WHITE PAPER

Automated Network Operating System Device Upgrades

apstra®

Table of Contents

Introduction

Network Device OS Upgrades are a required function in any modern enterprise. The OS can be affected by known or unknown bugs, security vulnerabilities, or more. The operator may also wish to upgrade the OS in order to activate a new feature. Whatever the reason is, with a fixed form factor device with a single CPU (or supervisor), we can expect some sort of outage due to the reload process during upgrades.

Here is a common experience for all network operators. A device upgrade is scheduled and all application owners are informed about the planned outage. The operator connects to the device via SSH and performs the file copy, changes the bootloader command to point to the new image, and issues the reboot command. Immediately all of the phones in the NOC begin ringing. It seems that the unfortunate operator typed .16 instead of .15 when setting up the SSH session, and has mistakenly rebooted the wrong device which had a large amount of traffic flowing through it at that moment. In addition, the device returned to operation after the reboot with new default settings in the configuration and also rejected several existing commands that were critical for service. The Ethernet management port cannot be reached, and the console port is not responding. The operator now has to grab a laptop and console cable and literally run down to the datacenter as fast as possible and connect to the device at 9600bps over a terminal emulator to manually check the large configuration by hand. As he or she runs through the building, they can hear shouting and complaints from every open door and cubicle. Like the device itself, the business is "down hard".

The example in this story is what we often refer to as a "resume generating event". But it is not the operator's fault, humans make mistakes. Typos occur in every few sentences. Not only was the operator not protected from making changes to devices that were in service, but there was no pre or post validation that the upgrade would be successful.

Even though network device upgrades are nicely packaged as a single file, the upgrade process is frequently problematic, as a result of the number of services that can theoretically be affected by upgrading a single device. For example, without adequate planning and organization, the upgrade of a core router can cause an interruption for all businesses at once. Network operators want a simple process that is guaranteed to work, with a higher level workflow that can manage simultaneous upgrades as well as upgrades across multiple vendor types. Since most vendors have a different procedure for the upgrade/downgrade process (POAP, ZTP, ONIE), that can be a somewhat tall order.

AOS supports Device Operating System (DOS) Upgrades for managed switches, allowing the operator to upgrade devices directly from the AOS Server within a consistent workflow process.

The following DOS upgrades are supported:

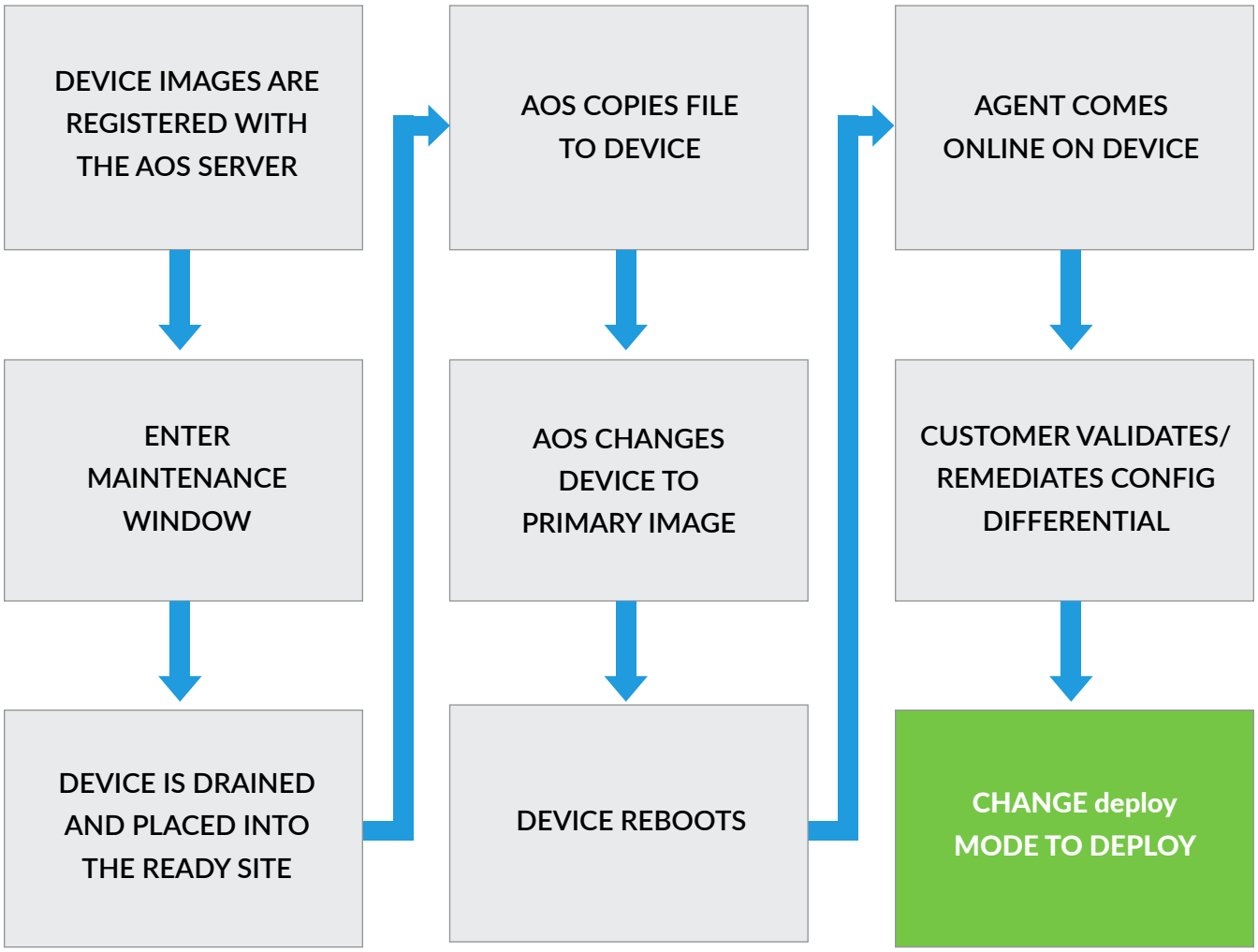
- Cisco NX-OS
- Arista EOS
- Cumulus Linux

All activities related to Device OS Upgrades are performed by the AOS Server. The AOS Agent running on the switch is NOT used for any of these workflows.

RECOMMENDATION 1:

Use AOS Maintenance Mode (Drain/Undrain) to remove all application traffic from the devices you wish to upgrade. Following the successful drain, change the deploy mode to Ready, which will remove the Service Config from the device (effectively eliminating it as a router in the topology). Placing the device into the Ready state will also eliminate the possibility of anomalies when the device reloads.

Device OS Upgrade Process - NX-OS, EOS



Device OS Upgrade Process - Cumulus Linux

For Cumulus the workflow is the same as the other platforms. Since as part of the upgrade the device is reset to factory state, there are a number of additional steps:

The AOS user is re-created after the upgrade. This ensures continued access by AOS and Agent operation

- The AOS agent is re-installed
- The Cumulus License is re-installed
- AOS base configuration is re-applied (management VRF)

Note: *When upgrading a Cumulus device AOS uses ONIE to upgrade to the new image and reset the device to factory state. For Cumulus it is imperative to have the same IP address before and after the upgrade. A DHCP server with a static DHCP assignment must be in place before any upgrade can be completed. More details can be found in the AOS documentation.*

After advanced preparation tasks are completed, Device OS Upgrade works as follows:

1. Select Devices from the AOS Devices > Agents page.
2. Select Upgrade action for a device. A dialog box presents all the images for the platform the device is currently running on.
3. Summarize and confirm the Device OS upgrade process.
4. Network Devices download the Device OS image.
5. Network Devices reload themselves with the new Device OS image.

Preparation

Register Device OS Images

The user will need to register Device OS images (e.g. EOS-4.18.4.1F.swi, nxos.7.0.3.I7.2.bin) with the AOS server. A dialog box similar to package installation page prompts the users for the following information:

- Path to local image or external link
- Platform
- Version
- Checksum - sha512sum (optional)

The AOS server will have an "images" directory `(/opt/aos/images/<platformnos_type>/version)` that the user can upload images via AOS UI. The options for <platformnos_type> include:

- **arista-eos - Arista EOS**
- **cisco-nxos - Cisco NXOS**
- **cumulus - Cumulus Linux**

Check OS Storage on Devices

The administrator needs to verify that there is enough space on each device before attempting the OS upgrade. This is not currently automated by AOS and OS upgrades will fail if there is not enough space or if the file system is corrupted.

For Arista upgrades, the process requires enough FLASH space to fit three images, two for the current image (on boot Arista makes a copy), and one for the new upgrade image. Prior to downloading the new image, we must delete any *swi files which are not the current image and the future upgrade image to make space for the boot. If there is not enough space for the copy of the boot image, upgrade will fail asking users to free up space. Otherwise systems on upgrade will end up in the boot prompt which is not desired.

Check MLAG Devices for Upgrade Compatibility

AOS does not currently have features to detect or remediate issues related to mixed version MLAG pairs. If the operator intends to upgrade an MLAG pair, either both switches should be upgraded at the same time, or due care should be taken to review the vendor's known bug list for the versions in question to ensure that an MLAG peer group with mixed NOS versions can be supported.

RECOMMENDATION 3:

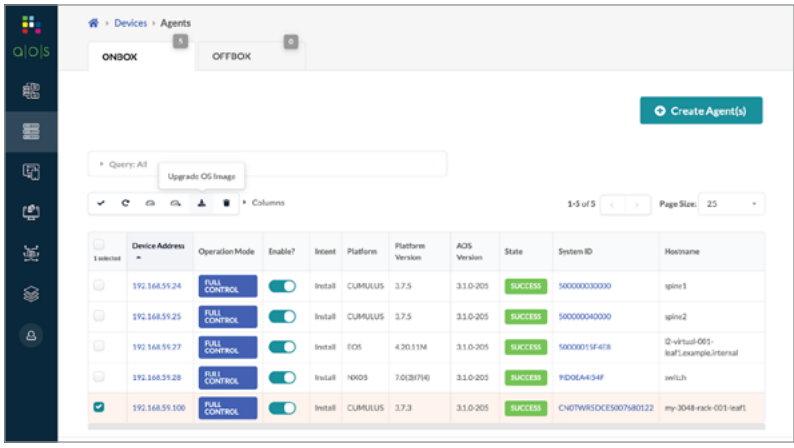
Always review the known issues, bug list and caveats for each release to ensure that the active features will not be affected on devices.

Upgrade Sequence

Note: *It is the user's responsibility to make sure the proper switches are selected for redundant upgrades. AOS will not verify device redundancy status for the Device OS upgrade process.*

Selecting Devices

Device OS Management is done from the "Devices", "Agents" page.



The user selects devices (from the same platform) from the list of devices. All devices selected will be upgraded to the same registered OS image file.

After selecting the devices to upgrade, the user clicks the "DOS Upgrade" button. If the set of devices is not valid, then an error dialog box explains why an upgrade can not be initiated. For example, if the user chose both EOS and NXOS systems, then on Upgrade an error dialog appears indicating that different platforms were selected.

Select Device OS Image

Assuming the selected devices are valid, a dialog appears presenting the list of registered OS images for that platform. Device selection is valid when all devices are the same platform and that platform is in the supported set. As of AOS 2.3, the supported platform set is EOS and NXOS.

AOS UI will list available Device OS images matching the selected Devices. The user will select a single image for the Device OS upgrade.

Note: *The user can use the same upgrade process to "downgrade" the Device OS.*

After the user selects valid network devices and clicks the "DOS Upgrade" button, a new upgrade job is scheduled.

Confirm Upgrade

AOS will confirm the Device OS upgrade with the user. AOS will list the current and target Device OS for each device.

AOS will verify available disk space for each device and will delete old images on the device to make room for the new image. At a minimum, AOS will keep the current image. If AOS is unable to make space is available for the device, AOS will display an error for that device.

Upgrade Status

On the list of Device Agents, "Active Tasks" list will list the status upgrade tasks.

The Active Tasks list will include the following information:

- **Management IP**
- **Job Type**
- **State**
  - **In Progress -** take name shows the current upgrade action
  - **Success** - Device successfully reloaded, new Device OS image verified
  - **Failed** - Success criteria is not met within defined timeout, error message provides additional failure information. Each platform provides numerous error messages for example:
    - Not enough space on device to upgrade OS. Free up space.
    - file <image os name> failed SHA512 verification

Upload Image to Devices

AOS will begin the process of upgrading the network devices.

1. AOS will upload the target Device OS image to the Device being upgraded from the AOS server. AOS will do as many simultaneous uploads as possible until the target Device OS image has been uploaded to all devices in the upgrade group.
2. Device installer will verify the Device OS image using the platforms SHA checksum convention.

If an error occurs during the upload process, an error will be raised. The user will have to correct the error and resubmit a new upgrade.

Validate Checksum on Device

AOS will automatically validate the checksum of the uploaded file against the defined checksum if one was provided during the image registration process. If the checksum does not validate the upgrade will fail.

Modify Boot Parameter and Reload Device

AOS will automatically change the boot file statements to match the new image that has been uploaded. AOS will then begin the process of reloading the network devices:

ARISTA

```
router#conf t

router(config)#boot system flash:
vEOS-lab-4.20.1F.swi

router(config)#exit

router#reload now
```

CISCO

```
switch# install all nxos
bootflash:nxos.7.0.3.I7.3.bin

switch# reload now
```

CUMULUS

```
This function is handled by the
onie-install command listed above.
```

Once the device upgrade is complete, the upgrade process will verify the device is back online.

Accept Device Config Diffs

In various operating systems, some parts of running configuration may change - for example boot filename, boot time, MLAG neighbor version, and sometimes some parts of configuration are cosmetically re-ordered. Devices including Cisco NX-OS will report a new version, and AOS will treat it as a configuration anomaly. This can be accepted as the new Pristine Config by going into the device and clicking the Accept Changes button after reviewing the configuration changes. These changes are mostly cosmetic, and safely accepted. AOS does not automatically accept these cosmetic changes in case there is something AOS doesn't recognize, so the administrator must approve them.

Certify Device

Device validation and certification is performed by the admin and can be augmented with custom IBA probes. Apstra recommends doing the following after devices come online after rebooting:

- Check for generic anomalies
- Check for configuration differential anomalies
- Resolve config diff anomalies (after review) by clicking "Accept Changes"
- Reenable any paused IBA probes related to this device
- Place the device into the Ready state before switching to the mode to Deploy

Restore Device to Service

In the blueprint the device is assigned to, switch the device Deploy Mode from Drain back to Deploy and commit.

Advanced Workflow Script Example

This workflow is an example of how to perform a rolling upgrade of the DOS in a fabric. This process should be automated outside of AOS by leveraging the AOS APIs.

1. Select all devices of role “spine”
2. Drain device1
3. Wait for no anomalies
4. Change device to ready
5. Wait for no anomalies
6. Upgrade DOS
7. Wait for system-agent to complete the upgrade process, with devices ending in READY status in system-agent UI
8. Potential Config Diffs - User Intervention
9. Accept Changes
10. Change device to deploy
11. Wait for no anomalies
12. Select device2
13. Repeat

Conclusion

AOS was designed to improve the lives of operators and increase the efficiency of businesses by rapidly upleveling the capabilities of the people who manage these systems. Prior to using AOS, a major financial services company had a single engineer working on OS upgrades, taking upwards of 8 months to upgrade 174 switches. The same tasks could have been completed with AOS Maintenance Mode and Device OS Upgrade in approximately 87 hours. In fact, with parallel OS upgrade job support, the entire network could have been upgraded in a single day.

www.apstra.com

sales@apstra.com
1-844-9APSTRA
333 Middlefield Rd, Menlo Park, CA 94025

apstra®