



Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 6.11.0 Patch 1

Upgrade HA Environment on ESM 6.11.0 Patch 1 to RHEL
6.9 or CentOS 6.9

July 21, 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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

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

<https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

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://community.saas.hpe.com/t5/ArcSight/ct-p/arc sight

Contents

Upgrade Procedure	4
Send Documentation Feedback	8

Upgrade Procedure

This document provides information on how to upgrade ESM 6.11.0 Patch 1 with the High Availability module (HA) as implemented on:

- RHEL 6.7 and 6.8 to support RHEL6.9
- CentOS 6.7 and 6.8 to support CentOS 6.9

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

- ESM 6.11.0
- HA implemented on the primary and secondary servers
- RHEL 6.7 or 6.8
- CentOS 6.7 or 6.8

To perform the upgrade:

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

```
chkconfig drbd off
```

To verify, run:

```
chkconfig --list drbd
```

```
drbd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

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:
`service heartbeat stop`

4. On the secondary server:

- a. Have yum configured to upgrade to the new operating system.
- b. Upgrade the operating system to RHEL 6.9 or CentOS 6.9.

Add an exclude statement for the following packages to your CentOS/RHEL 6 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-6
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue*
```

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-6
exclude=heartbeat* corosync* pacemaker* drbd* resource-agents cluster-glue*
```

- c. Download the HA Update from the HPE Software Support Online site (<http://softwaresupport.hpe.com>). The file name is HA_6.11_Update_For_6.90S.tgz. Be sure to verify the upgrade file. HPE provides a digital public key to enable you to verify that the signed software you received is indeed from HPE and has not been manipulated in any way by a third party. Visit the following site for information and instructions: <https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>
- d. Copy the HA update to the /tmp partition on the server.
- e. Install the HA update using these commands:

```
tar -zxvf HA_6.11_Update_For_6.90S.tgz
cd HA_6.11_Update_For_6.90S
./HAUpdate.sh
```

Note: This may take about 25 minutes to complete.

5. Run the following command as user *root* on the secondary server to bring it online:
`service heartbeat start`
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 *ESM High Availability Module User's 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.

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

Route Metric Size Issue:

If the route metric for the route associated with the Service-IP interface is larger than that of the default route this may cause pacemaker problems determining the netmask. One of the symptoms of this problem is pairs of messages in `/var/log/messages`:

```
'....: info: RA output: (Service-IP:start:stderr) ERROR: Cannot use default
route w/o netmask...'
'...: ERROR: [/usr/lib64/heartbeat/findif -C] failed...'
```

If these messages appear, run the following steps on the primary and secondary servers:

1. Run this command:
`ip route`
Results should be several lines including some similar to the following (in this example, the Host IP address is 12.34.156.78).
`default via xxx.xxx.xxx.xxx dev ens32 proto static metric 100`
`12.34.128.0/19 dev ens32 proto kernel scope link src 12.34.156.78 metric 1000`
2. Identify the Network ID and metric specified for:

- a. Default
 - b. Host IP (this line should include the Host IP)
3. If the metric is larger for the Host IP route than for the default route, run the following commands as user *root*:
- ```
ip route replace <CIDR and interface> metric <default route metric>
ip route delete <CIDR and interface> metric <host route metric>
```
- In the example, these commands would be:
- ```
ip route replace 12.34.128.0/19 dev ens32 metric 100  
ip route delete 12.34.128.0/19 dev ens32 metric 1000
```

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 HA Environment on ESM 6.11.0 Patch 1 to RHEL 6.9 or CentOS 6.9 (ESM 6.11.0 Patch 1)

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!