Micro Focus Security ArcSight ESM

Software Version: 7.4

Backup and Recovery Tech Note for Compact and Distributed Mode

Document Release Date: November 2020
Software Release Date: November 2020

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Summary

The information in this technical note applies to ArcSight ESM in both compact and distributed correlation modes. This procedure is for backing up ESM and recovering it on the same system or on a new system with a configuration that is identical to the original system.

This does not cover backup and recovery of any connectors that are installed on the original system.

For all backup operations, back up directly to data storage media other than the one that currently holds the data. Add up the sizes of all relevant files and folders to ensure that the backup media is large enough. Database tables compress well, but event archives do not.

Note: Steps specific to distributed mode are prefixed with **Distributed mode only**.

Some steps apply to compact and distributed mode but have special instructions for distributed mode. The portion that is specific to distributed mode is identified within the step.

Following is a summary of the backup procedure:

1. Shut down all of the ESM services except `mysqld` and `postgresql`. **Distributed mode only:** Do this on the persistor node.
2. Back up selected files and folders.
3. Export selected database tables.
4. Export trends.
5. Back up configuration data.
6. Back up archive data.
7. **Distributed mode only:** Back up the following services:
   - Repository
   - Distributed cache
   - Correlators
   - Aggregators
8. Restart the services.

Following is a summary of the recovery procedure:

1. Reinstall ESM.

   For more information, see the ESM Installation Guide.
2. Import database tables.
3. Import trend data.
4. Recover configuration data.

5. Recover the files and folders you backed up.
6. Recover archive data.
7. **Distributed mode only:** Recover the following services:
   - Repository
   - Message bus control and message bus data
   - Distributed cache
   - Correlators
   - Aggregators
8. Start all services.

Backing up ESM

Use this procedure to back up ESM (including data) installed in compact or distributed mode. For every file, directory, and exported database table, save the backup copy in a safe location on another computer.

To back up ESM:

1. Stop connectors so that they do not continue sending events to ESM.
2. As user `arcsight`, stop all of the ArcSight services except `mysqld` and `postgresql`. **Distributed mode only:** Do this on the persistor node.

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

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

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

3. Use the `cp` command to back up the following files and folders:
   - `/etc/hosts`
   - `/home/arcsight/.bash_profile`
   - `/opt/arcsight/logger/current/arcsight/logger/user/logger/logger.properties`
   - `/opt/arcsight/logger/data/mysql/my.cnf`
   - `/opt/arcsight/manager/config/database.properties`
   - `/opt/arcsight/manager/config/esm.properties` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/config/jetty` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/config/keystore*` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/config/server.properties`
   - `/opt/arcsight/manager/config/server.wrapper.conf`
   - `/opt/arcsight/java/esm/current/jre/lib/security/cacerts` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/user/manager/license` (back up the entire directory)

- **Distributed mode only:**
  - `/opt/arcsight/manager/config/cluster/hazelcast.xml` (do this on all nodes)
  - `/opt/arcsight/manager/config/cluster/hazelcast-client.xml` (do this on all nodes)
  - `/opt/arcsight/manager/config/jaas.config` (do this on all nodes)
  - `/opt/arcsight/var/config` (on all nodes, back up all files in this directory and subdirectories)
  - `/opt/arcsight/manager/tmp/default/processConfig.yaml` (do this on all nodes)
  - On all nodes where correlators are configured, `/opt/arcsight/manager/config/correlator.defaults.properties`
  - On all nodes where aggregators are configured, `/opt/arcsight/manager/config/aggregator.defaults.properties`

4. Run the following command to export system tables:

```
/opt/arcsight/manager/bin/arcsight export_system_tables  arcsight <mysql_
password>   arcsight –s
```

   Because the command generates a large file, Micro Focus recommends running `gzip /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql` and then backing up the resulting `.gz` file.

5. As user `arcsight`, run the following command to export selected tables from the database:

```
/opt/arcsight/logger/current/arcsight/bin/mysqldump -uarcsight -p
arcsight ${tablename}| gzip > /tmp/${tablename}.sql.gz
```

   where:

   - `-uarcsight` specifies to use the database user account called `arcsight`
   - `-p` specifies to prompt for a password
   - `arcsight` is the name of the database
   - `${tablename}` is the name of the table to export (see the list below)
   - the path (`/tmp/` in this case) is the desired location

   Specify the following tables:

   - `user_sequences`
   - `arc_event_annotation`
   - `arc_event_annotation_p`
   - `arc_event_path_info`

- arc_event_payload
- arc_event_payload_p
- arc_event_p
- arc_epd_stats

This command uses compression to reduce disk space. For large databases, compression is also likely to reduce the amount of time for the commands to complete.

The user_sequences table is the table where the ESM Manager gets event IDs from the database. Export the user_sequences table daily.

When the export is complete, copy the .gz file to the same backup location as the other backup files.

6. If you need to keep 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 -
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 backup files.

7. Make a note of the following items, which must match exactly on the computer where you recover the backup:
   - Operating system and version
   - Computer domain name, host name, and IP addresses
   - File system type
   - Path to the archive locations for each storage group
   - ESM version
   - MySQL password

- Timezone of the computer
- **Distributed mode only:** operating system version and ESM version on all nodes (you must install and configure the same versions on all nodes where you recover the backup)

8. Run the following command to back up configuration data:

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

The command creates a `configs.tar.gz` file in `/opt/arcsight/logger/current/arcsight/logger/tmp/configs`. Copy the `.gz` file to the same location as the other backup files.

9. Back up the archive located at `/opt/arcsight/logger/data/archives`.

Back up the archive separately. If the archive location has been moved to a SAN, set up a backup schedule there.

If you do not want to lose events that occurred since midnight (when the last archive was created), back up `/opt/arcsight/logger/data/logger`. However, in addition to the un-archived data since midnight, you will also archive events from each day from yesterday to the beginning of your retention period.

This backup also has to include the metadata. Ensure that the `postgresql` service is running.

Run the following command:

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

Copy `postgres_data.sql.gz` to a backup location.

10. **Distributed mode only:** Run the following command to back up the repository:

```
opt/arcsight/manager/bin/arcsight createRepoBackup <repo_instance>
```

Note: All repository instances create the same backup file, so you only need to back up one instance.

Assuming the repository instance is `repo2`, the command backs up `/opt/arcsight/var/data/repo2` to `/opt/arcsight/var/data/repo2Backup.tar.gz`. Save the file for the recovery procedure.

11. **Distributed mode only:** Make a note of all of the nodes where an `mbus` instance is running (for example, all nodes except the persistor node).
12. **Distributed mode only:** Make a note of all of the nodes where a repository instance is configured, along with the repository ID on each node.

13. As user `arcsight`, run the following command to restart the services:

Note: If your next step is to upgrade the operating system or reinstall ESM, skip this step and the next step.

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

14. Restart connectors.

Recovering ESM

This procedure recovers ESM on the same system or on a new system with a configuration that is identical to the original system. Ensure that the following items are the same on both systems:

- Operating system and version (if using `configbackup` and `disasterrecovery` commands as part of this process)
- Domain names, host names, and IP addresses
- File system type
- Path to the archive locations for each storage group
- ESM version

  Distributed mode only: If you are configuring a new system, when you install ESM in distributed mode, do not configure any services. The recovery procedure will automatically configure the services.
- MySQL password
- Timezone
- **Distributed mode only:** operating system version and ESM version on all nodes (you must install and configure the same versions on all nodes where you recover the backup)

To recover ESM:

1. Stop connectors so that they do not continue sending events to ESM.
2. Ensure that the system is running the same operating system and is configured with the same host name and IP addresses as the original system.

   Distributed mode only: Ensure that all computers on which you will install distributed services match the original computer configurations.
3. Reinstall ESM.

   Distributed mode only: Do not configure the distributed correlation services (`aggregator`, `correlator`, `dcache`, `repo`, `mbus_data`, and `mbus_control`). The services will be configured automatically.

   For more information, see the ESM Installation Guide.
4. **Distributed mode only:** If you have not done so already, run the following command on the persistor node:

   ```
   /etc/init.d/arcsight_services sshSetup
   ```
5. As user `arcsight`, stop all of the ArcSight services except `mysqld` and `postgresql`.

Distributed mode only: Do this on all nodes. Start services only on the persistor node.

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

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

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

6. As user `arcsight`, run the following command to import system tables:

   Note: If you compressed the exported file with `gzip`, unzip it:

   ```
   gzip -d <path>/arcsight_dump_system_tables.sql.gz
   ```

   ```
   /opt/arcsight/manager/bin/arcsight import_system_tables arcsight <mysql_password> arcsight <path>/arcsight_dump_system_tables.sql
   ```

   If you receive an error about the `user_sequence` table, run the following commands:

   ```
   gzip –d /tmp/${tablename}.sql.gz
   ```

   ```
   /opt/arcsight/logger/current/arcsight/bin/mysql -uarcsight -p arcsight < /tmp/user_sequences.sql
   ```

7. To import trend data, as user `arcsight`, run the following command:

   ```
   /opt/arcsight/logger/current/arcsight/bin/mysql -u arcsight -p arcsight < /tmp/arcsight_trends.sql
   ```

   The command above assumes that your trend data was copied from the backup to the `/tmp/` directory. Your file name or directory might differ.

8. Recover the back up files that you previously created:
   - `/etc/hosts`
   - `/home/arcsight/.bash_profile`
   - `/opt/arcsight/logger/current/arcsight/logger/user/logger/logger.properties`
   - `/opt/arcsight/logger/data/mysql/my.cnf`
   - `/opt/arcsight/manager/config/database.properties`
   - `/opt/arcsight/manager/config/esm.properties` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/config/jetty` **Distributed mode only:** Do this on all nodes.
   - `/opt/arcsight/manager/config/keystore*` **Distributed mode only:** Do this on all nodes.

- /opt/arcsight/manager/config/server.properties
- /opt/arcsight/manager/config/server.wrapper.conf
- /opt/arcsight/java/esm/current/jre/lib/security/cacerts **Distributed mode only:** Do this on all nodes.
- /opt/arcsight/manager/user/manager/license (recover the entire directory)
- **Distributed mode only:**
  - /opt/arcsight/manager/config/cluster/hazelcast.xml (do this on all nodes)
  - /opt/arcsight/manager/config/cluster/hazelcast-client.xml (do this on all nodes)
  - /opt/arcsight/manager/config/jaas.config (do this on all nodes)
  - /opt/arcsight/var/config (on all nodes, recover all files in this directory and subdirectories)
  - /opt/arcsight/manager/tmp/default/processConfig.yaml (do this on all nodes)
  - On all nodes where correlators are configured, /opt/arcsight/manager/config/correlator.defaults.properties
  - On all nodes where aggregators are configured, /opt/arcsight/manager/config/aggregator.defaults.properties

9. Log in and run a MySQL command to ensure that the database is running:

```
/opt/arcsight/logger/current/arcsight/bin/mysql -u arcsight -p<password>
arcsight
```

```
describe arc_resource;
```

If you can run both commands without errors, the MySQL database is operational.

10. Recover configuration data. **Distributed mode only:** Do this on the persistor node.
    a. Copy the configs.tar.gz file from the backup folder to the /opt/arcsight/logger/current/backups/ folder.
    b. Ensure that the logger services are stopped. If not, as user arcsight, run the arcsight_services command to stop them.
    c. Run the following commands:

```
cd /opt/arcsight/logger/current/arcsight/logger/bin
```

```
arcsight disasterrecovery start
```

The disasterrecovery command recovers the configs.tar.gz file. It requires that the operating system version be the same as it was when you ran configbackup.

11. Recover archive data. **Distributed mode only:** Do this on the persistor node.

a. Restore the archive files back to `/opt/arcsight/logger/data/archives`.

b. If you backed up `/opt/arcsight/logger/data/logger`, restore it and then run the following commands to recover the metadata:

```
gzip -d /opt/backup/postgres_data.sql.gz
```

```
/opt/arcsight/logger/current/arcsight/bin/psql -d rwdb -U web -f
/opt/backup/postgres_data.sql
```

This example assumes that your backup file is in the `/opt/backup` directory. Your location might differ.

12. As user `arcsight`, run the following commands to recover the tables that you exported in Backing up ESM. **Distributed mode only:** Do this on the persistor node.

```
gzip –d /tmp/${tablename}.sql.gz
```

```
/opt/arcsight/logger/current/arcsight/bin/mysql -uarcsight -p arcsight <
/tmp/${tablename}.sql
```

where:

- `-uarcsight` specifies to use the database user account called `arcsight`
- `-p` specifies to prompt for a password
- `arcsight` is the name of the database
- `${tablename}` is the name of the table to export
- the path (`/tmp/` in this case) is the desired recovery location

13. **Distributed mode only:** Recover repository instances:

> **Note:** These instructions assume that the instance that you backed up was `repo2`, and the instance you are recovering is `repo1`. Repeat this step for each node where repository instances were configured, using the repository ID for each node as recorded during the backup procedure.

a. Log in as user `arcsight`.

b. If the `/opt/arcsight/var/data` directory does not exist, create it.

c. Copy `repo2Backup.tar.gz` to `/opt/arcsight/var/data/repo1Backup.tar.gz`:

```
rm -rf /var/opt/arcsight/data/repo1
```

```
mkdir -p /var/opt/arcsight/data/repo1
```

```
ln -fs /var/opt/arcsight/data/repo1
```

```
/opt/arcsight/var/data
```

```
mkdir /opt/arcsight/var/tmp/repo1
```

```
mkdir /opt/arcsight/var/logs/repo1
```

```
/opt/arcsight/manager/mbus/bin/mbus_setup_bits.sh
```

d. Run the following command on the node where `repo1` was configured:

```
/opt/arcsight/manager/bin/arcsight extractRepoBackup repo1
```

e. Repeat the above steps for each repository instance.

f. On the persistor node, start the repository:

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

14. **Distributed mode only:** Run the following command on each of the nodes that had `mbus_control` and `mbus_data` instances, as recorded during the backup procedure:

```
/opt/arcsight/manager/bin/arcsight mbus-configure-instances
```

This command uses `mbus` instances that are defined in the restored information repository to set up `mbus` directories and configure `mbus` instances on the node.

During recovery, this command replaces the `mbus_setup` command that is typically used to create `mbus` instances after installation.

15. Restart the services:

(**Distributed mode only:** Do this on the persistor node.)

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

16. Restart connectors.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Backup and Recovery Tech Note for Compact and Distributed Mode (ESM 7.4)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!