



Mettez à niveau pour optimiser votre base installée

Digital Advisor

NetApp
February 19, 2026

Sommaire

- Mettez à niveau pour optimiser votre base installée 1
 - Améliorez votre offre de support dans Digital Advisor 1
 - Mise à jour du firmware AFF et FAS à l'aide d'un playbook Ansible 2
 - Téléchargez le package Ansible du firmware AFF et FAS depuis Digital Advisor..... 2
 - Mise à jour du firmware AFF et FAS à l'aide d'un package Ansible (utilisateurs expérimentés) 2
 - Installation et exécution du firmware AFF et FAS, package d'automatisation Ansible (débutants) 5

Mettez à niveau pour optimiser votre base installée

Améliorez votre offre de support dans Digital Advisor

Vous pouvez acheter une mise à niveau vers l'offre d'assistance pour accéder à d'autres fonctionnalités dans Digital Advisor.

Vous pouvez mettre à niveau votre offre de support afin d'optimiser votre base installée à l'aide des pratiques et des correctifs recommandés, de l'automatisation des mises à niveau avec des playbooks Ansible, des rapports et des évaluations d'activité, du support personnalisé, etc. Vous pouvez acheter la mise à niveau lors du renouvellement de vos contrats de support ou à tout autre moment à partir du tableau de bord système (nœud).



Vous pouvez choisir la mise à niveau vers AIQ uniquement si vous utilisez actuellement les offres de support SupportEdge Premium ou SupportEdge Secure.

Étapes

1. Cliquez sur **Afficher tous les systèmes** en regard du widget **Inventory**.
2. Dans le tableau de bord d'inventaire, sélectionnez le nœud (hôte) à mettre à niveau. Vous êtes redirigé vers le tableau de bord système ou nœud.
3. Cliquez sur **Upgrade** dans le widget **Configuration**.

Configuration

ClusterViewer

Overview

Customer Details

Cluster Name:
HighStor

Current Support Offering:
STANDARD [↑ Upgrade](#)

Hostname:
HighStor-01

Serial Number:
721549000065

Model:
FAS8040

OS Version:
9.3P5

4. Si vous le souhaitez, cliquez sur **Comparer les offres de support** pour consulter le tableau de comparaison et sélectionner l'offre de support qui répond à vos besoins. Vous pouvez également cliquer sur **support Offuoffres** dans le menu de navigation de gauche pour afficher le tableau de comparaison.
5. Sélectionnez le type de mise à niveau souhaité.
 - a. Ajoutez AIQ Upgrade à vos offres de support SupportEdge Premium ou SupportEdge Secure
 - b. Toute autre demande de mise à niveau
6. Ajoutez les commentaires que vous avez et cliquez sur **Envoyer**. Une demande d'achat de la mise à

niveau de l'offre de support est envoyée à l'équipe NetApp Renewals.

Mise à jour du firmware AFF et FAS à l'aide d'un playbook Ansible

Téléchargez le package Ansible du firmware AFF et FAS depuis Digital Advisor.

Pour limiter les risques identifiés et maintenir à jour votre système de stockage, nous vous recommandons de mettre à jour le firmware AFF et FAS à l'aide d'Ansible.

Avant de commencer

Avant de mettre à jour le firmware AFF et FAS à l'aide d'Ansible, vous devez :

- ["Installez et configurez Ansible sur votre système de stockage"](#)
- ["Installez Ansible 2.9 avec les collections de votre système de stockage"](#)
- Mettez à niveau votre système de stockage vers ONTAP 9.1 ou une version ultérieure
- Configurez votre compte avec un rôle d'administrateur

Étapes

1. Cliquez sur n'importe quel widget d'intégrité du tableau de bord ou cliquez sur **Afficher toutes les actions** pour afficher la liste de toutes les actions et de tous les risques.
2. Cliquez sur **Firmware Upgrade** pour afficher tous les risques de mise à niveau du micrologiciel.
3. Cliquez sur **mettre à jour le micrologiciel AFF et FAS** pour afficher tous les progiciels de mise à jour disponibles ou cliquez sur  à côté de chaque risque pour mettre à jour le package spécifique à ce risque.
4. Cliquez sur **Télécharger** pour télécharger les fichiers zip et mettre à jour votre système de stockage.

Le fichier zip contient les éléments suivants :

- Ansible PlayBook : fichier YAML contenant le script Ansible afin de procéder aux mises à jour du firmware du disque, du tiroir et du processeur de service.
- Inventaire - fichier YAML contenant les détails des systèmes applicables aux mises à jour du micrologiciel.
- Les packages de microprogramme de disques, de tiroirs et de processeur de service/BMC sont nommés respectivement **All.zip**, **All_shelf_fw.zip** et **<SP/BMC>_<numéro_version>_fw.zip**.



L'ajout manuel de clusters et de contrôleurs au fichier d'inventaire n'est pas pris en charge.

Mise à jour du firmware AFF et FAS à l'aide d'un package Ansible (utilisateurs expérimentés)

Les utilisateurs expérimentés peuvent installer et exécuter rapidement le package d'automatisation ansible du micrologiciel AFF et FAS.

Mise à jour du firmware avec Ansible à l'aide de NetApp Docker image

Étapes

1. Extrayez l'image Ansible Docker sur l'hôte Linux :

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

2. Exécutez l'image docker en tant que conteneur sur l'hôte Linux :

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



Le PlayBook Ansible et le fichier d'inventaire doivent avoir le même chemin.

3. Exécutez le PlayBook Ansible sur l'hôte Linux. Les mises à jour du micrologiciel s'exécutent en arrière-plan pendant quelques heures.

```
$ 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 les URL du firmware du disque, du firmware des tiroirs et du firmware du processeur de service sont **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** et **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, indiquez **http://<web-server>/path/** comme source d'entrée pour l'URL de base du pack du firmware. Si un ensemble de clusters avec différents identifiants de connexion est défini, le PlayBook Ansible doit être exécuté sur chaque cluster. Aucune modification n'est nécessaire au fichier d'inventaire car Ansible PlayBook ignore les clusters pour lesquels la connexion a échoué.

4. Connectez-vous au cluster en tant qu'administrateur du cluster et vérifiez que le nouveau firmware du disque a été installé :

```

::> 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

```

Mise à jour du firmware si Ansible est déjà utilisé

Étapes

1. Installez Python et Ansible, puis téléchargez les packages Python à l'aide du 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. Installez 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. Vérifiez que le PlayBook Ansible et le fichier d'inventaire se trouvent dans le même chemin, puis exécutez le PlayBook Ansible. Les mises à jour du micrologiciel s'exécutent en arrière-plan pendant quelques heures.

```
$ 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 les URL du firmware du disque, du firmware des tiroirs et du firmware du processeur de service sont **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** et **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, indiquez **http://<web-server>/path/** comme source d'entrée pour l'URL de base du pack du firmware. Si un ensemble de clusters avec différents identifiants de connexion est défini, le PlayBook Ansible doit être exécuté sur chaque cluster. Aucune modification n'est nécessaire au fichier d'inventaire car Ansible PlayBook ignore les clusters pour lesquels la connexion a échoué.

4. Connectez-vous au cluster en tant qu'administrateur du cluster et vérifiez que le nouveau firmware du disque a été installé :

```
::> 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
```

Installation et exécution du firmware AFF et FAS, package d'automatisation Ansible (débutants)

Hébergez les fichiers de firmware AFF et FAS sur un serveur web

Une fois le progiciel d'automatisation téléchargé, les fichiers du micrologiciel doivent être hébergés sur un serveur Web.

Le serveur Web peut être configuré de plusieurs façons. Pour obtenir des instructions sur la configuration d'un serveur Web simple à l'aide de Python, reportez-vous à la section ["Serveur web utilisant Python"](#).

Étape

1. Enregistrez l'URL de base du serveur Web. Si les URL du firmware du disque, du firmware des tiroirs et du firmware du processeur de service sont **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** et **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, enregistrez

http://<web-server>/path/ comme URL de base.

Le nom de fichier est automatiquement détecté par le PlayBook Ansible.

Mettez à jour le fichier d'inventaire pour la mise à jour du firmware AFF et FAS

Le fichier d'inventaire se compose des LIFs de gestion du cluster des systèmes éligibles pour les mises à jour de firmware. Elle contient la liste des clusters avec des informations sur le nom de fichier du firmware des disques et des tiroirs, si nécessaire.

Pour la mise à jour du micrologiciel du processeur de service, les noms d'hôte de nœud et l'adresse IP SP/BMC sont inclus dans le fichier d'inventaire.

Format du fichier d'inventaire

Voici un exemple de format de fichier d'inventaire avec des mises à jour du firmware des disques et des tiroirs :

```
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>
```

Dans cet exemple, les mises à jour du firmware des tiroirs et des disques s'appliquent aux mises à jour du firmware des clusters 1 et des disques, et SP/BMC, applicables au cluster-2.

Supprimer un cluster du fichier d'inventaire

Si vous ne souhaitez pas appliquer de mises à jour de micrologiciel sur un cluster particulier, vous pouvez supprimer le cluster du fichier d'inventaire.

Par exemple, si vous ne souhaitez pas appliquer de mise à jour du firmware des disques sur cluster-2, vous pouvez le supprimer du fichier d'inventaire à l'aide de la commande suivante :

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

Vous pouvez observer que toutes les données du cluster-2 ont été supprimées.

Si vous souhaitez appliquer uniquement les mises à jour du firmware des disques sur le cluster-1 et non les mises à jour du firmware des tiroirs, vous pouvez utiliser la commande suivante :

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

Vous pouvez constater que la clé et la valeur *shelf_fw_file* ont été supprimées du cluster-1.



L'ajout manuel de clusters ou de contrôleurs n'est pas pris en charge.

Exécutez le playbook Ansible à l'aide de l'image Docker NetApp.

Avant d'exécuter le PlayBook Ansible, vérifiez que le fichier **NetApp_Ansible_*.zip** a été extrait et que le serveur Web avec les fichiers de firmware des tiroirs ou des disques est prêt.

Avant de commencer

Avant d'exécuter le manuel de vente Ansible à l'aide de NetApp docker, vous devez :

- ["Téléchargez le pack Ansible Automation du firmware AFF et FAS"](#)
- ["Héberger les fichiers du micrologiciel à l'aide du serveur Web"](#)
- ["Travailler avec le fichier d'inventaire"](#)
- S'assurer que NetApp Docker est installé.

Étapes

1. ["Configuration de Docker"](#).
2. Extrayez l'image NetApp Docker depuis DockerHub en exécutant la commande suivante :

```
$ docker pull schmots1/netapp-ansible

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

Pour plus d'informations sur la commande docker pull, reportez-vous au ["Documentation Docker Pull"](#).

3. Exécutez l'image Docker en tant que conteneur et connectez-vous à ce conteneur pour exécuter le PlayBook Ansible.
4. Copiez le chemin d'accès du dossier qui contient le PlayBook Ansible extrait et les fichiers d'inventaire, par exemple **téléchargé_PlayBook_path**. Pour que l'exécution soit réussie, les fichiers PlayBook et d'inventaire doivent se trouver dans le même dossier.
5. Montez le dossier en tant que volume sur le conteneur Docker. Par exemple, pour monter le dossier **conteneur_path**, vous devez exécuter la commande suivante :

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

Le conteneur démarre et la console est maintenant à bash shell du conteneur. Pour plus d'informations sur la commande Docker Run, reportez-vous au ["Documentation Docker Run"](#).

6. Exécutez le PlayBook Ansible dans le conteneur à l'aide de la commande **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 un ensemble de clusters avec différents identifiants de connexion est défini, le PlayBook Ansible doit être exécuté sur chaque cluster. Aucune modification n'est nécessaire au fichier d'inventaire car Ansible PlayBook ignore les clusters pour lesquels la connexion a échoué.

Pour plus d'informations sur la commande **ansible-PlayBook**, reportez-vous au ["Documentation relative au manuel de vente Ansible"](#) Et pour exécuter le PlayBook Ansible en mode vérification (exécution à sec), reportez-vous à la ["Ansible : mode de vérification"](#).

Après avoir exécuté le manuel de vente Ansible, consultez le ["Validations de l'installation du micrologiciel"](#) pour les instructions post-exécution.

Exécutez le playbook Ansible sans l'image Docker NetApp.

Étapes

1. Installer ["Python"](#) et ["Ansible"](#).
2. Installez les modules Python requis à l'aide de **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. Installer la collection NetApp Ansible à l'aide de la commande **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
```

Pour plus d'informations sur la commande **ansible-Galaxy**, voir ["Documentation Ansible Galaxy"](#) Pour plus d'informations sur la collection NetApp Ansible, consultez le ["Page de collecte NetApp Ansible"](#).

4. Exécutez le PlayBook Ansible à l'aide de la commande **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 un ensemble de clusters avec différents identifiants de connexion est défini, le PlayBook Ansible doit être exécuté sur chaque cluster. Aucune modification n'est nécessaire au fichier d'inventaire car Ansible PlayBook ignore les clusters pour lesquels la connexion a échoué.

Pour plus d'informations sur la commande **ansible-PlayBook**, reportez-vous au ["Documentation relative au manuel de vente Ansible"](#) Et pour exécuter le Ansible PlayBook en mode vérification (exécution à sec), reportez-vous à la ["Ansible : mode de vérification"](#).

Après avoir exécuté le manuel de vente, reportez-vous au ["Validations de l'installation du micrologiciel"](#) pour les instructions post-exécution.

Validez l'installation du firmware AFF et FAS sur votre système de stockage.

Après l'exécution du PlayBook, connectez-vous au cluster en tant qu'administrateur du cluster.

Validation de l'installation du firmware du disque

Étapes

1. Vérifiez que le micrologiciel du lecteur est installé :

```
::*> 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
```

Pour plus d'informations sur la commande, reportez-vous à [{link-with-soulignements}\[Storage disk show^\]](#).

2. Vérifiez que le nouveau firmware NVMe Flash cache est installé :

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

Pour plus d'informations sur la commande, reportez-vous à [{link-with-souligns}\[system Controller flash-cache show^\]](#).

Validez l'installation du firmware du tiroir

Étapes

1. Vérifiez que le nouveau firmware du tiroir est mis à jour :

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

Dans le résultat de la commande, vérifiez que le firmware de chaque tiroir est mis à jour au niveau souhaité. Par exemple :

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

Pour plus d'informations sur la commande, reportez-vous à la section [{link-with-soulignements}\[system node run^\]](#).

2. Vérifier que le nouveau firmware ACP est mis à jour :

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

Pour plus d'informations sur la commande, reportez-vous à [Storage shelf ACP module show^](#)].

3. Vérifiez que le mode ACP souhaité est configuré :

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

Pour plus d'informations sur la commande, reportez-vous à [Storage shelf acp show^](#)].

4. Modifiez le mode ACP (canal) :

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

Pour plus d'informations sur la commande, reportez-vous à [Storage shelf acp configure^](#)].

Validation de l'installation du micrologiciel SP/BMC

Les mises à jour du firmware Ansible PlayBook pour le processeur de service/BMC sont activées avec une option permettant de vérifier l'installation du dernier firmware SP/BMC sur le contrôleur. Une fois la vérification terminée (les mises à jour peuvent prendre une durée maximale de deux heures), Ansible PlayBook applique les mises à jour internes du firmware des commutateurs en se connectant à la console SP/BMC.

Les informations de défaillance et de réussite du micrologiciel SP/BMC et des installations de firmware du commutateur interne seront notifiées à la fin de l'exécution d'Ansible PlayBook. Suivez les étapes indiquées dans le manuel Ansible PlayBook si l'installation du firmware du commutateur interne/du micrologiciel du processeur de service/BMC/du commutateur interne échoue.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.