

Upgrade HA Environment on ESM 6.8c to Support RHEL 6.6

This document provides information on how to upgrade ESM 6.8c (with High Availability (HA)) implemented on RHEL 6.5 to support RHEL 6.6. The starting state (before upgrade) is assumed to be:

- ESM 6.8c with the latest patches
- HA implemented on the primary and secondary servers
- RHEL 6.5 (on both primary and secondary servers)

To perform the upgrade:

- 1 Run the following `chkconfig` command 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 install HA, and to upgrade to RHEL 6.6.

- a Upgrade the operating system to RHEL 6.6.

- b Copy the HA upgrade to the server.

- c Install the HA upgrade using these commands:

- i `tar -xzf HAUpdateForRHEL6.6.tgz`

- ii `cd HAUpdateForRHEL6.6`

- iii `yum -y update *.rpm`

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

```
service heartbeat start
```

- 6 Repeat steps 3 through 5 on the primary server. It is expected that ESM will go down while the primary server is updating.
- 7 Run the following command as user *root* on the secondary server to take it off standby:
`crm_standby -D`
- 8 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`
- 9 Copy Patch 2 to the primary server and install it as directed, including stopping or removing services.

Copyright © 2016 Hewlett-Packard Development Company, L.P. Follow this link to see a complete statement of copyrights and acknowledgements: <http://www.hpenterprisesecurity.com/copyright>

January 12, 2016