Support de démarrage

Install and maintain

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-systems/fas2700/bootmedia-replace-overview.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Support de démarrage . . . 1
Présentation du remplacement du support de démarrage - FAS2700 . . . 1
Vérifier la prise en charge et l'état des clés de chiffrement - FAS2700 . . . 1
Étape 1 : Vérifiez la prise en charge NVE et téléchargez l'image ONTAP appropriée. . . . 2
Étape 2 : Vérifier l'état du gestionnaire de clés et la configuration de sauvegarde . . . 2
Arrêtez le contrôleur défectueux - FAS2700 . . . 5
Option 1 : plupart des configurations . . . 6
Option 2 : le contrôleur est dans un MetroCluster . . . 6
Remplacez le support de démarrage - FAS2700 . . . 7
Étape 1 : retirer le module de contrôleur . . . 7
Étape 2 : remplacer le support de démarrage . . . 9
Étape 3 : transférez l'image de démarrage sur le support de démarrage . . . 10
Démarrez l'image de restauration - FAS2700 . . . 12
Restauration du chiffrement - FAS2700 . . . 14
Renvoyez la pièce défectueuse à NetApp - AFF A220 et FAS2700 . . . 24

Support de démarrage

Présentation du remplacement du support de démarrage - FAS2700

Découvrez comment remplacer le support de démarrage sur un système FAS2700 et comprenez les différentes méthodes de remplacement.

Le support de démarrage stocke les fichiers image de démarrage primaire et secondaire utilisés par le système au démarrage. Selon la configuration de votre réseau, vous pouvez effectuer soit un remplacement non perturbateur (paire HA connectée au réseau), soit un remplacement perturbateur (nécessite deux redémarrages).

Le support de démarrage stocke un ensemble principal et secondaire de fichiers système (image de démarrage) que le système utilise lors du démarrage. Selon votre configuration réseau, vous pouvez effectuer un remplacement sans interruption ou sans interruption.

Vous devez disposer d'une clé USB, formatée en FAT32, avec la quantité de stockage appropriée pour maintenir le `image_xxx.tgz` fichier.

Vous devez également copier le `image_xxx.tgz` Fichier sur le lecteur flash USB pour une utilisation ultérieure dans cette procédure.

- Les méthodes pour remplacer un support de démarrage sans interruption et sans interruption nécessitent toutes deux la restauration du `var` système de fichiers :
  - Pour le remplacement sans interruption, la paire haute disponibilité doit être connectée à un réseau afin de restaurer le `var` système de fichiers.
  - Pour un remplacement perturbateur, vous n'avez pas besoin d'une connexion réseau pour restaurer le `var` le système de fichiers, mais le processus nécessite deux redémarrages.
- Vous devez remplacer le composant défectueux par un composant FRU de remplacement que vous avez reçu de votre fournisseur.
- Il est important d'appliquer les commandes au cours de la procédure suivante sur le nœud approprié :
  - Le noeud *trouble* est le noeud sur lequel vous effectuez la maintenance.
  - Le *Healthy node* est le partenaire HA du nœud douteux.

Vérifier la prise en charge et l'état des clés de chiffrement - FAS2700

Vérifiez la prise en charge et l'état de la clé de chiffrement avant d'arrêter le contrôleur défectueux sur un système FAS2700. Cette procédure comprend la vérification de la compatibilité de la version ONTAP avec NetApp Volume Encryption (NVE), la vérification de la configuration du gestionnaire de clés et la sauvegarde des informations de chiffrement pour garantir la sécurité des données lors de la récupération du support de démarrage.

Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de

démarrage. La récupération automatique du support de démarrage n'est pas prise en charge.

Étape 1 : Vérifiez la prise en charge NVE et téléchargez l'image ONTAP appropriée.

Déterminez si votre version ONTAP prend en charge le chiffrement de volume NetApp (NVE) afin de pouvoir télécharger l'image ONTAP appropriée pour le remplacement du support de démarrage.

Étapes

1. Vérifiez si votre version ONTAP prend en charge le chiffrement :

   `version -v`

   Si le résultat de cette commande indique `10no-DARE`, NVE n'est pas pris en charge par la version de votre cluster.

2. Téléchargez l'image ONTAP appropriée en fonction de la prise en charge NVE :
   - Si NVE est pris en charge : Téléchargez l'image ONTAP avec chiffrement de volume NetApp
   - Si NVE n'est pas pris en charge : Téléchargez l'image ONTAP sans chiffrement de volume NetApp

   Téléchargez l'image ONTAP depuis le site de support NetApp vers votre serveur HTTP ou FTP ou vers un dossier local. Vous aurez besoin de ce fichier image lors de la procédure de remplacement du support de démarrage.

Étape 2 : Vérifier l'état du gestionnaire de clés et la configuration de sauvegarde

Avant de mettre hors service le contrôleur défectueux, vérifiez la configuration du gestionnaire de clés et sauvegardez les informations nécessaires.

Étapes

1. Déterminez le gestionnaire de clés activé sur votre système :

Version ONTAP	Exécutez cette commande
ONTAP 9.14.1 ou version ultérieure	`security key-manager keystore show` • Si EKM est activé, `EKM` est répertorié dans la sortie de la commande. • Si OKM est activé, `OKM` est répertorié dans la sortie de la commande. • Si aucun gestionnaire de clés n'est activé, `No key manager keystores configured` est répertorié dans la sortie de la commande.

Version ONTAP	Exécutez cette commande
ONTAP 9.13.1 ou version antérieure	`security key-manager show-key-store` • Si EKM est activé, `external` est répertorié dans la sortie de la commande. • Si OKM est activé, `onboard` est répertorié dans la sortie de la commande. • Si aucun gestionnaire de clés n'est activé, `No key managers configured` est répertorié dans la sortie de la commande.

2. Selon que votre système dispose ou non d'un gestionnaire de clés, effectuez l'une des opérations suivantes :

   Si aucun gestionnaire de clés n'est configuré :

   Vous pouvez éteindre en toute sécurité le contrôleur défectueux et procéder à la procédure d'arrêt.

   Si un gestionnaire de clés est configuré (EKM ou OKM) :

   a. Saisissez la commande de requête suivante pour afficher l'état des clés d'authentification dans votre gestionnaire de clés :

      ```
      security key-manager key query
      ```

   b. Examinez le résultat et vérifiez la valeur dans le `Restored` colonne. Cette colonne indique si les clés d'authentification de votre gestionnaire de clés (EKM ou OKM) ont été restaurées avec succès.

3. Suivez la procédure appropriée en fonction de votre type de responsable clé :

Gestionnaire de clés externe (EKM)

Suivez ces étapes en fonction de la valeur indiquée. `Restored` colonne.

Si toutes les touches s'affichent `true` dans la colonne Restauré :

Vous pouvez éteindre en toute sécurité le contrôleur défectueux et procéder à la procédure d'arrêt.

Si des clés affichent une valeur autre que `true` dans la colonne Restauré :

a. Restaurez les clés d'authentification de gestion des clés externes sur tous les nœuds du cluster :

   ```
   security key-manager external restore
   ```

   Si la commande échoue, contactez le support NetApp .

b. Vérifiez que toutes les clés d'authentification sont restaurées :

   ```
   security key-manager key query
   ```

   Confirmez que le `Restored` affichages en colonne `true` pour toutes les clés d'authentification.

c. Si toutes les clés sont restaurées, vous pouvez éteindre en toute sécurité le contrôleur défectueux et procéder à la procédure d'arrêt.

Gestionnaire de clés intégré Onboard Key Manager (OKM)

Suivez ces étapes en fonction de la valeur indiquée. `Restored` colonne.

Si toutes les touches s'affichent `true` dans la colonne Restauré :

a. Sauvegardez les informations OKM :

   i. Passer en mode privilège avancé :

      ```
      set -priv advanced
      ```

   Entrer `y` lorsqu'on vous invite à continuer.

   i. Afficher les informations de sauvegarde de la gestion des clés :

      ```
      security key-manager onboard show-backup
      ```

   ii. Copiez les informations de sauvegarde dans un fichier séparé ou dans votre fichier journal.

      Vous aurez besoin de ces informations de sauvegarde si vous devez récupérer manuellement OKM lors de la procédure de remplacement.

   iii. Retour au mode administrateur :

      ```
      set -priv admin
      ```

b. Vous pouvez éteindre en toute sécurité le contrôleur défectueux et procéder à la procédure d'arrêt.

Si des clés affichent une valeur autre que `true` dans la colonne Restauré :

a. Synchroniser le gestionnaire de clés intégré :

```
security key-manager onboard sync
```

Saisissez la phrase de passe alphanumérique de 32 caractères pour la gestion des clés intégrées lorsque vous y êtes invité.

> Il s'agit de la phrase secrète globale du cluster que vous avez créée lors de la configuration initiale du gestionnaire de clés intégré. Si vous ne possédez pas cette phrase de passe, contactez l'assistance NetApp .

b. Vérifiez que toutes les clés d'authentification sont restaurées :

```
security key-manager key query
```

Confirmez que le `Restored` affichages en colonne `true` pour toutes les clés d'authentification et le `Key Manager` type affiche `onboard` .

c. Sauvegardez les informations OKM :

i. Passer en mode privilège avancé :

```
set -priv advanced
```

Entrer `y` lorsqu'on vous invite à continuer.

i. Afficher les informations de sauvegarde de la gestion des clés :

```
security key-manager onboard show-backup
```

ii. Copiez les informations de sauvegarde dans un fichier séparé ou dans votre fichier journal.

Vous aurez besoin de ces informations de sauvegarde si vous devez récupérer manuellement OKM lors de la procédure de remplacement.

iii. Retour au mode administrateur :

```
set -priv admin
```

d. Vous pouvez éteindre en toute sécurité le contrôleur défectueux et procéder à la procédure d'arrêt.

Arrêtez le contrôleur défectueux - FAS2700

Arrêtez ou prenez le contrôle du contrôleur défaillant en utilisant la procédure appropriée à votre configuration. Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de démarrage. La récupération automatique du support de démarrage n'est pas prise en charge.

Option 1 : plupart des configurations

Une fois les tâches NVE ou NSE terminées, vous devez arrêter le contrôleur pour cause de dysfonctionnement.

Étapes

1. Faites passer le contrôleur douteux à l'invite DU CHARGEUR :

Si le contrôleur en état de fonctionnement s'affiche…	Alors…
Invite DU CHARGEUR	Passez à la section retrait du module de contrôleur.
`Waiting for giveback…`	Appuyez sur Ctrl-C, puis répondez `y` lorsque vous y êtes invité.
Invite système ou invite de mot de passe (entrer le mot de passe système)	Prendre le contrôle défectueux ou l'arrêter à partir du contrôleur en bon état : `storage failover takeover -ofnode impaired_node_name` Lorsque le contrôleur douteux s'affiche en attente de rétablissement…, appuyez sur Ctrl-C et répondez `y`.

2. Dans l'invite DU CHARGEUR, entrez : `printenv` pour capturer toutes les variables environnementales de démarrage. Enregistrez le résultat dans votre fichier journal.

> Cette commande peut ne pas fonctionner si le périphérique d'amorçage est corrompu ou non fonctionnel.

Option 2 : le contrôleur est dans un MetroCluster

Une fois les tâches NVE ou NSE terminées, vous devez arrêter le contrôleur pour cause de dysfonctionnement.

> N'utilisez pas cette procédure si votre système se trouve dans une configuration MetroCluster à deux nœuds.

Pour arrêter le contrôleur défaillant, vous devez déterminer l'état du contrôleur et, si nécessaire, prendre le contrôle de façon à ce que le contrôleur en bonne santé continue de transmettre des données provenant du stockage défaillant du contrôleur.

- Si vous avez un cluster avec plus de deux nœuds, il doit être dans le quorum. Si le cluster n'est pas au quorum ou si un contrôleur en bonne santé affiche la valeur false pour l'éligibilité et la santé, vous devez corriger le problème avant de désactiver le contrôleur défaillant ; voir "Synchroniser un nœud avec le cluster".
- Si vous disposez d'une configuration MetroCluster, vous devez avoir confirmé que l'état de configuration MetroCluster est configuré et que les nœuds sont dans un état activé et normal (`metrocluster node show`).

Étapes

1. Si AutoSupport est activé, supprimez la création automatique de dossier en invoquant un message AutoSupport : `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   Le message AutoSupport suivant supprime la création automatique de dossiers pendant deux heures : `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Désactiver le rétablissement automatique depuis la console du contrôleur sain : `storage failover modify –node local -auto-giveback false`
3. Faites passer le contrôleur douteux à l'invite DU CHARGEUR :

Si le contrôleur en état de fonctionnement s'affiche…	**Alors…**
Invite DU CHARGEUR	Passez à l'étape suivante.
Attente du retour…	Appuyez sur Ctrl-C, puis répondez `y` lorsque vous y êtes invité.
Invite système ou invite de mot de passe (entrer le mot de passe système)	Prendre le contrôle défectueux ou l'arrêter à partir du contrôleur en bon état : `storage failover takeover -ofnode` *`impaired_node_name`* Lorsque le contrôleur douteux s'affiche en attente de rétablissement…, appuyez sur Ctrl-C et répondez `y`.

Remplacez le support de démarrage - FAS2700

Remplacez le support de démarrage défectueux sur un module contrôleur FAS2700. Cette procédure comprend le retrait du module contrôleur du châssis, le remplacement physique du composant de support de démarrage, le transfert de l'image de démarrage sur le support de remplacement à l'aide d'une clé USB et la restauration du système à son fonctionnement normal.

Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de démarrage. La récupération automatique du support de démarrage n'est pas prise en charge.

Pour remplacer le support de démarrage, vous devez retirer le module de contrôleur endommagé, installer le support de démarrage de remplacement et transférer l'image de démarrage sur une clé USB.

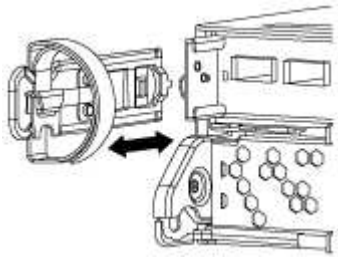
Étape 1 : retirer le module de contrôleur

Pour accéder aux composants à l'intérieur du contrôleur, vous devez d'abord retirer le module de contrôleur du système, puis retirer le capot du module de contrôleur.

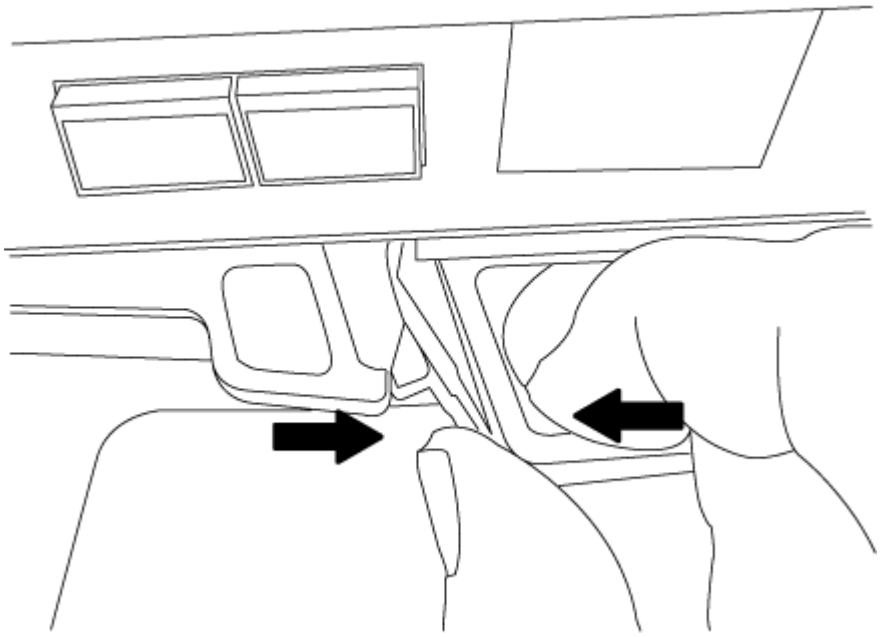
1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Desserrez le crochet et la bride de boucle qui relient les câbles au périphérique de gestion des câbles, puis débranchez les câbles système et les SFP (si nécessaire) du module de contrôleur, en maintenant une trace de l'emplacement où les câbles ont été connectés.

Laissez les câbles dans le périphérique de gestion des câbles de sorte que lorsque vous réinstallez le périphérique de gestion des câbles, les câbles sont organisés.

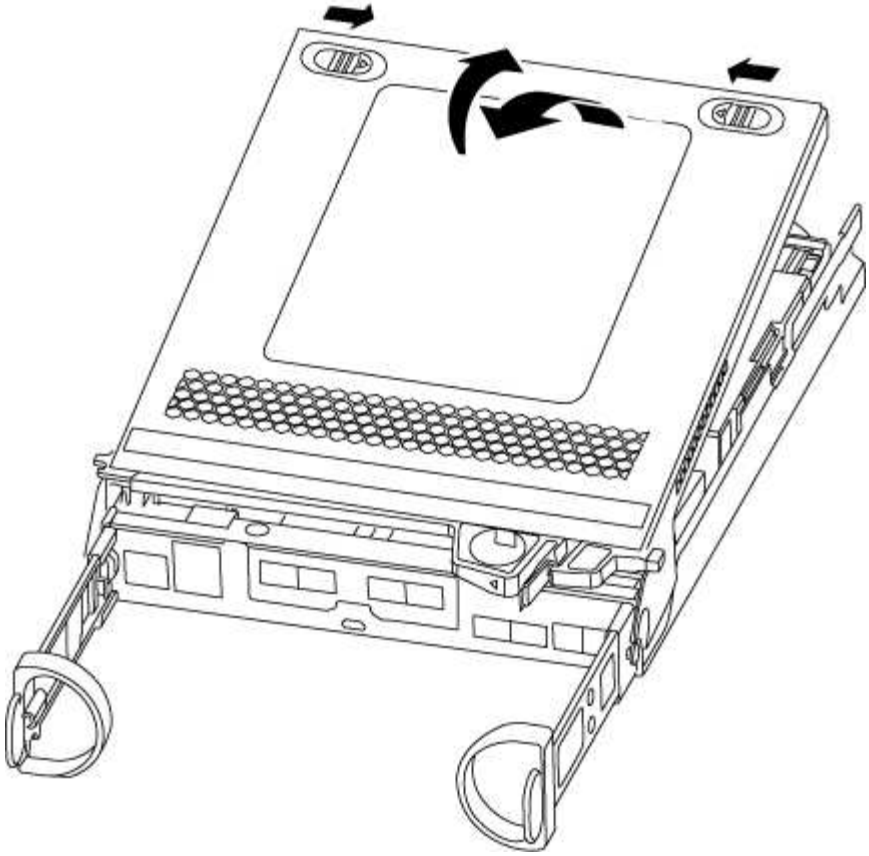
3. Retirez et mettez de côté les dispositifs de gestion des câbles des côtés gauche et droit du module de contrôleur.



4. Appuyez sur le loquet de la poignée de came jusqu'à ce qu'il se libère, ouvrez complètement la poignée de came pour libérer le module de contrôleur du fond de panier central, puis, à l'aide de deux mains, retirez le module de contrôleur du châssis.



5. Retournez le module de contrôleur et placez-le sur une surface plane et stable.
6. Ouvrez le capot en le faisant glisser dans les languettes bleues pour le dégager, puis faites pivoter le couvercle vers le haut et ouvrez-le.

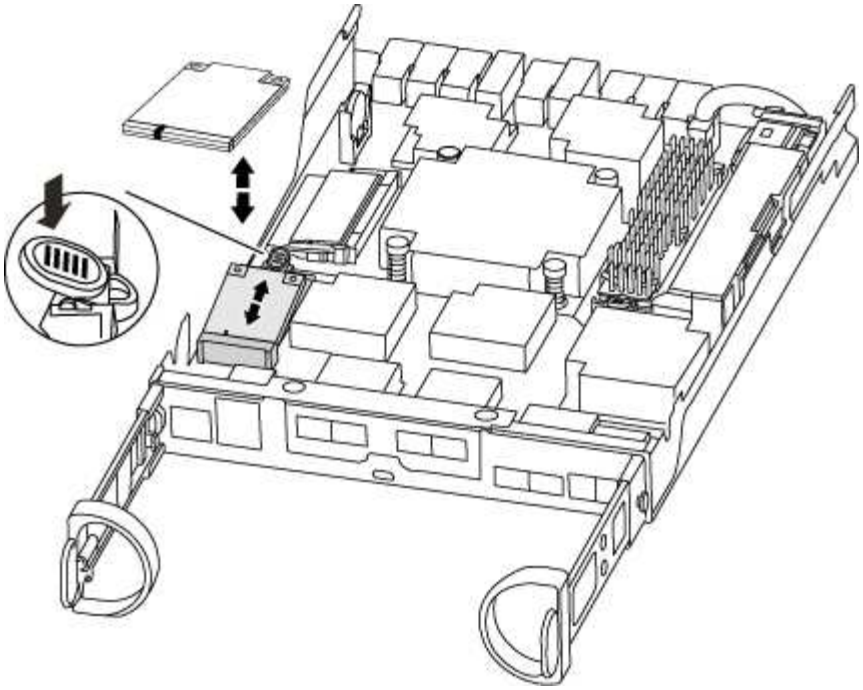


Étape 2 : remplacer le support de démarrage

Vous devez localiser le support de démarrage dans le contrôleur et suivre les instructions pour le remplacer.

Étapes

1. Si vous n’êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Recherchez le support de démarrage à l’aide de l’illustration suivante ou du mappage des FRU sur le module de contrôleur :



3. Appuyez sur le bouton bleu du logement du support de démarrage pour libérer le support de démarrage de son logement, puis tirez-le doucement hors du support de démarrage.

> Ne faites pas tourner ou tirer le support de démarrage directement vers le haut, car cela pourrait endommager le support ou le support de démarrage.

4. Alignez les bords du support de démarrage de remplacement avec le support de démarrage, puis poussez-le doucement dans le support.
5. Vérifiez le support de démarrage pour vous assurer qu'il est bien en place dans le support.

   Si nécessaire, retirez le support de démarrage et réinstallez-le dans le support.

6. Poussez le support de démarrage vers le bas pour engager le bouton de verrouillage sur le boîtier du support de démarrage.
7. Fermez le capot du module de contrôleur.

Étape 3 : transférez l'image de démarrage sur le support de démarrage

Vous pouvez installer l'image système sur le support de démarrage de remplacement à l'aide d'un lecteur flash USB avec l'image installée sur celui-ci. Cependant, vous devez restaurer le système de fichiers var au cours de cette procédure.

- Vous devez disposer d'une clé USB, formatée en FAT32, avec au moins 4 Go de capacité.
- Copie de la même version d'image de ONTAP que celle du contrôleur avec facultés affaiblies. Vous pouvez télécharger l'image appropriée depuis la section Downloads du site de support NetApp
  - Si NVE est activé, téléchargez l'image avec NetApp Volume Encryption, comme indiqué sur le bouton de téléchargement.
  - Si NVE n'est pas activé, téléchargez l'image sans NetApp Volume Encryption, comme indiqué sur le bouton de téléchargement.
- Si votre système est une paire haute disponibilité, vous devez disposer d'une connexion réseau.

- Si votre système est un système autonome, vous n'avez pas besoin d'une connexion réseau, mais vous devez effectuer un redémarrage supplémentaire lors de la restauration du système de fichiers var.

Étapes

1. Alignez l'extrémité du module de contrôleur avec l'ouverture du châssis, puis poussez doucement le module de contrôleur à mi-course dans le système.
2. Réinstallez le périphérique de gestion des câbles et recâblage du système, selon les besoins.

   Lors de la remise en état, n'oubliez pas de réinstaller les convertisseurs de support (SFP) s'ils ont été retirés.

3. Insérez la clé USB dans le logement USB du module de contrôleur.

   Assurez-vous d'installer le lecteur flash USB dans le logement étiqueté pour périphériques USB et non dans le port de console USB.

4. Poussez le module de contrôleur complètement dans le système, en vous assurant que la poignée de came se dégage du lecteur flash USB, appuyez fermement sur la poignée de came pour terminer l'installation du module de contrôleur, poussez la poignée de came en position fermée, puis serrez la vis moletée.

   Le contrôleur commence à démarrer dès qu'il est entièrement installé dans le châssis.

5. Interrompez le processus de démarrage pour qu'il s'arrête à l'invite DU CHARGEUR en appuyant sur Ctrl-C lorsque vous voyez démarrer L'AUTOBOOT, appuyez sur Ctrl-C pour annuler

   Si ce message ne s'affiche pas, appuyez sur Ctrl-C, sélectionnez l'option pour démarrer en mode maintenance, puis arrêtez le contrôleur pour démarrer LE CHARGEUR.

6. Pour les systèmes équipés d'un contrôleur dans le châssis, reconnectez les blocs d'alimentation et mettez les blocs d'alimentation sous tension.

   Le système commence à démarrer et s'arrête à l'invite DU CHARGEUR.

7. Définissez le type de connexion réseau à l'invite DU CHARGEUR :

   - Si vous configurez DHCP : `ifconfig e0a -auto`

     > Le port cible que vous configurez est le port cible que vous utilisez pour communiquer avec le contrôleur douteux à partir du contrôleur en bon état pendant la restauration du système de fichiers var avec une connexion réseau. Vous pouvez également utiliser le port e0M dans cette commande.

   - Si vous configurez des connexions manuelles : `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - Filer_addr est l'adresse IP du système de stockage.
     - Le masque de réseau est le masque de réseau du réseau de gestion connecté au partenaire haute disponibilité.
     - passerelle est la passerelle du réseau.
     - dns_addr est l'adresse IP d'un serveur de noms sur votre réseau.
     - dns_Domain est le nom de domaine DNS (Domain Name System).

Si vous utilisez ce paramètre facultatif, vous n'avez pas besoin d'un nom de domaine complet dans l'URL du serveur netboot. Vous avez uniquement besoin du nom d'hôte du serveur.

D'autres paramètres peuvent être nécessaires pour votre interface. Vous pouvez entrer `help ifconfig` à l'invite du micrologiciel pour plus de détails.

Démarrez l'image de restauration - FAS2700

Démarrez l'image de récupération ONTAP à partir de la clé USB sur un système FAS2700 pour restaurer le support de démarrage. Cette procédure comprend le démarrage à partir de la clé USB, la restauration du système de fichiers, la vérification des variables d'environnement et le retour du contrôleur à un fonctionnement normal après le remplacement du support de démarrage.

Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de démarrage. La récupération automatique du support de démarrage n'est pas prise en charge.

Vous devez démarrer l'image ONTAP à partir du lecteur USB, restaurer le système de fichiers et vérifier les variables environnementales.

Étapes

1. À partir de l'invite DU CHARGEUR, démarrez l'image de récupération à partir du lecteur flash USB : `boot_recovery`

   L'image est téléchargée à partir de la clé USB.

2. Lorsque vous y êtes invité, entrez le nom de l'image ou acceptez l'image par défaut affichée entre crochets sur votre écran.
3. Restaurez le système de fichiers var :

Si votre système dispose de…	Alors…
Une connexion réseau	a. Appuyez sur `y` lorsque vous êtes invité à restaurer la configuration de sauvegarde. b. Définissez le contrôleur sain sur le niveau de privilège avancé : `set -privilege advanced` c. Exécutez la commande restore backup : `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Renvoyer le contrôleur au niveau admin : `set -privilege admin` e. Appuyez sur `y` lorsque vous êtes invité à utiliser la configuration restaurée. f. Appuyez sur `y` lorsque vous êtes invité à redémarrer le contrôleur.

Si votre système dispose de…	Alors…
Aucune connexion réseau	a. Appuyez sur `n` lorsque vous êtes invité à restaurer la configuration de sauvegarde. b. Redémarrez le système à l'invite du système. c. Sélectionnez l'option **mettre à jour Flash dans Backup config** (Sync flash) dans le menu affiché. Si vous êtes invité à poursuivre la mise à jour, appuyez sur `y`.

4. Assurez-vous que les variables environnementales sont définies comme prévu :
   a. Prenez le contrôleur vers l'invite DU CHARGEUR.
   b. Vérifiez les paramètres de la variable d'environnement à l'aide de l' `printenv` commande.
   c. Si une variable d'environnement n'est pas définie comme prévu, modifiez-la avec le `setenv` *`environment-variable-name changed-value`* commande.
   d. Enregistrez vos modifications à l'aide du `savenv` commande.
5. Le suivant dépend de la configuration de votre système :
   - Si keymanager, NSE ou NVE intégré est configuré sur votre système, rendez-vous sur OKM, NSE et NVE si besoin
   - Si keymanager, NSE ou NVE intégré ne sont pas configurés sur votre système, effectuez les étapes de cette section.
6. Dans l'invite DU CHARGEUR, entrez le `boot_ontap` commande.

Si vous voyez…	Alors…
Invite de connexion	Passer à l'étape suivante.
Attente du retour…	a. Connectez-vous au contrôleur partenaire. b. Vérifiez que le contrôleur cible est prêt pour le rétablissement à l'aide du `storage failover show` commande.

7. Branchez le câble de la console au contrôleur partenaire.
8. Reaccordez le contrôleur à l'aide du `storage failover giveback -fromnode local` commande.
9. À l'invite du cluster, vérifiez les interfaces logiques avec le `net int -is-home false` commande.

   Si l'une des interfaces est indiquée comme « FALSE », restaurez ces interfaces à son port d'origine à l'aide de l' `net int revert` commande.
10. Déplacez le câble de la console vers le contrôleur réparé et exécutez le `version -v` Commande pour vérifier les versions de ONTAP.
11. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

Restauration du chiffrement - FAS2700

Restaurez le chiffrement sur le support de démarrage de remplacement. Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de démarrage. La récupération automatique du support de démarrage n’est pas prise en charge.

Suivez les étapes appropriées pour restaurer le chiffrement sur votre système en fonction de votre type de gestionnaire de clés. Si vous ne savez pas quel gestionnaire de clés votre système utilise, vérifiez les paramètres que vous avez enregistrés au début de la procédure de remplacement du support de démarrage.

Gestionnaire de clés intégré Onboard Key Manager (OKM)

Restaurez la configuration du gestionnaire de clés intégré (OKM) à partir du menu de démarrage ONTAP.

Avant de commencer

Assurez-vous d'avoir les informations suivantes à disposition :

- phrase secrète à l'échelle du cluster saisie pendant "activer la gestion des clés embarquées"
- "Informations de sauvegarde pour le gestionnaire de clés intégré"
- Vérification que vous disposez de la phrase secrète correcte et des données de sauvegarde à l'aide de "Comment vérifier la sauvegarde de gestion intégrée des clés et la phrase secrète au niveau du cluster" procédure

Étapes

Sur la manette défectueuse :

1. Connectez le câble de la console à la manette défectueuse.
2. Dans le menu de démarrage ONTAP , sélectionnez l'option appropriée :

Version ONTAP	Sélectionnez cette option

ONTAP 9.8 ou version ultérieure	Sélectionnez l'option 10.
	
	Affiche un exemple de menu de démarrage
	
	`Please choose one of the following:`
	
	`(1) Normal Boot.`
	`(2) Boot without /etc/rc.`
	`(3) Change password.`
	`(4) Clean configuration and initialize all disks.`
	`(5) Maintenance mode boot.`
	`(6) Update flash from backup config.`
	`(7) Install new software first.`
	`(8) Reboot node.`
	`(9) Configure Advanced Drive Partitioning.`
	`(10) Set Onboard Key Manager recovery secrets.`
	`(11) Configure node for external key management.`
	`Selection (1-11)? 10`

Version ONTAP	Sélectionnez cette option

ONTAP 9.7 et versions antérieures	Sélectionnez l'option cachée `recover_onboard_keymanager`
	
	Affiche un exemple de menu de démarrage
	
	`Please choose one of the following:`
	
	`(1) Normal Boot.`
	`(2) Boot without /etc/rc.`
	`(3) Change password.`
	`(4) Clean configuration and initialize all disks.`
	`(5) Maintenance mode boot.`
	`(6) Update flash from backup config.`
	`(7) Install new software first.`
	`(8) Reboot node.`
	`(9) Configure Advanced Drive Partitioning.`
	`Selection (1-19)?`
	`recover_onboard_keymanager`

3. Confirmez que vous souhaitez poursuivre le processus de récupération lorsque vous y êtes invité :

   Afficher l'exemple d'invite

   ```
   This option must be used only in disaster recovery procedures. Are you
   sure? (y or n):
   ```

4. Saisissez deux fois la phrase de passe au niveau du cluster.

   Lors de la saisie du mot de passe, la console n'affiche aucune entrée.

   Afficher l'exemple d'invite

   ```
   Enter the passphrase for onboard key management:

   Enter the passphrase again to confirm:
   ```

5. Saisissez les informations de sauvegarde :

   a. Collez l'intégralité du contenu de la ligne BEGIN BACKUP jusqu'à la ligne END BACKUP, y compris les tirets.

Afficher l'exemple d'invite

```
Enter the backup data:

---------------------------BEGIN
BACKUP---------------------------
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
34567890123456789012345678901234567890123456789012345678901234
56
45678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

---------------------------END
BACKUP---------------------------
```

b. Appuyez deux fois sur la touche Entrée à la fin de la saisie.

   Le processus de récupération est terminé et affiche le message suivant :

   ```
   Successfully recovered keymanager secrets.
   ```

Afficher l'exemple d'invite

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*******************************************************************
******************
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*******************************************************************
******************
```

+

> Ne poursuivez pas si le résultat affiché est autre que `Successfully recovered keymanager secrets` . Effectuez un dépannage pour corriger l'erreur.

6. Sélectionnez une option `1` depuis le menu de démarrage pour continuer le démarrage dans ONTAP.

Afficher l'exemple d'invite

```
*****************************************************************
******************
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****************************************************************
******************


(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Vérifiez que la console de la manette affiche le message suivant :

   ```
   Waiting for giveback…(Press Ctrl-C to abort wait)
   ```

   Sur la manette partenaire :

8. Restituez la manette défectueuse :

   ```
   storage failover giveback -fromnode local -only-cfo-aggregates true
   ```

   Sur la manette défectueuse :

9. Après avoir démarré avec uniquement l'agrégat CFO, synchronisez le gestionnaire de clés :

   ```
   security key-manager onboard sync
   ```

10. Saisissez la phrase secrète globale du cluster pour le gestionnaire de clés intégré lorsque vous y êtes invité.

Afficher l'exemple d'invite

```
Enter the cluster-wide passphrase for the Onboard Key Manager:

All offline encrypted volumes will be brought online and the
corresponding volume encryption keys (VEKs) will be restored
automatically within 10 minutes. If any offline encrypted
volumes are not brought online automatically, they can be
brought online manually using the "volume online -vserver
<vserver> -volume <volume_name>" command.
```

Si la synchronisation réussit, l'invite du cluster est renvoyée sans message supplémentaire. En cas d'échec de la synchronisation, un message d'erreur s'affiche avant le retour à l'invite du cluster. Ne poursuivez pas tant que l'erreur n'est pas corrigée et que la synchronisation n'a pas réussi.

11. Vérifiez que toutes les clés sont synchronisées :

    ```
    security key-manager key query -restored false
    ```

    La commande ne devrait renvoyer aucun résultat. Si des résultats apparaissent, répétez la commande de synchronisation jusqu'à ce qu'aucun résultat ne soit renvoyé.

    Sur la manette partenaire :

12. Restituez la manette défectueuse :

    ```
    storage failover giveback -fromnode local
    ```

13. Restaurez le rétablissement automatique si vous l'avez désactivé :

    ```
    storage failover modify -node local -auto-giveback true
    ```

14. Si AutoSupport est activé, restaurez la création automatique de dossiers :

    ```
    system node autosupport invoke -node * -type all -message MAINT=END
    ```

Gestionnaire de clés externe (EKM)

Restaurez la configuration du gestionnaire de clés externe à partir du menu de démarrage ONTAP.

Avant de commencer

Récupérez les fichiers suivants depuis un autre nœud du cluster ou depuis votre sauvegarde :

- `/cfcard/kmip/servers.cfg`fichier ou l'adresse et le port du serveur KMIP
- `/cfcard/kmip/certs/client.crt`fichier (certificat client)
- `/cfcard/kmip/certs/client.key`fichier (clé client)
- `/cfcard/kmip/certs/CA.pem`fichier (certificats d'autorité de certification du serveur KMIP)

Étapes

Sur la manette défectueuse :

1. Connectez le câble de la console à la manette défectueuse.
2. Sélectionnez une option `11` depuis le menu de démarrage ONTAP .

   Affiche un exemple de menu de démarrage

   ```
   (1)  Normal Boot.
   (2)  Boot without /etc/rc.
   (3)  Change password.
   (4)  Clean configuration and initialize all disks.
   (5)  Maintenance mode boot.
   (6)  Update flash from backup config.
   (7)  Install new software first.
   (8)  Reboot node.
   (9)  Configure Advanced Drive Partitioning.
   (10) Set Onboard Key Manager recovery secrets.
   (11) Configure node for external key management.
   Selection (1-11)? 11
   ```

3. Confirmez avoir recueilli les informations requises lorsque vous y êtes invité :

   Afficher l’exemple d’invite

   ```
   Do you have a copy of the /cfcard/kmip/certs/client.crt file?
   {y/n}
   Do you have a copy of the /cfcard/kmip/certs/client.key file?
   {y/n}
   Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
   Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
   ```

4. Saisissez les informations du client et du serveur lorsque vous y êtes invité :

   a. Saisissez le contenu du fichier de certificat client (client.crt), y compris les lignes BEGIN et END.
   b. Saisissez le contenu du fichier de clé client (client.key), y compris les lignes BEGIN et END.
   c. Entrez le contenu du fichier CA(s) du serveur KMIP (CA.pem), y compris les lignes BEGIN et END.
   d. Saisissez l’adresse IP du serveur KMIP.
   e. Saisissez le port du serveur KMIP (appuyez sur Entrée pour utiliser le port par défaut 5696).

Montrer l'exemple

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

Le processus de récupération est terminé et affiche le message suivant :

```
Successfully recovered keymanager secrets.
```

Montrer l'exemple

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Sélectionnez une option `1` depuis le menu de démarrage pour continuer le démarrage dans ONTAP.

Afficher l'exemple d'invite

```
*******************************************************************
***********
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*******************************************************************
***********

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

6. Restaurez le rétablissement automatique si vous l'avez désactivé :

   ```
   storage failover modify -node local -auto-giveback true
   ```

7. Si AutoSupport est activé, restaurez la création automatique de dossiers :

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

Renvoyez la pièce défectueuse à NetApp - AFF A220 et FAS2700

Retournez la pièce défectueuse à NetApp, tel que décrit dans les instructions RMA (retour de matériel) fournies avec le kit. Voir la "Retour de pièces et remplacements" page pour plus d'informations.

Le système FAS2700 ne prend en charge que les procédures de récupération manuelle du support de démarrage. La récupération automatique du support de démarrage n'est pas prise en charge.

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 DÉLICTUELLE (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.