



Update your AFF and FAS firmware using Ansible Playbook

Digital Advisor

NetApp

November 07, 2025

Table of Contents

Update your AFF and FAS firmware using Ansible Playbook	1
Download AFF and FAS firmware Ansible Automation package	1
Before you begin	1
Install and execute AFF and FAS firmware Ansible automation package (Experienced Users)	1
Firmware update with Ansible using NetApp Docker Image	2
Firmware update if Ansible is already used	3
Install and execute AFF and FAS firmware Ansible automation package (beginners)	4
Host firmware files using web server	4
Work with inventory file	4
Execute Ansible Playbook using NetApp Docker image	6
Execute Ansible Playbook without NetApp Docker image	7
Validate firmware installation	8

Update your AFF and FAS firmware using Ansible Playbook

Download AFF and FAS firmware Ansible Automation package

You should update the AFF and FAS firmware using Ansible to mitigate the identified risks and keep your storage system up to date.

Before you begin

Before updating AFF and FAS firmware using Ansible, you should:

- [Install and set up Ansible on your storage system](#)
- [Install Ansible 2.9 with collections on your storage system](#)
- Upgrade your storage system to ONTAP 9.1 or later
- Configure your account with an administrator role

Steps

1. Click any wellness widget on the dashboard or click **View All Actions** to view a list of all the actions and risks.
2. Click **Firmware Upgrade** to view all firmware upgrade risks.
3. Click **Update AFF and FAS Firmware** to view all available update packages or click  next to each risk to update the package specific to that risk.
4. Click **Download** to download the zip files and update your storage system.

The zip file contains the following:

- Ansible Playbook - A YAML file containing the Ansible script to perform the disk, shelf, and service processor firmware updates.
- Inventory - A YAML file containing the details of the systems that are applicable for firmware updates.
- Disk, Shelf, and Service Processor/BMC Firmware packages are named as **all.zip**, **all_shelf_fw.zip**, and **<SP/BMC>_<version_number>_fw.zip** respectively.



Manual addition of clusters and controllers to the inventory file is not supported.

Install and execute AFF and FAS firmware Ansible automation package (Experienced Users)

Experienced users can install and execute the AFF and FAS firmware ansible automation package quickly.

Firmware update with Ansible using NetApp Docker Image

Steps

1. Pull the Ansible Docker image to the Linux host:

```
$ docker pull schmots1/netapp-ansible
Using default tag: latest
latest: Pulling from schmots1/netapp-ansible
docker.io/schmots1/netapp-ansible:latest
```

2. Run the docker image as a container on the Linux host:

```
$ docker run -v <downloaded_playbook_path>:<container_path> -it
schmots1/netapp-ansible:latest /bin/bash
```



The Ansible Playbook and the inventory file should be in the same path.

3. Execute the Ansible Playbook on the Linux host. Firmware updates run in the background for a few hours.

```
$ cd <container_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*****
```



If the URLs for disk firmware, shelf firmware, and service processor firmware are http://<web-server>/path/all_shelf_fw.zip, <http://<web-server>/path/all.zip> and http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip, provide <http://<web-server>/path/> as the input for the base URL to the firmware package. If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

4. Log in to the cluster as the cluster administrator and verify that the new drive firmware has been installed:

```
::> storage disk show -fields firmware-revision,model
disk      firmware-revision model
-----
1.11.0    NA01          X423_HCOBE900A10
1.11.1    NA01          X423_HCOBE900A10
1.11.2    NA01          X423_HCOBE900A10
1.11.3    NA01          X423_HCOBE900A10
1.11.4    NA01          X423_HCOBE900A10
```

Firmware update if Ansible is already used

Steps

1. Install Python and Ansible and then download the Python packages using PIP:

```
$ pip install netapp-lib requests paramiko

Installing collected packages: netapp-lib, requests, paramiko
Successfully installed netapp-lib-2020.3.12 requests-2.23.0 paramiko-
2.7.2
```

2. Install the NetApp Ansible Collection:

```
To install the collection only for the current user:
$ ansible-galaxy collection install netapp.ontap
```

```
For universal installation:
$ ansible-galaxy collection install netapp.ontap -p
/usr/share/ansible/collections
$ chmod -R +rw /usr/share/ansible/collections
```

3. Ensure that the Ansible Playbook and the inventory file are in the same path and then execute the Ansible Playbook. Firmware updates run in the background for a few hours.

```
$ cd <playbook_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware_disk.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*****
```



If the URLs for disk firmware, shelf firmware, and service processor firmware are `http://<web-server>/path/all_shelf_fw.zip`, `http://<web-server>/path/all.zip` and `http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip`, provide `http://<web-server>/path/` as the input for the base URL to the firmware package. If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

4. Log in to the cluster as the cluster administrator and verify that the new drive firmware has been installed:

```
::> storage disk show -fields firmware-revision,model
disk      firmware-revision model
-----
1.11.0    NA01          X423_HCOBE900A10
1.11.1    NA01          X423_HCOBE900A10
1.11.2    NA01          X423_HCOBE900A10
1.11.3    NA01          X423_HCOBE900A10
1.11.4    NA01          X423_HCOBE900A10
```

Install and execute AFF and FAS firmware Ansible automation package (beginners)

Host firmware files using web server

After you download the automation package, the firmware files should be hosted on a web server.

The web server can be set up in multiple ways. For instructions to set up a simple web server using Python, refer to [Webserver using Python](#).

Step

1. Save the base URL of the web server. If the URLs for disk firmware, shelf firmware, and service processor firmware are `http://<web-server>/path/all_shelf_fw.zip`, `http://<web-server>/path/all.zip`, and `http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip`, save `http://<web-server>/path/` as the base URL.

The filename is automatically detected by the Ansible Playbook.

Work with inventory file

The inventory file consists of the cluster management LIFs of the systems that are eligible for firmware updates. It contains the list of clusters with disk and shelf firmware filename information wherever applicable.

For service processor firmware update, node hostnames and SP/BMC IP is included in the inventory file.

Inventory file format

The following is a sample inventory file format with both disk and shelf firmware updates:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
    shelf_fw_file: all_shelf_fw.zip

  - clustername: <cluster management LIF-2>
    disk_fw_file: all.zip
    sp_nodes:
      - hostname: <node hostname 1>
        sp_fw_file: SP_FW_308-03990_11.5.zip
        sp_fw_type: bmc
        sp_fw_ver: '11.5'
        sp_ip: <BMC IP>
      - hostname: <node hostname 2>
        sp_fw_file: SP_FW_308-03991_5.8.zip
        sp_fw_type: sp
        sp_fw_ver: '5.8'
        sp_ip: <SP IP>
```

In the example, both shelf and disk firmware updates are applicable on cluster-1 and disk and SP/BMC firmware updates are applicable on cluster-2.

Delete a cluster from the inventory file

In case you do not want to apply firmware updates on a particular cluster, you can remove the cluster from the inventory file.

For example, if you do not want to apply disk firmware updates on cluster-2, you can remove it from the inventory file using the following command:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
    shelf_fw_file: all_shelf_fw.zip
```

You can observe that all the data for cluster-2 has been deleted.

If you want to apply only disk firmware updates on cluster-1 and not shelf firmware updates, you can do so using the following command:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
```

You can see that the `shelf_fw_file` key and value have been removed from cluster-1.



Manual addition of clusters or controllers is not supported.

Execute Ansible Playbook using NetApp Docker image

Before you execute the Ansible Playbook, ensure that the **NetApp_Ansible_*.zip** file has been extracted and the web server with disk or shelf firmware files is ready.

Before you begin

Before executing Ansible Playbook using NetApp docker, you should:

- [Download AFF and FAS firmware Ansible Automation package](#)
- [Host the firmware files using the web server](#)
- [Work with the inventory file](#)
- Ensure that NetApp Docker is installed.

Steps

1. [Set up Docker](#).
2. Pull the NetApp Docker image from DockerHub by executing the following command:

```
$ docker pull schmots1/netapp-ansible

Using default tag: latest
latest: Pulling from schmots1/netapp-ansible
docker.io/schmots1/netapp-ansible:lates
```

For more information about the docker pull command, refer to the [Docker Pull Documentation](#).

3. Run the Docker image as a container and log in to the container to execute the Ansible Playbook.
4. Copy the path of the folder which contains the extracted Ansible Playbook and inventory files, for example, **downloaded_playbook_path**. The Ansible Playbook and inventory files should be in the same folder for successful execution.
5. Mount the folder as a volume on the Docker container. For example, to mount the folder **container_path**, you should execute the following command:

```
$ docker run -v <downloaded_playbook_path>:<container_path> -it
schmots1/netapp-ansible:latest /bin/bash
```

The container starts and the console is now at bash shell of the container. For more information about the Docker Run command, refer to the [Docker Run Documentation](#).

6. Execute the Ansible Playbook inside the container using the **ansible-playbook** command:

```
$ cd <container_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*****
```



If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

For more information about the **ansible-playbook** command, refer to the [Ansible Playbook Documentation](#) and to execute the Ansible playbook in check mode (dry run), refer to [Ansible: Check mode](#).

After executing the Ansible Playbook, refer to the [Firmware Installation Validations](#) for post-execution instructions.

Execute Ansible Playbook without NetApp Docker image

Steps

1. Install [Python](#) and [Ansible](#).
2. Install the required Python packages using **pip**:

```
$ pip install netapp-lib requests paramiko

Installing collected packages: netapp-lib, requests, paramiko
Successfully installed netapp-lib-2020.3.12 requests-2.23.0 paramiko-2.7.2
```

3. Install NetApp Ansible collection using the **ansible-galaxy** command:

```
To install the collection only for the current user
$ ansible-galaxy collection install netapp.ontap
```

```
To do a more universal installation,
$ ansible-galaxy collection install netapp.ontap -p
/usr/share/ansible/collections

$ chmod -R +rw /usr/share/ansible/collections
```

For more information about the `ansible-galaxy` command, refer to [Ansible Galaxy Documentation](#) and for more information about the NetApp Ansible Collection, refer to the [NetApp Ansible Collection page](#).

4. Execute the Ansible Playbook using `ansible-playbook` command:

```
$ cd <downloaded_playbook_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*****
```



If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

For more information about the `ansible-playbook` command, refer to the [Ansible Playbook Documentation](#) and to execute the Ansible Playbook in check mode (dry run), refer to [Ansible: Check mode](#).

After executing the playbook, refer to the [Firmware Installation Validations](#) for post-execution instructions.

Validate firmware installation

After the execution of the playbook, log in to the cluster as the cluster administrator.

Validate disk firmware installation

Steps

1. Verify that the drive firmware is installed:

```
::*> storage disk show -fields firmware-revision,model
disk      firmware-revision model
-----
1.11.0    NA01          X423_HCOBE900A10
1.11.1    NA01          X423_HCOBE900A10
1.11.2    NA01          X423_HCOBE900A10
1.11.3    NA01          X423_HCOBE900A10
1.11.4    NA01          X423_HCOBE900A10
```

For more information about the command, refer to [storage disk show](#).

2. Verify that the new NVMe Flash Cache firmware is installed:

```
::*> system controller flash-cache show
```

For more information about the command, refer to [system controller flash-cache show](#).

Validate shelf firmware installation

Steps

1. Verify that the new shelf firmware is updated:

```
::*> system node run -node * -command sysconfig -v
```

In the output, verify that each shelf's firmware is updated to the desired level. For example:

```
Shelf 1: IOM6 Firmware rev. IOM6 A: 0191 IOM3 B: 0191
```

For more information about the command, refer to [system node run](#).

2. Verify that the new ACP firmware is updated:

```
::*> storage shelf acp module show -instance
```

For more information about the command, refer to [storage shelf acp module show](#).

3. Verify that the desired ACP mode is configured:

```
::*> storage shelf acp show
```

For more information about the command, refer to [storage shelf acp show](#).

4. Change the ACP mode (channel):

```
::*> storage shelf acp configure -channel [in-band | out-of-band]
```

For more information about the command, refer to [storage shelf acp configure](#).

Validating SP/BMC Firmware installation

The Ansible Playbook for Service Processor/BMC firmware updates is enabled with an option to verify the installation of latest SP/BMC firmware on the controller. After the verification is complete (the updates could take a maximum time of two hours), the Ansible Playbook applies internal switch firmware updates by connecting to the SP/BMC console.

The failure and success information for SP/BMC firmware and the internal switch firmware installations will be notified at the end of Ansible Playbook execution. Follow the steps mentioned in the Ansible Playbook in case the SP/BMC firmware/internal switch firmware installation fails.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.