aruba
NETWORKS

1344 CROSSMAN AVE
SUNNYVALE, CA 94089

T: 1.408.227.4500
FAX: 1.408.227.4550

WWW.ARUBANETWORKS.COM

Field Bulletin: ARUBA-PFB-20150430_Leap_Second **Revision: 4** (May 22, 2015)
Confidentiality Level: Aruba Customers & Partners only

Aruba Products and June 30th 2015 Leap Second

Products covered in the advisory

- Aruba Mobility Controllers
- Aruba Instant
- Aruba AirMesh Routers
- Aruba Mobility Access Switches
- AirWave Management Platform
- ClearPass Policy Manager
- Analytics and Location Engine

Summary

The International Earth Rotation and Reference Systems Service has decided to insert a one-second adjustment known as Leap Second to ensure the Coordinated Universal Time (UTC) is in sync with solar/astronomical time. These Leap Seconds are irregularly timed in response to changes in the Earth's rotation. Such a leap second adjustment is expected to occur on June 30th, 2015.

Reference: http://www.nist.gov/pml/div688/leapseconds.cfm

This advisory is to notify which Aruba products and software releases may be affected by this time adjustment and provide guidance on workarounds or software patches.
This advisory will be updated as additional/relevant information becomes available.

Affected Products

- Aruba Mobility Controllers – 7200 Series and 7000 Series Controllers
- Aruba Instant – IAP-134/135, RAP-155/155P, IAP-114/115, IAP-103, IAP-204/205, IAP-214/215, IAP-224/225, IAP-274/275
- ClearPass Policy Manager – All Versions
- AirWave Management Platform – All Versions
- Analytics and Location Engine – All Versions

What Products Are NOT Affected?

- Aruba Mobility Controllers – M3Mk1, 3000 series and 600 series
- Aruba Instant – IAP-92/93, IAP-104/105, RAP-3WN/3WNP, IAP-175, RAP/IAP-108, RAP/IAP-109 running InstantOS 4.0.0.10 or above release
- Aruba Mobility Access Switches
- Aruba AirMesh Routers

Call to action

Aruba Mobility Controllers

- Aruba M3MK1, 3000 Series and 600 Series controllers are NOT affected.

- Aruba 7200 Series and 7000 Series Controllers are affected.
  The fixes require making significant changes to the ArubaOS kernel which we have elected not to do at this time.

  1. Disable NTP services at least 24 hours prior to June 30, 2015 and then re-enable NTP services 24 hours afterwards. The controller will not require a reboot when NTP is disabled and re-enabled.
  2. If there are large numbers of controllers, blocking NTP updates to the controllers 24 hours prior to June 30, 2015 may be preferred. This would minimize the number of changes required.

Q. What happens if NTP is not disabled on the controller?

There is a high chance that the controller will reboot.

Q. Do I need to worry about this if NTP is not enabled?

The controller is not affected if NTP is not enabled.

Q. What is different with leap second this year vs. previous years?

The leap second adjustment affected devices with kernel running specific versions. The kernel version running on the M3, 3000 series and 600 series are NOT affected. The 7200 and 7000 series controller are affected and our exposure may have been minimized because the 7200 platform was just ramping up.

- ## Aruba Instant

  - Following IAP models are NOT Affected:

    IAP-92/93, IAP-104/105, RAP-3WN/3WNP, IAP-175, RAP/IAP-108, RAP/IAP-109 running InstantOS 4.0.0.10 or later release are NOT affected.

  - Any other IAP model that is not in the above list is affected.

    To mitigate the issue, disable NTP services at least 24 hours prior to June 30, 2015 and then re-enable NTP services 24 hours afterwards.

    Blocking NTP updates to the IAP cluster or disconnecting the NTP server 24 hours prior to June 30, 2015 can be used as a workaround.

Q. What happens if NTP is not disabled on the IAP?

There is a high chance that the IAP will reboot.

Q. Do I need to worry about this if NTP is not enabled?

The IAP is not affected if NTP is not enabled.

Q. How to disable NTP service on IAP?

Configure the NTP server to an unreachable IP/domain.

- ## AirWave Management Platform

  - Airwave 8.0.8 is available for download and will address the leap second.
  - Customers who are using NTP will not be affected.
  - Customers with older versions of Airwave who do not use NTP can update the tzdata package with this command:

    ```
    # yum update tzdata\*
    ```

  - Customers who don't use NTP and don't update the tzdata package will end up with the clock off by a second (assuming it was correct in the first place). We don't anticipate any other side effects.

- ## Analytics and Location Engine

Customers should use the following command to update CentOS.

```
# yum update tzdata\*
```

- ## ClearPass Policy Manager

ClearPass versions 6.2 and higher include updates to address potential leap second related issues. However, recent test scripts supplied by RedHat indicate that ClearPass is still susceptible and not fully compliant to handle the upcoming leap second, irrespective of whether NTP is enabled or not. Disabling NTP is also not a recommended practice for ClearPass installations as it can create severe authentication-related issues.

To ensure system stability and avoid any unforeseen system hang or crash, we encourage customers to install the "Leap Second Update Patch for ClearPass 6.x.x" which was released on May 12th, at the earliest opportunity before June 30th, 2015. This out-of-cycle patch is being provided for the following actively supported releases as well as End of Development/Support releases:

- ClearPass Policy Manager 6.2.6
- ClearPass Policy Manager 6.3.6
- ClearPass Policy Manager 6.4.x
- ClearPass Policy Manager 6.5.0/6.5.1

This patch will also be included in future software releases such as ClearPass 6.5.2.

Please use any of the methods listed below to install the patch.

A. Installing the Patch Online Using the Software Updates Portal:

1. Open ClearPass Policy Manager and go to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware and Patch Updates** area, find the **ClearPass Leap Second Update** patch and click the **Download** button in its row.
3. Click **Install**.

4. When the installation is complete and the status is shown as **Needs Restart**, proceed to restart ClearPass. After reboot, the status for the patch will be shown as **Installed**. The ClearPass Policy Manager version number will not change.

B. Installing the Patch Offline Using the Patch File from support.arubanetworks.com and HTTP:

1. Download the appropriate **ClearPass Leap Second Update** from the Support site.
2. Post the patch file to a local HTTP server.
3. Open an SSH session to the ClearPass appliance using the ‘appadmin’ account.
4. Type '**system update –i <http location of the file>**’
5. When the installation is complete, issue ’**system restart**'. After reboot, the status for the patch will be shown as **Installed**. The ClearPass Policy Manager version number will not change.

C. Installing the Patch Offline Using the Patch File from support.arubanetworks.com and SCP:

1. Download the appropriate **ClearPass Leap Second Update** from the Support site.
2. Post the patch file to a local SCP server.
3. Open an SSH session to the ClearPass appliance using the ‘appadmin’ account.
4. Type '**system update –i < user@<scp location of the file>**'
5. When the installation is complete, issue ’**system restart**'. After reboot, the status for the patch will be shown as **Installed**. The ClearPass Policy Manager version number will not change.

D. Installing the Patch Offline Using the Patch File from support.arubanetworks.com:

1. Download the appropriate **ClearPass Leap Second Update** from the Support site.
2. Open the ClearPass Policy Manager Admin UI and go to **Administration > Agents and Software Updates > Software Updates**.
3. At the bottom of the **Firmware and Patch Updates** area, click **Import Updates** and browse to the downloaded patch file.
4. Click **Install**.
5. When the installation is complete and the status is shown as **Needs Restart**, proceed to restart ClearPass. After reboot, the status for the patch will be shown as **Installed**. The ClearPass Policy Manager version number will not change.

Aruba is committed to proactively communicating recommendations on code versions, features and functionality to ensure optimal network operation and customer satisfaction. Please feel free to contact the Aruba Technical Assistance Center (TAC) team if you need further clarifications regarding this bulletin. The Aruba technical support e-mail is support@arubanetworks.com. The Aruba TAC team will facilitate further product related discussions with the product management team for customers that desire to do so.