



HP ArcSight Express

Software Version: AE 4.0

Technical Note: ArcSight Express Backup and Recovery

December 14, 2015

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Summary	4
Backing up ESM with CORR-Engine	5
Restoring ESM with CORR-Engine	8
Send Documentation Feedback	11

Summary

The information in this technical note applies to ArcSight Express 4.0. This procedure is for backing up the CORR-Engine and restoring it to the same machine or a new machine that has been set up to look exactly like the original machine.

This does not cover backup and restore of the ConApp and connectors.

To back up the entire installation in one operation, stop all services and make a copy of `/opt/arcsight` on another storage medium. Include `/etc/hosts` and `/etc/init.d`. This can take a long time, if you have terabytes of data.

For all backup operations, back up directly to data storage media other than the one the data is currently on. You should make sure that this backup media is large enough, so take the time to add up the sizes of all the relevant files and folders. Database tables compress pretty well, but event archives do not.

The more selective backup and restore procedures are as follows.

Back up the CORR-Engine:

- Shutdown ESM services except `mysqld` and `postgresql`.
- Backup selected files and folders.
- Export certain database tables.
- Export trends.
- Back up configuration data.
- Back up archive data.
- Restart the services.

Restore:

- Import database tables.
- Import trend data.
- Restore configuration data.
- Restore the files and folders you backed up.
- Restore archive data.
- Start all services.

Backing up ESM with CORR-Engine

Use this procedure to back up the AE 4.0 CORR-Engine and data. It is expected that for every file, directory, and exported database table, that you save the backup copy in some safe location on another machine.

1. Stop your connectors:

If you stop the connectors, they mark the event where they left off and start in the same place when you restart them. Eventually they catch up. If you let the connectors run after ESM has been stopped, they will cache the data they are collecting. When you restart ESM, all connectors dump their cached events to ESM at the same time. If you have many connectors, the sudden dump from all of them can overload the system and some events might be dropped. Therefore, we recommend that you stop all connectors before step 2.

2. Stop services:

Run the `arcsight_services` command as user *arcsight* to shut down all services except the `mysqld` service and the `postgresql` service. Refer to the "ArcSight_Services Command" topic in the "Administrative Commands" appendix of the *ESM Administrator's Guide*.

3. Back up files:

Back up the following files and folders using the `copy` command.

- `/home/arcsight/.bash_profile`
- `/opt/arcsight/logger/data/mysql/my.cnf`
- `/etc/hosts`
- `/opt/arcsight/manager/config/server.properties`
- `/opt/arcsight/manager/config/database.properties`
- `/opt/arcsight/logger/current/arcsight/logger/user/logger/logger.properties`
- `/opt/arcsight/manager/config/server.wrapper.conf`
- `/opt/arcsight/manager/config/jetty`
- `/opt/arcsight/manager/jre/lib/security/cacerts`
- `/opt/arcsight/manager/user/manager/license/arcsight.lic`

4. Export system tables:

Run the `export_system_tables` command:

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

This generates a very large file, so you are recommended to run
`gzip /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql`
and then back up the resulting `.gz` file to your safe backup location.

5. Dump selected tables:

Export selected tables from the database (as user *arcsight*) using the following command format:

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

...where:

- uarcsight says to use the database user account called *arcsight*.
- p followed by a space means it prompts you for a password.
- arcsight is the name of the database.
- \${tablename} is the name of the table to export, from the list, below.
- The path, /tmp/, in this case, can be anywhere you want.

Specify the following tables:

- user_sequences
- arc_event_annotation
- arc_event_annotation_p
- arc_event_payload
- arc_event_payload_p

This command uses compression to greatly reduce disk space. For large databases, compression is also likely to make the commands finish faster.

The `user_sequences` table is the table where the ESM manager gets the 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 files you backed up off the machine.

6. Export trends:

If you need to keep trends, use the following commands to export them. You should be logged in as user *arcsight*. Enter each line on the command line and press return:

```
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 off the machine.

7. Back up archive data:

Make a note of the following, which must match exactly on the machine to which you restore:

- Operating system and version
- Computer domain name and hostname
- File system type
- Path to the archive locations for each storage group
- ESM version
- MySQL password
- Timezone of the machine

8. Back up the archive located at /opt/arcsight/logger/data/archives. Back it up separately. If the archive location has been moved to a SAN, set up a backup schedule there.

If you cannot afford 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 also get events from each day from yesterday to the beginning of your retention period, which are also in the archives.

This backup also has to include the metadata. Make sure the postgresql service is up and running (bring it up if it's down).

Run this 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.

9. Restart services:

Run the following command as user *arcsight* to restart services. Skip this if your next step is to upgrade the operating system or reinstall ESM.

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

10. Restart connectors

Restoring ESM with CORR-Engine

This procedure is designed for restoring to the same machine. Make sure the following characteristics have not changed since you made your backups:

- Operating system and version
- Computer domain name and hostname
- File system type
- Path to the archive locations for each storage group
- ESM version
- MySQL password
- Timezone of the machine

1. Stop your connectors:

If you stop the connectors, they mark the event where they left off and start in the same place when you restart them. Eventually they catch up. If you let the connectors run after ESM has been stopped, they will cache the data they are collecting. when you restart ESM, all connectors dump their cached events to ESM at the same time. If you have many connectors, the sudden dump from all of them can overload the system and some events might be dropped. Therefore, we recommend that you stop all connectors before step 2.

2. Stop services:

Run the `arcsight_services` command as user *arcsight* to shut down all services except the `mysqld` service and the `postgresql` service. Refer to the "ArcSight_Services Command" topic in the "Administrative Commands" appendix of the *ESM Administrator's Guide*.

3. Import system tables:

If you compressed the exported file with gzip, unzip it with this command:

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


Run the `import_system_tables` command as user *arcsight*.

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

4. Import trend data:

To import trend data, run the following command on the command line as user *arcsight*:

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

This command assumes that your trend data has been copied from backup to the `/tmp/` directory. Your file name or directory may be different.

5. Restore files:

Restore all the files listed in ["Back up files:" on page 5](#).

6. Restore archive data.

Copy all of the backup copies of the archives (that were in `/opt/arcsight/logger/data/archives`) to a mounted directory: `/opt/old_archives`.

Run the `restorearchives` command as follows:

```
/opt/arcsight/logger/current/arcsight/logger/bin/arcsight restorearchives -r
/opt/old_archives -C clear
```

Note: `-C clear` Clears all events currently in the system and deletes any existing archive files that are currently listed in the database. It does this before the restoration operation to clear out the system.

This command allows you to restore archive backups to a new system after a system failure. This tool assumes that you have already copied the archive backups to the location on the new system where your storage archive is located. That is, this restoration does not copy the archives into the system, you do that. It is restoring these archive entries to the new system's database. The command does not copy archive files to the `/opt/arcsight/logger/data/archives` directory.

Refer to the *ESM Administrator's Guide*, in "Appendix A: Administrative Commands," for the syntax and more information.

If you backed up `/opt/arcsight/logger/data/logger`, restore it, too. Then restore the metadata by running these two commands:

```
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
```

These commands assume that your backup file is in the `/opt/backup` directory. Change it to wherever you backed up that file.

7. Restore dumped tables:

Run the following commands as user *arcsight* to restore the tables that were exported with the `mysqldump` command:

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

...where:

-uarcsight says to use the database user account called *arcsight*.

-p followed by a space means it prompts you for a password.

The next *arcsight* is the name of the database.

\${tablename} is the name of the table to export.

The path, `/tmp/`, in this case, is wherever you are restoring the table from.

Run the following command to stop and start `mysqld`:

```
/sbin/service arcsight_services stop mysqld  
/sbin/service arcsight_services start mysqld
```

8. Restart services:

Run the following commands as user *root* to restart services:

```
/opt/arcsight/manager/bin/setup_services.sh  
/etc/init.d/arcsight_services start all
```

9. 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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on Technical Note: ArcSight Express Backup and Recovery (ArcSight Express 4.0)

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 arc-doc@hpe.com.

We appreciate your feedback!