**Step 1: Preparing your new hardware**

During this step, the administrator needs to first verify the software version from the deployment. If required, complete a QRadar install on the new hardware. The installation of the new appliance uses a temporary IP address until the old hardware is removed from the deployment later on.

**Step 2: Preparing your old Console appliance**

During this step, the administrator needs to verify they have a recent configuration backup file from the old Console. If a recent configuration backup does not exist, then administrators can use the procedure below to create an On-Demand Backup.

By default, configuration backups are stored in /store/backup on the QRadar Console and a recent backup should be copied to a safe location, such as the administrator’s workstation or another QRadar system in the deployment.

**Step 3: Reassigning IP addresses on the old Console appliance**

The administrator is now ready to change the IP address of the old Console to an unused or decommissioned IP range. This will be done -manually- by adjusting the network configuration file directly, **not using the common “qchange\_netsetup” command**.

Using this method, allows for the changing of the physical IP address of the system to avoid conflicts, but also allows for quick reversion to the old address, in the event the backup restore does not complete successfully on the new system. After the IP address is changed on the existing console, it cannot reach/effect any changes to the other hosts in the deployment, until/unless the ip address is reverted, if required.

**Step 4: Setting IP addresses on the new Console appliance**

At this point, the new console hardware will assume the ip address of the old console. To make this change, use the qchange\_netsetup command.

**Step 5: Moving certificates and custom generated private/public key pairs (as required)**

Appliances that manage scanners and log sources that authenticate should copy the certificates from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources. If the administrator has custom generated private keys, these also need to be migrated by transferring /etc/ssh and /root/.ssh directories.

**Step 6: Restoring the configuration backup to the new Console appliance**

The configuration backup from the old Console can now be applied to the new hardware. In most cases, it is recommended that the administrator uses secure copy (SCP) to move the file to the QRadar Console.

The backup import facility in the User Interface (UI) has a size limit of 512 MBs. If your environment has a large configuration, the configuration backup size may grow beyond what the UI supports.

**Step 7: How to transfer event and flow data to the new hardware**

The attached utility was designed by QRadar L3 engineering to facilitate moving data from /store/ariel of an old appliance to a new appliance. Data is moved in one month intervals to keep performance impact at a minimum.

This utility does not move certificates or configurations, only data is /store/ariel/; however, it does leverage rsync, so SSH traffic must be allowed to migrate the data. The administrator might be required to accept SSH keys and provide root password for the target server to stat the transfer.

**Step 8: Migration complete**

At this point, the migration should be complete. You may want to keep the old console on hand for a few days to ensure there are no other issues that may arise that requires you to revert to the old appliance.