Aggiorna il firmware di AFF e FAS utilizzando Ansible Playbook

Digital Advisor

NetApp
April 10, 2024

Sommario

Aggiorna il firmware di AFF e FAS utilizzando Ansible Playbook

Scarica il pacchetto di automazione Ansible del firmware AFF e FAS

È necessario aggiornare il firmware AFF e FAS utilizzando Ansible per ridurre i rischi identificati e mantenere aggiornato il sistema storage.

Prima di iniziare

Prima di aggiornare il firmware AFF e FAS utilizzando Ansible, è necessario:

- "Installare e configurare Ansible sul sistema storage"
- "Installare Ansible 2.9 con raccolte sul sistema storage"
- Aggiorna il tuo sistema storage a ONTAP 9.1 o versione successiva
- Configurare l'account con un ruolo di amministratore

Fasi

1. Fare clic su un widget wellness nella dashboard o fare clic su **View All Actions** (Visualizza tutte le azioni) per visualizzare un elenco di tutte le azioni e i rischi.
2. Fare clic su **firmware Upgrade** (aggiornamento firmware) per visualizzare tutti i rischi di aggiornamento del firmware.
3. Fare clic su **Update AFF and FAS firmware** (Aggiorna firmware e aggiornamento firmware) per visualizzare tutti i pacchetti di aggiornamento disponibili oppure fare clic su accanto a ciascun rischio per aggiornare il pacchetto specifico in base a tale rischio.
4. Fare clic su **Download** per scaricare i file zip e aggiornare il sistema di storage.

   Il file zip contiene quanto segue:

   - Ansible Playbook - un file YAML contenente lo script Ansible per eseguire gli aggiornamenti del firmware del disco, dello shelf e del processore di servizio.
   - Inventario - un file YAML contenente i dettagli dei sistemi applicabili agli aggiornamenti del firmware.
   - I pacchetti di dischi, shelf e processori di servizio/firmware BMC sono denominati rispettivamente **all.zip**, **all_shelf_fw.zip** e **<SP/BMC>_<version_number>_fw.zip**.

> L'aggiunta manuale di cluster e controller al file di inventario non è supportata.

Installazione ed esecuzione del pacchetto di automazione AFF e FAS (utenti esperti)

Gli utenti esperti possono installare ed eseguire rapidamente il pacchetto di automazione AFF e FAS firmware ansible.

Aggiornamento del firmware con Ansible utilizzando NetApp Docker Image

Fasi

1. Estrarre l'immagine di Ansible Docker sull'host Linux:

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

2. Eseguire l'immagine del docker come container sull'host Linux:

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

> Il Playbook Ansible e il file di inventario devono trovarsi nello stesso percorso.

3. Eseguire il manuale Ansible Playbook sull'host Linux. Gli aggiornamenti del firmware vengono eseguiti in background per alcune ore.

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

> Se gli URL del firmware del disco, del firmware dello shelf e del firmware del processore di servizio sono **/http://<web-server>/path/all_shelf_fw.zip**, * http://<web-server>/path/all.zip* e **/http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, fornire * http://<web-server>/path/* come input per l'URL di base del pacchetto firmware. Se sono presenti cluster con credenziali di accesso diverse, è necessario eseguire Ansible Playbook su ciascun cluster. Non sono necessarie modifiche al file di inventario, in quanto Ansible Playbook salta i cluster per i quali l'accesso non è riuscito.

4. Accedere al cluster come amministratore del cluster e verificare che il nuovo firmware del disco sia stato installato:

```
::> 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
```

Aggiornamento del firmware se Ansible è già in uso

Fasi

1. Installare Python e Ansible e quindi scaricare i pacchetti Python usando 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. Installare 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. Assicurarsi che il Playbook Ansible e il file di inventario si trovino nello stesso percorso, quindi eseguire il Playbook Ansible. Gli aggiornamenti del firmware vengono eseguiti in background per alcune ore.

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

> Se gli URL del firmware del disco, del firmware dello shelf e del firmware del processore di servizio sono **/http://<web-server>/path/all_shelf_fw.zip**, * http://<web-server>/path/all.zip* e **/http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, fornire * http://<web-server>/path/* come input per l'URL di base del pacchetto firmware. Se sono presenti cluster con credenziali di accesso diverse, è necessario eseguire Ansible Playbook su ciascun cluster. Non sono necessarie modifiche al file di inventario, in quanto Ansible Playbook salta i cluster per i quali l'accesso non è riuscito.

4. Accedere al cluster come amministratore del cluster e verificare che il nuovo firmware del disco sia stato installato:

```
::> 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
```

Installare ed eseguire il pacchetto di automazione Ansible del firmware AFF e FAS (principianti)

Ospitare i file del firmware utilizzando il server Web

Dopo aver scaricato il pacchetto di automazione, i file del firmware dovrebbero essere ospitati su un server Web.

Il server Web può essere configurato in diversi modi. Per istruzioni su come configurare un semplice server Web utilizzando Python, fare riferimento a. "Webserver con Python".

Fase

1. Salvare l'URL di base del server Web. Se gli URL del firmware del disco, del firmware dello shelf e del firmware del processore di servizio sono **/http://<web-server>/path/all_shelf_fw.zip**, * http://<web-server>/path/all.zip* e **/http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, salvare * http://<web-server>/path/* come URL di base.

Il nome del file viene rilevato automaticamente da Ansible Playbook.

Lavorare con il file di inventario

Il file di inventario è costituito dalle LIF di gestione del cluster dei sistemi idonei per gli aggiornamenti del firmware. Contiene l'elenco dei cluster con informazioni sul nome del file del firmware del disco e dello shelf, laddove applicabile.

Per l'aggiornamento del firmware del Service Processor, i nomi host dei nodi e l'IP SP/BMC sono inclusi nel file di inventario.

Formato del file di inventario

Di seguito viene riportato un esempio di formato di file di inventario con aggiornamenti del firmware di dischi e shelf:

```
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>
```

Nell'esempio, gli aggiornamenti del firmware per shelf e disco sono applicabili al cluster-1 e gli aggiornamenti del firmware per disco e SP/BMC sono applicabili al cluster-2.

Eliminare un cluster dal file di inventario

Se non si desidera applicare gli aggiornamenti del firmware su un cluster specifico, è possibile rimuovere il cluster dal file di inventario.

Ad esempio, se non si desidera applicare gli aggiornamenti del firmware del disco sul cluster-2, è possibile rimuoverlo dal file di inventario utilizzando il seguente comando:

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

È possibile osservare che tutti i dati del cluster 2 sono stati cancellati.

Se si desidera applicare solo gli aggiornamenti del firmware del disco sul cluster-1 e non gli aggiornamenti del firmware dello shelf, utilizzare il seguente comando:

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

È possibile notare che la chiave e il valore di *shelf_fw_file* sono stati rimossi dal cluster-1.

L'aggiunta manuale di cluster o controller non è supportata.

Esegui Ansible Playbook utilizzando l'immagine di NetApp Docker

Prima di eseguire il manuale Ansible, assicurarsi che il file **NetApp_Ansible_*.zip** sia stato estratto e che il server Web con i file del firmware del disco o dello shelf sia pronto.

Prima di iniziare

Prima di eseguire Ansible Playbook con NetApp docker, devi:

- "Scarica il pacchetto di automazione Ansible del firmware AFF e FAS"
- "Ospitare i file del firmware utilizzando il server Web"
- "Lavorare con il file di inventario"
- Assicurarsi che NetApp Docker sia installato.

Fasi

1. "Configurare Docker".
2. Estrarre l'immagine di NetApp Docker da DockerHub eseguendo il seguente comando:

   ```
   $ docker pull schmots1/netapp-ansible

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

   Per ulteriori informazioni sul comando di pull di docker, fare riferimento a. "Documentazione Docker Pull".

3. Eseguire l'immagine Docker come container e accedere al container per eseguire il manuale Ansible.
4. Copiare il percorso della cartella che contiene il Playbook Ansible estratto e i file di inventario, ad esempio **downloaded_playbook_path**. Il Playbook Ansible e i file di inventario devono trovarsi nella stessa cartella per una corretta esecuzione.
5. Montare la cartella come volume sul contenitore Docker. Ad esempio, per montare la cartella **container_path**, eseguire il seguente comando:

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

Il container si avvia e la console si trova nella shell bash del container. Per ulteriori informazioni sul comando Docker Run, fare riferimento a. "Documentazione di Docker Run".

6. Esegui il manuale Ansible all'interno del container usando il 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]
*****************************************************************
```

> Se sono presenti cluster con credenziali di accesso diverse, è necessario eseguire Ansible Playbook su ciascun cluster. Non sono necessarie modifiche al file di inventario, in quanto Ansible Playbook salta i cluster per i quali l'accesso non è riuscito.

Per ulteriori informazioni sul comando **ansible-playbook**, fare riferimento a. "Documentazione di Ansible Playbook" E per eseguire il playbook Ansible in modalità check (dry run), fare riferimento a. "Ansible: Modalità di controllo".

Dopo aver eseguito il manuale Ansible Playbook, fare riferimento a. "Convalide per l'installazione del firmware" per istruzioni post-esecuzione.

Esegui Ansible Playbook senza immagine di NetApp Docker

Fasi

1. Installare "Python" e. "Ansible".
2. Installare i pacchetti Python richiesti usando **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. Installare NetApp Ansible collection utilizzando il comando **ansible-galaxy**:

```
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
```

Per ulteriori informazioni sul comando ansible-galaxy, fare riferimento a. "Documentazione Ansible Galaxy" Per ulteriori informazioni su NetApp Ansible Collection, consultare "Pagina NetApp Ansible Collection".

4. Eseguire il manuale Ansible Playbook utilizzando il 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]
*****************************************************************
```

> Se sono presenti cluster con credenziali di accesso diverse, è necessario eseguire Ansible Playbook su ciascun cluster. Non sono necessarie modifiche al file di inventario, in quanto Ansible Playbook salta i cluster per i quali l'accesso non è riuscito.

Per ulteriori informazioni sul comando **ansible-playbook**, fare riferimento a. "Documentazione di Ansible Playbook" E per eseguire il manuale Ansible in modalità check (dry run), fare riferimento a. "Ansible: Modalità di controllo".

Dopo aver eseguito il manuale, fare riferimento a. "Convalide per l'installazione del firmware" per istruzioni post-esecuzione.

Convalidare l'installazione del firmware

Dopo l'esecuzione del manuale, accedere al cluster come amministratore del cluster.

Convalidare l'installazione del firmware del disco

Fasi

1. Verificare che il firmware del disco sia installato:

```
::*> 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
```

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[storage disk show^].

2. Verificare che il nuovo firmware NVMe Flash cache sia installato:

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

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[system controller flash-cache show^].

Convalidare l'installazione del firmware dello shelf

Fasi

1. Verificare che il nuovo firmware dello shelf sia aggiornato:

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

Nell'output, verificare che il firmware di ogni shelf sia aggiornato al livello desiderato. Ad esempio:

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

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[system node run^].

2. Verificare che il nuovo firmware ACP sia aggiornato:

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

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[show del modulo acp dello shelf di storage^].

3. Verificare che la modalità ACP desiderata sia configurata:

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

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[storage shelf acp show^].

4. Modificare la modalità ACP (canale):

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

Per ulteriori informazioni sul comando, fare riferimento a {link-with-underscore}[storage shelf acp configure^].

Convalida dell'installazione del firmware SP/BMC

Il manuale Ansible Playbook per gli aggiornamenti del firmware di Service Processor/BMC è abilitato con un'opzione per verificare l'installazione del firmware SP/BMC più recente sul controller. Una volta completata la verifica (gli aggiornamenti potrebbero richiedere un tempo massimo di due ore), Ansible Playbook applica gli aggiornamenti del firmware dello switch interno effettuando la connessione alla console SP/BMC.

Le informazioni relative al guasto e al successo delle installazioni del firmware SP/BMC e del firmware dello switch interno verranno notificate al termine dell'esecuzione di Ansible Playbook. Seguire la procedura indicata nel manuale Ansible Playbook nel caso in cui l'installazione del firmware SP/BMC/firmware switch interno non riesca.

Ulteriori informazioni

Puoi ottenere aiuto e trovare ulteriori informazioni attraverso varie risorse.

- "Informazioni per la risoluzione dei problemi"
- "Slack Workspace"
- Mailto:ng-active-iq-feedback@netapp.com[e-mail]
- Pulsante Support in Digital Advisor per supporto e feedback.