalling the Tool

To uninstall the tool, run the following command from `/opt/arcsight/resourcemigration/UninstallerData` directory:

```
./Uninstall_ArcSight_Resource_Migration
```

This uninstaller does not uninstall the logs folder or log files. By default the folder is:

```
/opt/arcsight/resourcemigration/logs.
```

After running the uninstaller, delete this folder and the files in it manually.