Actualice el firmware de AFF y FAS con el libro de aplicaciones de Ansible

Digital Advisor

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/es-es/active-iq/task_update_AFF_FAS_firmware.html on April 10, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Actualice el firmware de AFF y FAS con el libro de aplicaciones de Ansible 1
Descargue el paquete de automatización de Ansible con firmware AFF y FAS 1
Instalar y ejecutar el paquete de automatización de Ansible con firmware AFF y FAS (usuarios con experiencia) 1
Instalar y ejecutar el paquete de automatización de Ansible del firmware AFF y FAS (principiantes) 4

Actualice el firmware de AFF y FAS con el libro de aplicaciones de Ansible

Descargue el paquete de automatización de Ansible con firmware AFF y FAS

Debe actualizar el firmware de AFF y FAS con Ansible para reducir los riesgos identificados y mantener actualizado el sistema de almacenamiento.

Antes de empezar

Antes de actualizar el firmware de AFF y FAS con Ansible, debe:

- "Instale y configure Ansible en el sistema de almacenamiento"
- "Instale Ansible 2.9 con colecciones en el sistema de almacenamiento"
- Actualice su sistema de almacenamiento a ONTAP 9.1 o posterior
- Configure su cuenta con una función de administrador

Pasos

1. Haga clic en cualquier widget de bienestar del panel o haga clic en **Ver todas las acciones** para ver una lista de todas las acciones y riesgos.
2. Haga clic en **actualización del firmware** para ver todos los riesgos de actualización del firmware.
3. Haga clic en **Actualizar AFF y firmware de FAS** para ver todos los paquetes de actualización disponibles o haga clic en junto a cada riesgo para actualizar el paquete específico de ese riesgo.
4. Haga clic en **Descargar** para descargar los archivos zip y actualizar el sistema de almacenamiento.

   El archivo zip contiene lo siguiente:

   - Libro de aplicaciones de Ansible: Archivo YLMA que contiene el script de Ansible para realizar actualizaciones del firmware del procesador de servicio, de la bandeja y del disco.
   - Inventario: Archivo YAML que contiene los detalles de los sistemas que se aplican para las actualizaciones de firmware.
   - Los paquetes de firmware de disco, estante y procesador de servicio/BMC se denominan **all.zip**, **all_shelf_fw.zip** y **<SP/BMC>_<version_number>_fw.zip** respectivamente.

No se admite la adición manual de clústeres y controladoras al archivo de inventario.

Instalar y ejecutar el paquete de automatización de Ansible con firmware AFF y FAS (usuarios con experiencia)

Los usuarios con experiencia pueden instalar y ejecutar rápidamente el paquete de automatización de Ansible del firmware AFF y FAS.

Actualización de firmware con Ansible mediante la imagen de Docker de NetApp

Pasos

1. Tire de la imagen de Ansible Docker al host Linux:

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

2. Ejecute la imagen docker como contenedor en el host Linux:

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

> El libro de aplicaciones de Ansible y el archivo de inventario deben estar en la misma ruta.

3. Ejecute el libro de aplicaciones de Ansible en el host Linux. Las actualizaciones de firmware se ejecutan en segundo plano durante unas horas.

```
$ 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]
*****************************************************************
```

> Si las direcciones URL del firmware del disco, del firmware de la bandeja y del procesador de servicio son **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** y **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, proporcione *\http://<web-server>/path/ como la dirección URL del paquete de entrada del firmware base. Si hay un conjunto de clústeres con credenciales de inicio de sesión diferentes, debe ejecutarse el libro de aplicaciones de Ansible en cada clúster. No es necesario realizar ningún cambio en el archivo de inventario, ya que el libro de aplicaciones de Ansible omite los clústeres para los que no se ha podido iniciar sesión.

4. Inicie sesión en el clúster como administrador del clúster y compruebe que el nuevo firmware de la unidad se haya instalado:

```
::> 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
```

Actualización de firmware si ya se utiliza Ansible

Pasos

1. Instale Python y Ansible y, a continuación, descargue los paquetes de Python mediante 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. Instale la colección de Ansible de NetApp:

```
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. Asegúrese de que el libro de aplicaciones de Ansible y el archivo de inventario están en la misma ruta y, a continuación, ejecute el libro de aplicaciones de Ansible. Las actualizaciones de firmware se ejecutan en segundo plano durante unas horas.

```
$ 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]
*****************************************************************
```

> Si las direcciones URL del firmware del disco, del firmware de la bandeja y del procesador de servicio son **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** y **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, proporcione *\http://<web-server>/path/ como la dirección URL del paquete de entrada del firmware base. Si hay un conjunto de clústeres con credenciales de inicio de sesión diferentes, debe ejecutarse el libro de aplicaciones de Ansible en cada clúster. No es necesario realizar ningún cambio en el archivo de inventario, ya que el libro de aplicaciones de Ansible omite los clústeres para los que no se ha podido iniciar sesión.

4. Inicie sesión en el clúster como administrador del clúster y compruebe que el nuevo firmware de la unidad se haya instalado:

```
::> 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
```

Instalar y ejecutar el paquete de automatización de Ansible del firmware AFF y FAS (principiantes)

Aloja los archivos de firmware mediante el servidor web

Después de descargar el paquete de automatización, los archivos de firmware se deben alojar en un servidor web.

El servidor Web se puede configurar de varias formas. Para obtener instrucciones sobre cómo configurar un servidor web sencillo mediante Python, consulte "Servidor web mediante Python".

Paso

1. Guarde la URL base del servidor web. Si las direcciones URL del firmware del disco, del firmware de la bandeja y del procesador de servicio son **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-**

server>/path/all.zip y **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, guarde *\http://<web-server>/URL como la base.

El libro de aplicaciones de Ansible detecta automáticamente el nombre de archivo.

Trabaje con el archivo de inventario

El archivo de inventario consta de los LIF de administración del clúster de los sistemas que pueden optar a las actualizaciones de firmware. Contiene la lista de clústeres con información de nombre de archivo del firmware de disco y bandeja donde sea aplicable.

Para la actualización del firmware del procesador de servicio, los nombres de host de nodos y la IP de SP/BMC se incluyen en el archivo de inventario.

Formato de archivo de inventario

A continuación se muestra un formato de archivo de inventario con actualizaciones de disco y de firmware de bandeja:

```
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>
```

En el ejemplo, las actualizaciones de firmware de la bandeja y del disco son aplicables en las actualizaciones de firmware del clúster-1 y del disco, y del SP/BMC se aplican en el clúster-2.

Elimine un clúster del archivo de inventario

En caso de que no desee aplicar actualizaciones de firmware en un clúster determinado, puede quitar el clúster del archivo de inventario.

Por ejemplo, si no desea aplicar actualizaciones de firmware de disco en clúster-2, puede quitarlo del archivo de inventario con el siguiente comando:

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

Puede observar que se han eliminado todos los datos del clúster-2.

Si desea aplicar solo las actualizaciones de firmware del disco en cluster-1 y no las actualizaciones de firmware de la bandeja, puede hacerlo mediante el siguiente comando:

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

Puede ver que la clave y el valor *shelf_fw_File* se han eliminado del cluster-1.

No se admite la adición manual de clústeres o controladoras.

Ejecute el libro de aplicaciones de Ansible con la imagen de Docker de NetApp

Antes de ejecutar el libro de aplicaciones de Ansible, asegúrese de que se ha extraído el archivo **NetApp_Ansible_*.zip** y que el servidor web con archivos de firmware de disco o bandeja está listo.

Antes de empezar

Antes de ejecutar el libro de aplicaciones de Ansible con el Docker de NetApp, debe:

- "Descargue el paquete de automatización de Ansible con firmware AFF y FAS"
- "Aloja los archivos de firmware mediante el servidor web"
- "Trabaje con el archivo de inventario"
- Compruebe que NetApp Docker esté instalado.

Pasos

1. "Configure Docker".
2. Tire de la imagen de NetApp Docker desde DockerHub ejecutando el siguiente comando:

   ```
   $ docker pull schmots1/netapp-ansible

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

   Para obtener más información acerca del comando docker pull, consulte "Documentación de Docker Pull".

3. Ejecute la imagen de Docker como contenedor e inicie sesión en el contenedor para ejecutar el libro de aplicaciones de Ansible.
4. Copie la ruta de la carpeta que contiene el libro de aplicaciones de Ansible y los archivos de inventario extraídos, por ejemplo, **ruta_de_libro_descargados**. El libro de aplicaciones de Ansible y los archivos de inventario deben estar en la misma carpeta para una ejecución correcta.
5. Monte la carpeta como un volumen en el contenedor Docker. Por ejemplo, para montar la carpeta **Container_PATH**, debe ejecutar el siguiente comando:

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

   El contenedor se inicia y la consola se encuentra ahora en el shell bash del contenedor. Si quiere más información acerca del comando Docker Run, consulte "Documentación de Docker Run".

6. Ejecute el libro de aplicaciones de Ansible dentro del contenedor con el comando **ansible-playbook**:

   ```
   $ 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]
   ***************************************************************
   ```

   Si hay un conjunto de clústeres con credenciales de inicio de sesión diferentes, debe ejecutarse el libro de aplicaciones de Ansible en cada clúster. No es necesario realizar ningún cambio en el archivo de inventario, ya que el libro de aplicaciones de Ansible omite los clústeres para los que no se ha podido iniciar sesión.

Para obtener más información acerca del comando **ansible-playbook**, consulte "Documentación del libro de estrategia de Ansible" Y para ejecutar la tableta Ansible playbook en el modo de comprobación (ejecución en seco), consulte "Ansible: Modo de comprobación".

Después de ejecutar el libro de aplicaciones de Ansible, consulte "Validaciones de instalación del firmware" para obtener instrucciones posteriores a la ejecución.

Ejecute el libro de aplicaciones de Ansible sin imagen de Docker de NetApp

Pasos

1. Instale "Python" y.. "Ansible".
2. Instale los paquetes Python necesarios utilizando **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. Instale la colección Ansible de NetApp con el comando **Ansible-galy**:

```
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
```

Para obtener más información sobre el comando ansible-galy, consulte "Documentación de Ansible Galaxy" Si desea obtener más información sobre la colección de Ansible de NetApp, consulte "Página de la colección Ansible de NetApp".

4. Ejecute el libro de aplicaciones de Ansible con el comando * ansible-playbook*:

```
$ 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]
*****************************************************************
```

> Si hay un conjunto de clústeres con credenciales de inicio de sesión diferentes, debe ejecutarse el libro de aplicaciones de Ansible en cada clúster. No es necesario realizar ningún cambio en el archivo de inventario, ya que el libro de aplicaciones de Ansible omite los clústeres para los que no se ha podido iniciar sesión.

Para obtener más información acerca del comando **ansible-playbook**, consulte "Documentación del libro de estrategia de Ansible" Y para ejecutar el libro de aplicaciones de Ansible en el modo de comprobación (ejecución en seco), consulte "Ansible: Modo de comprobación".

Tras ejecutar el libro de estrategia, consulte "Validaciones de instalación del firmware" para obtener instrucciones posteriores a la ejecución.

Validar la instalación del firmware

Tras ejecutar el libro de estrategia, inicie sesión en el clúster como administrador del clúster.

Validar la instalación del firmware de disco

Pasos

1. Compruebe que el firmware de la unidad esté instalado:

```
::*> 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
```

   Para obtener más información acerca del comando, consulte {link-with-underscores}[storage disk show^].

2. Compruebe que el nuevo firmware de Flash Cache de NVMe esté instalado:

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

   Para obtener más información acerca del comando, consulte {link-with-underscores}[system controller flash-cache show^].

Validar la instalación del firmware de la bandeja

Pasos

1. Compruebe que el nuevo firmware de la bandeja se haya actualizado:

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

   En el resultado, verifique que el firmware de cada bandeja se actualice al nivel deseado. Por ejemplo:

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

   Para obtener más información sobre el comando, consulte {link-with-underscores}[system node run^].

2. Compruebe que se haya actualizado el nuevo firmware de ACP:

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

Para obtener más información sobre el comando, consulte {link-with-underscores}[storage shelf acp module show^].

3. Compruebe que el modo ACP deseado esté configurado:

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

Para obtener más información sobre el comando, consulte {link-with-underscores}[storage shelf acp show^].

4. Cambie el modo ACP (canal):

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

Para obtener más información sobre el comando, consulte {link-with-underscores}[storage shelf acp configure^].

Validar la instalación del firmware del SP/BMC

El libro de aplicaciones de Ansible para las actualizaciones del firmware del procesador de servicios/BMC está habilitado con una opción para verificar la instalación del firmware más reciente del SP/BMC en la controladora. Una vez finalizada la verificación (las actualizaciones pueden tardar dos horas en completarse), el libro de aplicaciones de Ansible PlayBook aplica las actualizaciones de firmware del switch interno conectando con la consola del SP/BMC.

La información de fallo y éxito del firmware del SP/BMC y de las instalaciones de firmware de switch internas recibirán una notificación al final de la ejecución del libro de aplicaciones de Ansible. Siga los pasos mencionados en el libro de aplicaciones de Ansible en caso de que se produzca un error en la instalación del firmware del SP/BMC/switch interno.

Obtenga más información

Puede obtener ayuda y encontrar más información mediante varios recursos.

- "Información sobre solución de problemas"
- "Espacio de trabajo Slack"
- Correo:ng-active-iq-feedback@netapp.com[correo electrónico]
- Botón de asistencia técnica del asesor digital para obtener asistencia y comentarios.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.