
Micro Focus Security ArcSight ESM

Software Version: 6.11.0 Patch 3

Upgrade to RHEL 7.3 + Spectre Hotfix or RHEL 7.4 or 7.5 on a G9 Appliance

Document Release Date: September 30, 2018

Software Release Date: September 30, 2018



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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/ctp/productdocs

Contents

Upgrading a G9 Appliance Running ESM 6.11.0 Patch 3	4
Verify OS Upgrade File	4
Upgrading a Single Appliance	5
Upgrading a Single Appliance to RHEL 7.3	5
Upgrading a Single Appliance to RHEL 7.4	6
Upgrading a Single Appliance to RHEL 7.5	6
Upgrading High Availability Appliances	8
Upgrading HA Appliances to RHEL 7.3 with Spectre Meltdown Hotfix	8
Upgrading HA Appliances to RHEL 7.4	12
Upgrading HA Appliances to RHEL 7.5	16
Send Documentation Feedback	19

Upgrading a G9 Appliance Running ESM 6.11.0 Patch 3

This document provides information on how to upgrade from Red Hat Enterprise Linux RHEL 7.3 to RHEL 7.3 with Spectre RHEL 7.4 or RHEL 7.5 on a G9 appliance running ESM 6.11.0 Patch 3.

Verify OS Upgrade File

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do>

Upgrading a Single Appliance

Use this procedure when you *do not* have the High Availability Module (HA).

Upgrading a Single Appliance to RHEL 7.3

Note: This upgrade to RHEL 7.3 will also automatically install the Spectre Meltdown fix.

1. Log in to the system as user root.
2. As user root, transfer the upgrade file to the target system in the `/tmp` partition..

The file is named `esm_osupgrade_rhel73_20180306104731.tar.gz`

3. Stop all arcsight services by running the following command:

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

4. From the directory where you put the archive in step 4, extract it as follows:

```
/bin/tar zxvf esm_osupgrade_rhel73_20180306104731.tar.gz
```

5. Change directory:

```
cd esm-rhel73upgrade
```

6. Run the following command to make the script executable:

```
chmod 0700 osupgrade
```

7. Run the following command to start the upgrade:

```
./osupgrade 2>&1 | tee osupgrade.log
```

8. Make sure the system is rebooted after the script completes.

9. If any ArcSight services are not restarted automatically, restart them.

10. Check the operating system version by running the following command:

```
cat /etc/redhat-release
```

The result of this command should be:

```
Red Hat Enterprise Linux Server release 7.3
```

11. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

The RHEL 7.3 upgrade, which includes the fix for the Spectre meltdown issue, is now complete.

Upgrading a Single Appliance to RHEL 7.4

1. Log in to the system as user `root`.
2. As user `root`, transfer the upgrade file to the target system in the `/tmp` partition..
The file is named `esm_osupgrade_rhel74_20180430095302.tar.gz`
3. Stop all arcsight services by running the following command:
`/etc/init.d/arcsight_services stop all`
4. From the directory where you put the archive in step 4, extract it as follows:
`/bin/tar zxvf esm_osupgrade_rhel74_20180430095302.tar.gz`
5. Change directory:
`cd esm-rhel74upgrade`
6. Run the following command to make the script executable:
`chmod 0700 osupgrade`
7. Run the following command to start the upgrade:
`./osupgrade 2>&1 | tee osupgrade.log`
8. Make sure the system is rebooted after the script completes.
9. If any ArcSight services are not restarted automatically, restart them.
10. Check the operating system version by running the following command:
`cat /etc/redhat-release`
The result of this command should be:
`Red Hat Enterprise Linux Server release 7.4`
11. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

The RHEL 7.4 upgrade is now complete.

Upgrading a Single Appliance to RHEL 7.5

1. Log in to the system as user `root`.
2. As user `root`, transfer the upgrade file to the target system in the `/tmp` partition..
The file is named `esm_osupgrade_rhel75_20180828142739.tar.gz`
3. Stop all arcsight services by running the following command:
`/etc/init.d/arcsight_services stop all`
4. From the directory where you put the archive in step 4, extract it as follows:
`/bin/tar zxvf esm_osupgrade_rhel75_20180828142739.tar.gz`
5. Change directory:
`cd esm-rhel75upgrade`

6. Run the following command to make the script executable:
`chmod 0700 osupgrade`
7. Run the following command to start the upgrade:
`./osupgrade 2>&1 | tee osupgrade.log`
8. Make sure the system is rebooted after the script completes.
9. If any ArcSight services are not restarted automatically, restart them.
10. Check the operating system version by running the following command:
`cat /etc/redhat-release`
The result of this command should be:
`Red Hat Enterprise Linux Server release 7.5`
11. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

The RHEL 7.5 upgrade is now complete.

Upgrading High Availability Appliances

Use this procedure when you have the High Availability Module (HA) and you are upgrading the operating system on both the primary and the secondary appliances.

Note: Upgrade the secondary server before the primary server.

Upgrading HA Appliances to RHEL 7.3 with Spectre Meltdown Hotfix

Note: This upgrade to RHEL 7.3 will also automatically install the Spectre Meltdown fix.

Prepare the Two Servers: Primary and Secondary:

1. On *both* servers:
 - a. Run the following command as **root** to disable `drbd.service`:
`systemctl disable drbd.service`
 - b. Verify with this command:
`systemctl list-unit-files --type=service |grep drbd`
`drbd.service` is shown as disabled. Make sure to keep this disabled setting throughout the upgrade process.
2. Put the *secondary* server on standby by running this command as **root**:
`crm_standby -v true`
3. Take the *secondary* server offline by running this command as **root**:
`systemctl stop heartbeat`
`systemctl disable heartbeat`
4. Proceed with the upgrade of the secondary server, "[Upgrade to RHEL 7.3 on the Secondary:](#)" [below](#).

Upgrade to RHEL 7.3 on the Secondary:

1. Log in to the system as user `root`.
2. As user `root`, transfer the following three files to the `/tmp` partition:
`esm_osupgrade_rhel73_20180306104731.tar.gz`
`HA_6.11.0_Update_For7.3OS.tgz`

3. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel73_20180306104731.tar.gz` as follows:

```
tar zxvf esm_osupgrade_rhel73_20180306104731.tar.gz
```
 4. Change directory:

```
cd esm-rhel73upgrade
```
 5. Run the following command to make the script executable:

```
chmod 0700 osupgrade
```
 6. Run the following command to start the upgrade:

```
./osupgrade 2>&1 | tee osupgrade.log
```
 7. Make sure the system is rebooted after the script completes.
 8. Check the operating system version by running the following command:

```
cat /etc/redhat-release
```

The result of this command should be:

```
Red Hat Enterprise Linux Server release 7.3
```
 9. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -xvf HA_6.11.0_Update_For_7.3OS.tgz
cd HA_6.11.0_Update_For_7.3OS
./HAupdate.sh
```
- Note:** Allow 25 minutes or so for this step to complete.
10. Run the following command as user `root` on the secondary server to bring it online:

```
systemctl start heartbeat
systemctl enable heartbeat
```
 11. Proceed to the upgrade on the primary server, "[Upgrade to RHEL 7.3 on the Primary:](#)" below.

Upgrade to RHEL 7.3 on the Primary:

1. Log in to the system as user `root`.
2. As user `root`, transfer the following files to `/tmp` partition:

```
esm_osupgrade_rhel73_20180306104731.tar.gz
HA_6.11.0_Update_For_7.3OS.tgz
```
3. Stop all arcsight services by running the following command:

```
service arcsight_services stop all
```

Note: ArcSight ESM will not be available for about 25 minutes.
4. Run the following command as user `root` on the primary server to take it offline:

```
systemctl stop heartbeat
systemctl disable heartbeat
```
5. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel73_`

```
20180306104731.tar.gz
```

```
/bin/tar zxvf esm_osupgrade_rhel73_20180306104731.tar.gz
```

6. Change directory:

```
cd rhel73-upgrade
```
7. Run the following command to make the script executable:

```
chmod 0700 osupgrade
```
8. Run the following command to start the upgrade:

```
./osupgrade 2>&1 | tee osupgrade.log
```
9. Make sure the system is rebooted after the script completes.
10. Check the operating system version by running the following command:

```
cat /etc/redhat-release
```

The result of this command should be:

```
Red Hat Enterprise Linux Server release 7.3
```
11. Update the HA rpms to support HA on the 7.3 operating system. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -zxvf HA_6.11.0_Update_For_7.3OS.tgz  
cd HA_6.11.0_Update_For_7.3OS  
./HAUpdate.sh
```

Note: Allow 25 minutes or so for this step to complete.

12. Enter this command as a fix for a Linbit bug in the 7.3 operating system for HA that causes a large delay in the transfer of services when one system in the cluster goes offline:

```
crm configure property cluster-recheck-interval=1M
```

The following messages are displayed:

```
WARNING: unrecognized CIB element <built-in function Comment>  
ERROR: cib-bootstrap-options: attribute expected-quorum-votes does not exist
```

Enter **y** at the prompt:

```
Do you still want to commit (y/n)? y
```
13. Run the following command as user *root* on the primary server to bring it online:

```
service heartbeat start  
systemctl enable heartbeat
```
14. Return to the secondary server.
15. Run the following command as user *root* on the secondary server to bring it online:

```
crm_standby -D
```
16. Run the following command as user *root*, (on either server) to make sure the HA status is OK:

```
/usr/lib/arc sight/highavail/bin/arc sight_cluster status
```
17. If any ArcSight services are not restarted automatically restart them on the primary server (where the */opt/arc sight* resides and you can run the command `service arc sight_services start`).

18. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

Note: If, after the upgrade, the disks do not connect, run `arcsight_cluster diagnose` to clear the problem.

The RHEL 7.3 upgrade is now completed on the HA environment.

Upgrading HA Appliances to RHEL 7.4

Prepare the Two Servers: Primary and Secondary:

1. On *both* servers:
 - a. Run the following command as **root** to disable `drbd.service`:
`systemctl disable drbd.service`
 - b. Verify with this command:
`systemctl list-unit-files --type=service |grep drbd`
`drbd.service` is shown as disabled. Make sure to keep this disabled setting throughout the upgrade process.
2. Put the *secondary* server on standby by running this command as **root**:
`crm_standby -v true`
3. Take the *secondary* server offline by running this command as **root**:
`systemctl stop heartbeat`
`systemctl disable heartbeat`
4. Proceed with the upgrade of the secondary server, "[Upgrade to RHEL 7.4 on the Secondary:](#)" [below](#).

Upgrade to RHEL 7.4 on the Secondary:

1. Log in to the system as user `root`.
2. As user `root`, transfer the following three files to the `/tmp` partition:
`esm_osupgrade_rhel74_20180430095302.tar.gz`
`HA_6.11.0_Update_For_7.4OS.tgz`
`esm_ha_support_rpms_rhel74.tar.gz`
3. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel74_20180430095302.tar.gz` as follows:
`tar zxvf esm_osupgrade_rhel73_20180306104731.tar.gz`
4. Change directory:
`cd esm-rhel74upgrade`
5. Run the following command to make the script executable:
`chmod 0700 osupgrade`
6. Run the following command to start the upgrade:
`./osupgrade 2>&1 | tee osupgrade.log`
7. Make sure the system is rebooted after the script completes.
8. Check the operating system version by running the following command:
`cat /etc/redhat-release`

The result of this command should be:

Red Hat Enterprise Linux Server release 7.4

9. From the directory where you put the archive in step 2, extract and install the HA Support RPMs using the following commands:

```
tar -zxvf esm_ha_support_rpms_rhel74.tar.gz
cd esm_ha_support_rpms_rhel74
./install_ha_support_pkgs.sh
```

10. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -xvf HA_6.11.0_Update_For_7.4OS.tgz
cd HA_6.11.0_Update_For_7.4OS
./HAupdate.sh
```

Note: Allow 25 minutes or so for this step to complete.

11. Run the following command as user *root* on the secondary server to bring it online:

```
systemctl start heartbeat
systemctl enable heartbeat
```
12. Proceed to the upgrade on the primary server, "[Upgrade to RHEL 7.4 on the Primary:](#)" below.

Upgrade to RHEL 7.4 on the Primary:

1. Log in to the system as user *root*.
2. As user *root*, transfer the following three files to /tmp partition:

```
esm_osupgrade_rhel74_20180430095302.tar.gz
HA_6.11.0_Update_For_7.4OS.tgz
esm_ha_support_rpms_rhel74.tar.gz
```
3. Stop all arcsight services by running the following command:

```
service arcsight_services stop all
```

Note: ArcSight ESM will not be available for about 25 minutes.
4. Run the following command as user *root* on the primary server to take it offline:

```
systemctl stop heartbeat
systemctl disable heartbeat
```
5. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel74_20180430095302.tar.gz` as follows:

```
/bin/tar zxvf esm_osupgrade_rhel74_20180430095302.tar.gz
```
6. Change directory:

```
cd rhel74-upgrade
```
7. Run the following command to make the script executable:

```
chmod 0700 osupgrade
```
8. Run the following command to start the upgrade:

```
./osupgrade 2>&1 | tee osupgrade.log
```

9. Make sure the system is rebooted after the script completes.
10. Check the operating system version by running the following command:

```
cat /etc/redhat-release
```

The result of this command should be:

```
Red Hat Enterprise Linux Server release 7.3
```
11. From the directory where you put the archive in step 2, extract and install the HA Support RPMs using the following commands:

```
tar -zxvf esm_ha_support_rpms_rhel74.tar.gz  
cd esm_ha_support_rpms_rhel74  
./install_ha_support_pkgs.sh
```
12. Update the HA rpms to support HA on the 7.4 operating system. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -zxvf HA_6.11.0_Update_For_7.4OS.tgz  
cd HA_6.11.0_Update_For_7.4OS  
./HAUpdate.sh
```

Note: Allow 25 minutes or so for this step to complete.
13. Enter this command as a fix for a Linbit bug in the 7.3 operating system for HA that causes a large delay in the transfer of services when one system in the cluster goes offline:

```
crm configure property cluster-recheck-interval=1M
```

The following messages are displayed:

```
WARNING: unrecognized CIB element <built-in function Comment>  
ERROR: cib-bootstrap-options: attribute expected-quorum-votes does not exist
```

Enter **y** at the prompt:

```
Do you still want to commit (y/n)? y
```
14. Run the following command as user *root* on the primary server to bring it online:

```
systemctl start heartbeat  
systemctl enable heartbeat
```
15. Return to the secondary server.
16. Run the following command as user *root* on the secondary server to bring it online:

```
crm_standby -D
```
17. Run the following command as user *root*, (on either server) to make sure the HA status is OK:

```
/usr/lib/arc sight/highavail/bin/arc sight_cluster status
```
18. If any ArcSight services are not restarted automatically restart them on the primary server (where the */opt/arc sight* resides and you can run the command `service arc sight_services start`).
19. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

Note: If, after the upgrade, the disks do not connect, run `arc sight_cluster diagnose` to clear the problem.

The RHEL 7.4 upgrade is now completed on the HA environment.

Upgrading HA Appliances to RHEL 7.5

Prepare the Two Servers: Primary and Secondary:

1. On *both* servers:
 - a. Run the following command as **root** to disable `drbd.service`:
`systemctl disable drbd.service`
 - b. Verify with this command:
`systemctl list-unit-files --type=service |grep drbd`
`drbd.service` is shown as disabled. Make sure to keep this disabled setting throughout the upgrade process.
2. Put the *secondary* server on standby by running this command as **root**:
`crm_standby -v true`
3. Take the *secondary* server offline by running this command as **root**:
`systemctl stop heartbeat`
`systemctl disable heartbeat`
4. Proceed with the upgrade of the secondary server, "[Upgrade to RHEL 7.5 on the Secondary:](#)" [below](#).

Upgrade to RHEL 7.5 on the Secondary:

1. Log in to the system as user `root`.
2. As user `root`, transfer the following three files to the `/tmp` partition:
`esm_osupgrade_rhel75_20180828142739.tar.gz`
`HA_6.11.0_Update_For_7.5OS.tgz`
`esm_ha_support_rpms_rhel75.tar.gz`
3. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel75_20180828142739.tar.gz` as follows:
`tar zxvf esm_osupgrade_rhel75_20180828142739.tar.gz`
4. Change directory:
`cd esm-rhel75upgrade`
5. Run the following command to make the script executable:
`chmod 0700 osupgrade`
6. Run the following command to start the upgrade:
`./osupgrade 2>&1 | tee osupgrade.log`
7. Make sure the system is rebooted after the script completes.
8. Check the operating system version by running the following command:
`cat /etc/redhat-release`

The result of this command should be:

Red Hat Enterprise Linux Server release 7.5

9. From the directory where you put the archive in step 2, extract and install the HA Support RPMs using the following commands:

```
tar -zxvf esm_ha_support_rpms_rhel75.tar.gz
cd esm_ha_support_rpms_rhel75
./install_ha_support_pkgs.sh
```

10. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -xvf HA_6.11.0_Update_For_7.5OS.tgz
cd HA_6.11.0_Update_For_7.5OS
./HAupdate.sh
```

Note: Allow 25 minutes or so for this step to complete.

11. Run the following command as user *root* on the secondary server to bring it online:

```
service heartbeat start
systemctl enable heartbeat
```
12. Proceed to the upgrade on the primary server, "[Upgrade to RHEL 7.5 on the Primary:](#)" below.

Upgrade to RHEL 7.5 on the Primary:

1. Log in to the system as user *root*.
2. As user *root*, transfer the following three files to /tmp partition:

```
esm_osupgrade_rhel75_20180828142739.tar.gz
HA_6.11.0_Update_For_7.5OS.tgz
esm_ha_support_rpms_rhel75.tar.gz
```
3. Stop all arcsight services by running the following command:

```
service arcsight_services stop all
```

Note: ArcSight ESM will not be available for about 25 minutes.
4. Run the following command as user *root* on the primary server to take it offline:

```
systemctl stop heartbeat
systemctl disable heartbeat
```
5. From the directory where you put the archive in step 2, extract `esm_osupgrade_rhel75_20180828142739.tar.gz` as follows:

```
/bin/tar zxvf esm_osupgrade_rhel75_20180828142739.tar.gz
```
6. Change directory:

```
cd rhel75-upgrade
```
7. Run the following command to make the script executable:

```
chmod 0700 osupgrade
```
8. Run the following command to start the upgrade:

```
./osupgrade 2>&1 | tee osupgrade.log
```
9. Make sure the system is rebooted after the script completes.

10. Check the operating system version by running the following command:

```
cat /etc/redhat-release
```

The result of this command should be:

```
Red Hat Enterprise Linux Server release 7.5
```

11. From the directory where you put the archive in step 2, extract and install the HA Support RPMs using the following commands:

```
tar -zxvf esm_ha_support_rpms_rhel75.tar.gz
cd esm_ha_support_rpms_rhel75
./install_ha_support_pkgs.sh
```

12. Update the HA rpms to support HA on the 7.5 operating system. From the directory where you put the archive in step 2, extract and install the HA update using the following commands:

```
tar -zxvf HA_6.11.0_Update_For_7.5OS.tgz
cd HA_6.11.0_Update_For_7.5OS
./HAUpdate.sh
```

Note: Allow 25 minutes or so for this step to complete.

13. Enter this command as a fix for a Linbit bug in the 7.5 operating system for HA that causes a large delay in the transfer of services when one system in the cluster goes offline:

```
crm configure property cluster-recheck-interval=1M
```

The following messages are displayed:

```
WARNING: unrecognized CIB element <built-in function Comment>
ERROR: cib-bootstrap-options: attribute expected-quorum-votes does not exist
```

Enter **y** at the prompt:

```
Do you still want to commit (y/n)? y
```

14. Run the following command as user *root* on the primary server to bring it online:

```
systemctl start heartbeat
systemctl enable heartbeat
```

15. Return to the secondary server.

16. Run the following command as user *root* on the secondary server to bring it online:

```
crm_standby -D
```

17. Run the following command as user *root*, (on either server) to make sure the HA status is OK:

```
/usr/lib/arcsight/highavail/bin/arcsight_cluster status
```

18. If any ArcSight services are not restarted automatically restart them on the primary server (where the */opt/arcsight* resides and you can run the command `service arcsight_services start`).

19. Start the ArcSight Console to make sure you can log in successfully. Check a few features to make sure they are operating as expected.

Note: If, after the upgrade, the disks do not connect, run `arcsight_cluster diagnose` to clear the problem.

The RHEL 7.5 upgrade is now completed on the HA environment.

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 Upgrade to RHEL 7.3 + Spectre Hotfix or RHEL 7.4 or 7.5 on a G9 Appliance (ESM 6.11.0 Patch 3)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!