CyberRes

Product Guide

ArcSight ESM Upgrading Guide

A comprehensive guide covering necessary steps to upgrade ArcSight ESM version 6.9.1 to the current released version (7.5).

Upgrading ArcSight ESM

This document provides comprehensive instruction to complete an upgrade starting at ESM 6.9.1 up to ESM 7.5. Each section provides the minimal number of steps necessary to ensure a successful upgrade. Failure to complete each step may result in a failed upgrade or extended times to troubleshoot and complete upgrades.

Overview

This document is designed to facilitate upgrades from ArcSight Enterprise Security Manager (ESM) 6.9.1 to the current released version (7.5), including the necessary operating system upgrades. After you have upgraded to the current version, Micro Focus recommends following the procedures in the Upgrade Guide for ESM to perform future upgrades.

Note: Micro Focus has provided estimated times to complete the individual steps throughout the upgrade. These times were performed in a lab environment with typical event and content data. The provided times are highly dependent on environmental variables such as system performance, amounts of data present within ArcSight, and other factors. Actual times in a specific customer production environment will vary.

Total end-to-end time to upgrade from 6.9.1 to 7.5 in the Micro Focus lab environment: 5 hours

Before Performing Each Version Upgrade

The following steps are required before performing each version upgrade.

1. Back up the `/opt/arcsight` directory.

   If you do not want to back up events and archives, you can exclude the following directories from the backup:

   - `/opt/arcsight/logger/data/archives`
   - `/opt/arcsight/logger/data/indexes`
   - `/opt/arcsight/logger/data/logger`

   Note: After you restore the backup, ensure that the /opt/arcsight/logger/data/logger/ directory exists before you start the services.

2. Stop the Manager and run the `resvalidate` command.

3. Export system tables.

   Because the export generates a large file, Micro Focus recommends running the following command and backing up the resulting `.gz` file:

   ```
   gzip /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql
   ```

4. If needed, export trends. As user `arcsight`, run the following commands:

   ```
   DBTODUMP=arcsight
   SQL="SET group_concat_max_len = 10240;"
   SQL="${SQL} SELECT GROUP_CONCAT(table_name separator ' ')"
   SQL="${SQL} FROM information_schema.tables WHERE table_schema='${DBTODUMP}'"
   SQL="${SQL} AND (table_name like 'arc_trend%');"
   TBLIST=`/opt/arcsight/logger/current/arcsight/bin/mysql -u arcsight -p <mysql_password> -AN -e"${SQL}"`
   /opt/arcsight/logger/current/arcsight/bin/mysqldump -u arcsight -p ${DBTODUMP} ${TBLIST} > /tmp/arcsight_trends.sql
   ```

   When the export is complete, copy the `.sql` file to the same backup location as the other files you backed up.

5. Back up configuration data by executing the following command:

   ```
   /opt/arcsight/logger/current/arcsight/logger/bin/arcsight configbackup
   ```

   This creates the file:

   ```
   /opt/arcsight/logger/current/arcsight/logger/tmp/configs/configs.tar.gz.
   ```

   Copy this file to the same location as the other files you backed up.

Upgrading from ESM 6.9.1 and RHEL/CentOS 7.1 to ESM 6.9.1 Patch 3

Approximate time to upgrade to ESM 6.9.1 Patch 3: 12 minutes

1. As user `arcsight`, stop the Manager

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

2. As user `arcsight`, run the `resvalidate` command and fix any issues that it reports. To reduce the amount of time it takes to run `resvalidate`, increase the java heap size as well as the cache size for zones (there are 39909 zones). The cache size should be appropriate for the number of filters/zones. For example, if you have 200,000 zones, you can increase the cache size to 200K. Ensure that you increase the heap size accordingly.

   Add the following properties to the `server.properties` file:

   ```
   resource.broker.cache.size.Filter=2500
   resource.broker.cache.size.Zone=40000
   ```

   Execute the following commands:

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate
   -persist false
   ```

3. Copy `ArcSightESMSuitePatch-2137.tar` to your preferred location and untar it as user arcsight
4. Stop all ArcSight services

   ```
   service arcsight_services stop all
   ```

5. As user `arcsight`, start the install by executing the patch binary

   ```
   cd <location of patch>
   ./ArcSightESMSuitePatch.bin
   ```

6. As user `arcsight`, start all services

   ```
   service arcsight_services start all
   ```

7. Upgrade the ArcSight Console to ESM 6.9.1

Upgrading from RHEL/CentOS 7.1 and ESM 6.9.1 Patch3 to RHEL/CentOS 7.3 and ESM 6.11

Approximate time to upgrade to RHEL 7.3 and ESM 6.11: 68 minutes

Important: If there are large trends with IP addresses, the upgrade process might take longer to complete. Review your trends before starting the upgrade and delete or truncate the trend data if it is not used.

Run the following SQL query to list the largest trends:

```
mysql> select table_name, table_rows from
information_schema.tables where table_name like
'arc_trend_%' order by table_rows desc limit 10;
```

1. As user `arcsight`, stop the Manager

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

2. As user `arcsight`, run the`resvalidate` command and fix any issues that it reports

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate
   -persist false
   ```

3. As user `arcsight`, export system tables

   ```
   /opt/arcsight/manager/bin/arcsight export_
   system_tables <username> <password> <dbname> -s
   ```

4. As user `arcsight`, back up configuration data

   ```
   /opt/arcsight/logger/current/arcsight/logger/
   bin/arcsight configbackup
   ```

5. As user `arcsight`, backup archive data

   ```
   /opt/arcsight/logger/current/arcsight/bin/pg_
   dump -d rwdb -c -n data -U web |gzip -9 -v > /
   tmp/postgres_data.sql.gz
   ```

6. As user `root`, stop all services

   ```
   service arcsight_services stop all
   ```

7. Upgrade the operating system to RHEL/CentOS 7.3 and reboot when complete
8. Verify that all services are available

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

9. Download `ArcSightESMSuite-6.11.0.2149.0.tar` and untar it as user `root`
10. As user `root`, stop the services

    ```
    Tools/stop_services.sh
    ```

11. As user `arcsight`, begin the upgrade by executing the installer

    ```
    ./ArcSightESMSuite.bin
    ```

12. As user `root`, set up the services

    /opt/arcsight/manager/bin/setup_services.sh

13. Ensure that all services are running and the version is correct

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

14. Upgrade the ArcSight Console to ESM 6.11
15. Optionally, upgrade the connectors

Upgrading from ESM 6.11 to ESM 6.11 Patch 3

Approximate time to upgrade to ESM 6.11 Patch 3: 10 minutes

1. Download `ArcSightESMSuitePatch-2260.tar` and untar it as user `arcsight`.
2. As user `arcsight`, stop the services

   ```
   service arcsight_services stop all
   ```
3. As user `arcsight`, begin the upgrade by executing the installer

   ```
   ./ArcSightESMSuitePatch.bin
   ```
4. As user `arcsight`, start the services

   ```
   service arcsight_services start all
   ```
5. Upgrade the ArcSight Console to ESM 6.11.3

Upgrading from ESM 6.11 Patch 3 to RHEL/CentOS 7.4 and ESM 7.0 Patch 1

Approximate time to upgrade to RHEL 7.4 and ESM 7.0 Patch 1: 63 minutes

1. As user `arcsight`, stop the Manager

   ```
   /etc/init.d/arcsight_services stop manager
   ```
2. As user `arcsight`, run the `resvalidate` command and fix any issues that it reports

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate
   -persist false
   ```
3. As user `arcsight`, export system tables

   ```
   /opt/arcsight/manager/bin/arcsight export_
   system_tables <username> <password> <dbname> -s
   ```
4. As user `arcsight`, back up configuration data

   ```
   /opt/arcsight/manager/bin/arcsight export_
   system_tables <username> <password> <dbname> -s
   ```
5. As user `arcsight`, backup archive data

   ```
   /opt/arcsight/logger/current/arcsight/bin/pg_
   dump -d rwdb -c -n data -U web |gzip -9 -v > /
   tmp/postgres_data.sql.gz
   ```
6. As user `root`, stop all services

   ```
   service arcsight_services stop all
   ```
7. Upgrade the operating system to RHEL/CentOS 7.4 and reboot the system
8. Verify that all services are available

   ```
   /etc/init.d/arcsight_services status
   ```
9. Download `ArcSightESMSuite-7.0.0.2234.1.tar` and untar it as user `root`
10. As user `root`, stop the services

    ```
    Tools/stop_services.sh
    ```
11. As user `arcsight`, install the binary and complete the upgrade

    ```
    ./ArcSightESMSuite.bin
    ```
12. As user `root`, set up the services

    ```
    /opt/arcsight/manager/bin/setup_services.sh
    ```
13. Ensure that all services are running and the version is correct

    ```
    /etc/init.d/arcsight_services status
    ```
14. Upgrade the ArcSight Console to ESM 7.0.1
15. Optionally, upgrade the connectors

Upgrading from ESM 7.0 Patch 1 to RHEL/CentOS 7.7 and ESM 7.2

Approximate time to upgrade to ESM 7.2: 1 hour

Note: This ESM upgrade includes an upgrade of MySQL from version 5.1.24 to version 5.7.21.

1. As user `arcsight`, stop the Manager

   ```
   /etc/init.d/arcsight_services stop manager
   ```
2. As user `arcsight`, run the `resvalidate` command and fix any issues that it reports

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate
   -persist false
   ```
3. As user `arcsight`, export system tables

   ```
   /opt/arcsight/manager/bin/arcsight export_
   system_tables <username> <password> <dbname> -s
   ```
4. As user `arcsight`, back up configuration data

   ```
   /opt/arcsight/logger/current/arcsight/logger/
   bin/arcsight configbackup
   ```
5. As user `arcsight`, backup archive data

   ```
   /opt/arcsight/logger/current/arcsight/bin/pg_
   dump -d rwdb -c -n data -U web |gzip -9 -v > /
   tmp/postgres_data.sql.gz
   ```
6. As user `root`, stop all services

   ```
   /opt/arcsight/services/init.d/arcsight_services
   stop all
   ```
7. Upgrade the operating system to RHEL/CentOS 7.7 and reboot the system
8. Verify that all services are available

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

9. Download `ArcSightESMSuite-7.2.0.2420.0.tar` and untar it as user `arcsight`
10. As user `root`, stop the services

    `Tools/stop_services.sh`

    Note: You may need to kill the ArcSight processes if the services do not stop and you receive the message:

    `FAIL: timed out awaiting stop of execprocsvc service execprocsvc heartbeat "execproc": available`

    To kill a process

    `pkill –u arcsight`

    `/etc/init.d/arcsight_services stop all.`
11. Specify a global event ID generator ID. As user `arcsight`, create the file `/opt/arcsight/geid.txt` and add the generator ID to the file. The generator ID is an integer between 0 and 16384 (0 and 16384 are not valid):

    `geid.generator.id=<Global_Event_ID_Generator_ID>`
12. If your `/opt/arcsight/logger/data/mysql/ibdata` file size is larger than 200 GB, shrink the mysql database. If you do not shrink the ibdata file, the time to perform this upgrade will increase substantially.

    ```
    cd /opt/arcsight/logger/current/arcsight/bin
    ./mysqldump --max_allowed_packet=512M  --all-databases –ignore-table=arcsight.arc_event --ignore-table=arcsight.events  --socket=/opt/arcsight/logger/current/runtime/mysql.sock -u arcsight -p > small_database.sql
    ```

    As the `arcsight` user, import `small_database.sql` to a test environment running a fresh install of ESM matching the production version

    `/opt/arcsight/manager/bin/arcsight import_system_tables -uarcsight -parcsight arcsight <path to mysql tables.mysql>`

    On the test environment create a tar the `/opt/arcsight/logger/data/mysql` directory

    On the production environment, move the mysql directory to a new location in order to retain a backup copy. Then replace the old mysql directory with the small mysql tar file from the test environment.

    ```
    mv /opt/arcsight/logger/data/mysql /opt/arcsight/logger/data/mysql_large
    /etc/init.d/arcsight_services stop all.
    ```

    Untar the mysql folder from the test environment
13. As user `arcsight`, install the binary and complete the upgrade

    `./ArcSightESMSuite.bin`
14. As user `root`, set up the services.

    `/opt/arcsight/manager/bin/setup_services.sh`
15. Ensure that all services are running and the version is correct

    `/etc/init.d/arcsight_services status`
16. Upgrade the ArcSight Console to ESM 7.2
17. Upgrade ArcSight Connectors to latest versions. This is a ***required*** step.

Upgrading from ESM 7.2 to ESM 7.4

Approximate time to upgrade to ESM 7.4: 40 minutes

Note: When upgrading from ESM 7.2 to ESM 7.4, a tool runs in the background to update the case history to support new functionality in ArcSight Fusion. Please wait for the task to complete before you restart the services. To determine the status, check `/opt/arcsight/var/logs/misc/casehistorybuilder.log`. It is OK to set up the services before the task is complete.

Note: This ESM upgrade includes an upgrade of PostgreSQL from version 8.3 to version 11.4.

1. As user `arcsight`, stop the Manager

   `/etc/init.d/arcsight_services stop manager`
2. As user `arcsight`, run the `resvalidate` command and fix any issues that it reports

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate -persist false
   ```
3. As user `arcsight`, export system tables

   `/opt/arcsight/manager/bin/arcsight export_system_tables <username> <password> <dbname> -s`
4. As user `arcsight`, back up configuration data

   `/opt/arcsight/logger/current/arcsight/logger/bin/arcsight configbackup`
5. As user `arcsight`, backup archive data

   `/opt/arcsight/logger/current/arcsight/bin/pg_dump -d rwdb -c -n data -U web |gzip -9 -v > /tmp/postgres_data.sql.gz`
6. As user `root`, start the Manager

   `service arcsight_services start manager`

7. Download `ArcSightESMSuite-7.4.0.2463.0.tar` and untar it as user `arcsight`
8. As user `root`, stop the services

   `Tools/stop_services.sh`
9. As user `arcsight`, install the binary and complete the upgrade

   `./ArcSightESMSuite.bin`

   If you receive the following message, install the latest tzdata rpm as user `root`:

   ```
   Pre-Install check failed: A timezone version
   2020a or later rpm for your operating system
   must be installed to update timezone info for
   all ESM components. Please exit the installer,
   install the latest OS timezone update and return
   to update timezone for all ESM components.
   ```

   If you receive the following message run `chown -R arcsight: arcsight /opt/arcsight/` to resolve the error:

   ```
   A previous installation was detected but is not
   upgradable:
   While checking eligibility for upgrade, the
   following error was found:
   Please ensure all files under /opt/arcsight are
   owned by user arcsight.
   18 files were found not owned by arcsight. See
   the list in
   /opt/arcsight/upgradelogs/nonArcSightFiles.txt
   ```
10. As user `root`, set up the services.

    `/opt/arcsight/manager/bin/setup_services.sh`
11. Ensure that all services are running and the version is correct

    `/etc/init.d/arcsight_services status`
12. Upgrade the ArcSight Console to ESM 7.4
13. Optionally, upgrade the connectors

Upgrading from ESM 7.4 to ESM 7.5

Approximate time to upgrade to ESM 7.5: 42 minutes

1. As user `arcsight`, stop the Manager

   `/etc/init.d/arcsight_services stop manager`
2. As user `arcsight`, run the `resvalidate` command and fix any issues that it reports

   ```
   export ARCSIGHT_JVM_OPTIONS="-Xmx16284m"
   /opt/arcsight/manager/bin/arcsight resvalidate
   -persist false
   ```
3. As user `arcsight`, export system tables

   `/opt/arcsight/manager/bin/arcsight export_ system_tables <username> <password> <dbname> -s`
4. As user `arcsight`, back up configuration data

   `/opt/arcsight/logger/current/arcsight/logger/ bin/arcsight configbackup`
5. As user `arcsight`, backup archive data

   `/opt/arcsight/logger/current/arcsight/bin/pg_ dump -d rwdb -c -n data -U web |gzip -9 -v > / tmp/postgres_data.sql.gz`
6. As user `root`, start the Manager

   `service arcsight_services start manager`
7. Download `ArcSightESMSuite-7.5.0.2516.0.tar` and untar it as user `arcsight`
8. As user `root`, stop the services

   `Tools/stop_services.sh`
9. As user `arcsight`, install the binary and complete the upgrade

   `./ArcSightESMSuite.bin`
10. As user `root`, set up the services.

    `/opt/arcsight/manager/bin/setup_services.sh`
11. Ensure that all services are running and the version is correct

    `/etc/init.d/arcsight_services status`
12. Upgrade the ArcSight Console to ESM 7.5
13. Optionally, upgrade the connectors

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business