
Micro Focus Security

ArcSight High Availability Module

Software Version: 7.0 Patch 2

**Upgrade HA Environment on ESM 7.0/ESM 7.0 P 1 to
either RHEL 7.4, RHEL 7.5, CentOS 7.4 or CentOS 7.5**

Document Release Date: February 22, 2019

Software Release Date: February 22, 2019



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 2019 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

Upgrade Procedure from ESM 7.0 to ESM 7.0 Patch 2	4
Upgrading to RHEL 7.4	4
Upgrading to RHEL 7.5	6
Upgrade Procedure from ESM 7.0 Patch 1 to ESM 7.0 Patch 2	8
Send Documentation Feedback	12

Upgrade Procedure from ESM 7.0 to ESM 7.0 Patch 2

Upgrading to RHEL 7.4

This document provides information on how to upgrade ESM 7.0 Patch 2 with the High Availability module (HA) as implemented on:

- RHEL 7.3 with spectre to support RHEL 7.4

The starting state (before upgrade) is assumed to be:

- ESM 7.0
- HA implemented on the primary and secondary servers
- RHEL 7.3 with spectre

To perform the upgrade:

1. Run the following command to disable `drbd.service` as user *root* on both servers before you start the upgrade:

```
systemctl disable drbd.service
```

To verify, run:

```
systemctl list-unit-files --type=service |grep drbd  
drbd.service disabled
```

This setting should persist.

2. Run the following command as user *root* on the secondary server to put it on standby:

```
crm_standby -v true
```
3. Run the following command as user *root* on the secondary server to take it offline:

```
systemctl stop heartbeat  
systemctl disable heartbeat
```

4. On the secondary server:

- a. Have yum configured to upgrade to the new operating system.
- b. Upgrade the operating system to RHEL 7.4.

Add an exclude statement for the following packages to your RHEL 7 base repo configuration (/etc/yum.repos.d/RHEL-Base.repo), under the updates section.

It should look something like this for RHEL:

```
[updates]
name=RHEL-$releasever - Updates
mirrorlist=http://mirrorlist.rhel.org/?release=$releasever&arch=$basearch&repo=updates
#baseurl=http://mirror.rhel.org/rhel/$releasever/updates/$basearch/gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RHEL-7
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue* linbit-cluster-stack-heartbeat* libqb*
```

- c. Download the HA Upgrade from Software Support. The file name is HA_7.0.0_Update_For_7.4OS.tgz.

Be sure to verify the upgrade file. A digital public key is provided to enable you to verify that the signed software you received is indeed from a trusted source and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do>

- d. Copy the HA update to the /tmp partition on the server.
- e. Install the HA update using these commands:

```
cd HA_7.0.0_Update_For_7.4OS/
cd dist/
tar xf HA_7.0.0_Update_For_7.4OS.tgz
cd HA_7.0.0_Update_For_7.4OS
./HAUpdate.sh
```

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

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

6. Stop ArcSight services on the primary server:

```
service arcsight_services stop all
```

ArcSight Services will not be available until after the OS upgrade is completed on the primary server.

7. Repeat steps 3 through 5 on the primary server. It is expected that ESM will go down while the primary server is updating.
8. Run the following command as user *root* on the secondary server to take it off standby:
`crm_standby -D`
9. Run the following command as user *root*, (on either server) to check the HA installation, as described in the HA Users Guide, in the "Verify HA Installation" section:
`/usr/lib/arc sight/highavail/bin/arc sight_cluster status`
10. 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`)
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.
12. Please refer to the Release notes for 7.0 patch 2 and follow the patch update on HA setup.

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

Upgrading to RHEL 7.5

This document provides information on how to upgrade ESM 7.0 Patch 2 with the High Availability module (HA) as implemented on:

- RHEL 7.3 with spectre to support RHEL 7.5

The starting state (before upgrade) is assumed to be:

- ESM 7.0
- HA implemented on the primary and secondary servers
- RHEL 7.3 with spectre

To perform the upgrade:

1. Run the following command to disable `drbd.service` as user *root* on both servers before you start the upgrade:
`systemctl disable drbd.service`
To verify, run:
`systemctl list-unit-files --type=service |grep drbd`
`drbd.service disabled`
This setting should persist.
2. Run the following command as user *root* on the secondary server to put it on standby:
`crm_standby -v true`
3. Run the following command as user *root* on the secondary server to take it offline:

```
systemctl stop heartbeat
systemctl disable heartbeat
```

4. On the secondary server:

a. Have yum configured to upgrade to the new operating system.

b. Upgrade the operating system to RHEL 7.5.

Add an exclude statement for the following packages to your RHEL 7 base repo configuration (/etc/yum.repos.d/RHEL-Base.repo), under the updates section.

It should look something like this for RHEL:

```
[updates]
name=RHEL-$releasever - Updates
mirrorlist=http://mirrorlist.rhel.org/?release=$releasever&arch=$basearch&repo=updates
#baseurl=http://mirror.rhel.org/rhel/$releasever/updates/$basearch/gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RHEL-7
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue* linbit-cluster-stack-heartbeat* libqb*
```

c. Download the HA Upgrade from Software Support. The file name is HA_7.0.0_Update_For_7.5OS.tgz.

Be sure to verify the upgrade file. A digital public key is provided to enable you to verify that the signed software you received is indeed from a trusted source and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h22253.www2.hpe.com/eCommerce/efulfillment/digitalSignIn.do>

d. Copy the HA update to the /tmp partition on the server.

e. Install the HA update using these commands:

```
cd HA_7.0.0_Update_For_7.5OS/
cd dist/
tar xf HA_7.0.0_Update_For_7.5OS.tgz
cd HA_7.0.0_Update_For_7.5OS/
./HAUpdate.sh
```

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

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

6. Stop ArcSight services on the primary server:

```
service arcsight_services stop all
```

ArcSight Services will not be available until after the OS upgrade is completed on the primary server.

7. Repeat steps 3 through 5 on the primary server. It is expected that ESM will go down while the primary server is updating.
8. Run the following command as user *root* on the secondary server to take it off standby:
`crm_standby -D`
9. Run the following command as user *root*, (on either server) to check the HA installation, as described in the HA Users Guide, in the "Verify HA Installation" section:
`/usr/lib/arcsight/highavail/bin/arcsight_cluster status`
10. 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`)
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.
12. Please refer to the Release notes for 7.0 patch 2 and follow the patch update on HA setup.

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

Upgrade Procedure from ESM 7.0 Patch 1 to ESM 7.0 Patch 2

This document provides information on how to upgrade ESM 7.0 Patch 1 with the High Availability module (HA) as implemented on:

- RHEL 7.4
- CentOS 7.4

The starting state (before upgrade) is assumed to be:

- ESM 7.0 Patch 1
- HA implemented on the primary and secondary servers
- RHEL 7.4
- CentOS 7.4.

To perform the upgrade:

1. Run the following command to disable `drbd.service` as user *root* on both servers before you start the upgrade:

```
systemctl disable drbd.service
```

To verify, run:


```
systemctl list-unit-files --type=service |grep drbd  
drbd.service disabled
```

This setting should persist.

2. Run the following command as user *root* on the secondary server to put it on standby:
`crm_standby -v true`
3. Run the following command as user *root* on the secondary server to take it offline:
`systemctl stop heartbeat`
`systemctl disable heartbeat`

4. On the secondary server:

- a. Have yum configured to upgrade to the new operating system.
- b. Upgrade the operating system to RHEL 7.5 or CentOS 7.5.

Add an exclude statement for the following packages to your CentOS/RHEL 7 base repo configuration (/etc/yum.repos.d/CentOS-Base.repo), under the updates section. It should look something like this for CentOS:

```
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue* linbit-cluster-stack-heartbeat* libqb*
```

It should look something like this for RHEL:

```
[updates]
name=RHEL-$releasever - Updates
mirrorlist=http://mirrorlist.rhel.org/?release=$releasever&arch=$basearch&repo=updates
#baseurl=http://mirror.rhel.org/rhel/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RHEL-7
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue* linbit-cluster-stack-heartbeat* libqb*
```

- c. Download the HA Upgrade from Software Support. The file name is HA_7.0.0_Update_For_7.5OS.tgz.

Be sure to verify the upgrade file. A digital public key is provided to enable you to verify that the signed software you received is indeed from a trusted source and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do>

- d. Copy the HA update to the /tmp partition on the server.
- e. Install the HA update using these commands:

```
cd HA_7.0.0_Update_For_7.5OS/
cd dist/
tar xf HA_7.0.0_Update_For_7.5OS.tgz
```

```
cd HA_7.0.0_Update_For_7.50S/  
./HAUpdate.sh
```

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

```
systemctl enable heartbeat  
systemctl start heartbeat
```
6. Stop ArcSight services on the primary server:

```
service arcsight_services stop all
```

ArcSight Services will not be available until after the OS upgrade is completed on the primary server.
7. Repeat steps 3 through 5 on the primary server. It is expected that ESM will go down while the primary server is updating.
8. Run the following command as user *root* on the secondary server to take it off standby:

```
crm_standby -D
```
9. Run the following command as user *root*, (on either server) to check the HA installation, as described in the HA Users Guide, in the "Verify HA Installation" section:

```
/usr/lib/arcsight/highavail/bin/arcsight_cluster status
```
10. 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`)
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.
12. Please refer to the Release notes for 7.0 patch 2 and follow the patch update on HA setup.

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

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 HA Environment on ESM 7.0/ESM 7.0 P 1 to either RHEL 7.4, RHEL 7.5, CentOS 7.4 or CentOS 7.5 (High Availability Module 7.0 Patch 2)

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!