Hewlett Packard
Enterprise

# HPE Security ArcSight ESM

Software Version: 6.11.0

## Upgrade Failure Recovery for ESM Upgrades

March 7, 2017

# Legal Notices

## Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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.

HPE Security 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 Hewlett Packard Enterprise 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



Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

# Support

## Contact Information

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

# Contents

# Introduction

The information in this technical note applies only to upgrade failures during a supported upgrade. Refer to the Upgrade Guide for this release or the latest HPE ArcSight ESM Support Matrix for supported upgrade paths.

**Note:** This document is for internal use. It is written for HPE Customer Support personnel who are tasked with helping customers with their upgrade efforts.

If you encounter a failure when upgrading to ESM 6.11.0, identify which component was being upgraded when the failure occurred and then follow the corresponding failure recovery process for the component in this document.

# Before You Begin the Recovery

Before you begin the recovery process:

- **Check for failures**
  First look at the high level `suite_upgrade.log` log file to get an idea of which component upgrade failed. Use that information to figure out which of the Logger or Manager component's upgrade failed, and which of their log files to look in. Refer to the Upgrade Guide for the location of the log files.

  If Logger upgrade failed, go to "Recovering From Logger Upgrade Failure" on page 6.

  If Manager upgrade failed, go to "Recovering From Manager Upgrade Failure" on page 7.

  If MySQL tzupdate failed, go to "Recovering From Time Zone Update Failure" on page 9.

  Before you begin the recovery process fix whatever caused the upgrade failure.

- **Scripts used for failure recovery**
  Copy these scripts that are used during the failure recovery to `/opt/work` directory on the ESM system. Create the directory if it does not already exist. You can find these scripts on `\\engibrix.arst.hpeswlab.net\Released\ESM\6.11.0\Upgrade Recovery Kit`. The scripts are in a `.tgz` file.

  Make sure that *arcsight* and *root* users have read, write, and execution permission to the `/opt/work` folder and all the scripts within.

  If you encounter an error when running these scripts, see "Resolving Errors When Running the Recovery Scripts" on page 10 for help.

# Commands to Start and Stop Components

The commands to start and stop a component can be run either as user *root* or user *arcsight*. If `stop` does not stop a service, use `tryForceStop`, instead. The commands are:

**ArcSight Manager:**

```
/opt/arcsight/services/init.d/arcsight_services start manager
```

```
/opt/arcsight/services/init.d/arcsight_services stop manager
```

Or:

```
/opt/arcsight/services/init.d/arcsight_services tryForceStop manager
```

**Logger:**

```
/opt/arcsight/services/init.d/arcsight_services start logger_servers
```

To stop Logger, first stop the `loggerd` process as user *arcsight*:

```
/opt/arcsight/logger/current/arcsight/logger/bin/loggerd quit
```

and then stop Logger by running:

```
/opt/arcsight/services/init.d/arcsight_services stop logger_servers
```

**MySQL:**

```
/opt/arcsight/services/init.d/arcsight_services start mysqld
```

```
/opt/arcsight/services/init.d/arcsight_services stop mysqld
```

**Postgresql:**

```
/opt/arcsight/services/init.d/arcsight_services start postgresql
```

```
/opt/arcsight/services/init.d/arcsight_services stop postgresql
```

**All ArcSight Services:**

```
/opt/arcsight/services/init.d/arcsight_services start all
```

```
/opt/arcsight/services/init.d/arcsight_services stop all
```

`monit`, which restarts services, should be stopped by now. But if it is not, you can kill all processes by using the command:

```
kill <pid>
```

**Status of all services:**

```
/opt/arcsight/services/init.d/arcsight_services status all
```

# Recovering From Logger Upgrade Failure

The Logger upgrade logs are located as follows:

Logger overall upgrade log:

`/opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log`

Mysql log:

`/opt/arcsight/logger/current/arcsight/logger/logs/initmysqluser.log`

Postgres log:

`/opt/arcsight/logger/current/arcsight/logger/logs/postgressql_upgrade.out`

Follow these steps to recover from a failure during the Logger upgrade:

1. Make sure that no arcsight services (manager, logger_web, logger_servers, mysqld, postgresql) are running by running the command:

   `/opt/arcsight/services/init.d/arcsight_services status all`

   Stop any services that are running. See "Commands to Start and Stop Components" on the previous page for the command to do so.

2. While logged in as the *arcsight* user, run:

   ```
   cd /opt/work
    ./logger_upgrade_recover.sh
   ```

   This script restores the PostgreSQL database to the state prior to the upgrade using the dump file generated in the beginning of the upgrade process. The dump file to use for upgrade from ESM 6.9.1c is:

   `/opt/arcsight/logger/current/arcsight/logger/user/logger/esm691c.postgres.xxxxxx-xx_xx-xx-xx.dump`

   Make sure that no error is reported. The `logger_upgrade_recover.sh.<TIMESTAMP>.log` log file is generated in the folder where the `logger_upgrade_recover.sh` script is located. It contains the standard output and standard error from running the script.

3. While logged in as user *arcsight*, run this command to resume the upgrade process from the Logger component upgrade

   `/opt/work/upgrade2.sh 1`

   The parameter value of 1 indicates that the upgrade will resume from the Logger component.

   A log file called `upgrade2.sh.<TIMESTAMP>.log` is generated in the folder where the `upgrade2.sh` script is located. `<TIMESTAMP>` represents the time when the `upgrade2.sh` script was run. This log contains the standard output and standard error from running the script.

# Recovering From Manager Upgrade Failure

Open the upgrade log file:

/opt/arcsight/manager/upgrade/out/<TIMESTAMP>/logs/upgrade/server.upgrade.log

Each upgrade attempt creates a new <TIMESTAMP> folder with the name of the folder containing the time that the upgrade was run. Make sure to choose the right <TIMESTAMP> folder that matches the time that you ran the upgrade.

Look for the following lines in the log:

- `[INFO ][default.com.arcsight.install.wizard.silent.WizardTextPanelImpl] Progress: <Correct System Tables Columns>`
- `[INFO ][default.com.arcsight.install.wizard.silent.WizardTextPanelImpl] Progress: <Upgrade system tables>`
- `[INFO ][default.com.arcsight.install.wizard.silent.WizardTextPanelImpl] Progress: <Upgrade system indexes>`
- `[INFO ][default.com.arcsight.install.wizard.silent.WizardTextPanelImpl] Progress: <Upgrade user functions>`

There are two recovery scenarios:

**Scenario 1:**

If the `server.upgrade.log` log does not exist or you do not see any of the above lines, you can resume the upgrade by following these steps:

1. Log in as user *arcsight*.
2. Make sure that the logger, mysqld, and postgresql services are running:
   `/opt/arcsight/services/init.d/arcsight_services status all`
   Start the logger, mysqld, and postgresql services if they are not running. See "Commands to Start and Stop Components" on page 5.
3. Make sure that the ArcSight Manager is not running. See "Commands to Start and Stop Components" on page 5.
   Run the following command:
   `/opt/work/upgrade2.sh 2`
   This script generates a log file called `upgrade2.sh.<TIMESTAMP>.log` in the folder where the `upgrade2.sh` script is located. `<TIMESTAMP>` represents the time when you ran the `upgrade2.sh` script. This log contains the standard output and standard error from running the script.

**Scenario 2:**

If at least one or all of the lines mentioned in "Recovering From Manager Upgrade Failure" on the previous page can be found in the `server.upgrade.log` logs, do the following:

1. Make sure that logger, mysqld, and postgresql services are running:

   `/opt/arcsight/services/init.d/arcsight_services status all`

   Start the logger, mysqld and postgresql services if they are not running. See "Commands to Start and Stop Components" on page 5 for the commands to do so.
2. Make sure that the ArcSight Manager is not running. See "Commands to Start and Stop Components" on page 5 for the commands to do so.
3. Run the following command while logged in as user arcsight to restore system tables:

   `mgr_upgrade_recover.sh <mysqlDBPassword> <DumpFilePath>`

   where `<mysqlDBPassword>` is the MySQL password for user arcsight and `<DumpFilePath>` is the last good system table dump file from your your pre-upgrade system. By default, a dump file is generated in the `/opt/arcsight/manager/tmp/` folder.
4. While logged in as user *arcsight*, run the following command to resume the upgrade:

   `/opt/work/upgrade2.sh 2`

   This script generates a log file called `upgrade2.sh.<TIMESTAMP>.log` in the folder where the `upgrade2.sh` script is located. `<TIMESTAMP>` represents the time when you ran the `upgrade2.sh` script. This log contains the standard output and standard error from running the script.

# Recovering From Time Zone Update Failure

1. Make sure that the ArcSight Manager is not running. If it is running, stop it. See "Commands to Start and Stop Components" on page 5.
2. While logged in as user *arcsight*, run the following command to resume the upgrade process from where it failed:
   `/opt/work/upgrade2.sh 4`
   This script generates a log file called `upgrade2.sh.<TIMESTAMP>.log` in the folder where the `upgrade2.sh` script is located. `<TIMESTAMP>` represents the time when you ran the `upgrade2.sh` script. This log contains the standard output and standard error from running the script.

# Resolving Errors When Running the Recovery Scripts

This section informs you about what you need to do if when you run a recovery script, it returns an error message.

```
Error Message: "<service_name> still running"
```

This is an indication that some services are still running. These services need to be stopped first before proceeding because they will interfere with the upgrade process if running.

Stop the services and re-run the scripts.

The following are some of the options you have to stop the services. They are listed here in the order of preference, so try them in the order shown. Only if one does not work, use the next one.

1. If you need to stop all the services, use `arcsight_services` to stop the services one by one or all at once.
2. If using `arcsight_services` does not work, use the following commands to stop services:
   To stop the Manager:
   ```
   cd /opt/arcsight/manager/; bin/arcsight managerstop
   ```
   To stop aps:
   ```
   /opt/arcsight/logger/current/arcsight/service/aps stop
   ```
   To stop logger_httpd:
   ```
   /opt/arcsight/logger/current/arcsight/service/apache stop
   ```
   To stop Logger:
   ```
   /opt/arcsight/logger/current/arcsight/logger/bin/loggerd quit
   /opt/arcsight/logger/current/arcsight/service/arcsight_logger stop
   ```
   To stop MySQL:
   ```
   /opt/arcsight/logger/current/arcsight/service/mysql stop
   ```
   To stop postgresql:
   ```
   /opt/arcsight/logger/current/arcsight/service/postgresql stop
   ```
   To stop monit:
   ```
   /opt/arcsight/services/init.d/arcsight_services stop
   /opt/arcsight/services/init.d/arcsight_services uninstall
   /opt/arcsight/services/init.d/arcsight_services clean
   ```
3. If the above commands above do not work, use the `kill <pid>` command to stop the running processes, where `<pid>` is the ID of the process you want to stop. If the owner of the process is *root*, run the command as the *root* user.

If you notice that services are being restarted with a different process id, it probably means that monit is still running. You can double check that monit is running with the command `pgrep monit`. Monit is running if this command produces any output. If it is running, you can kill the process by using the command `kill <pid>`.

# 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 Upgrade Failure Recovery for ESM Upgrades (ESM 6.11.0)**

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!