Support de démarrage

Install and maintain

NetApp
January 10, 2025

Sommaire

Support de démarrage

Présentation du remplacement des supports de démarrage - FAS2820

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 cryptage - FAS2820

Avant d'arrêter le contrôleur défaillant, vérifiez si votre version de ONTAP prend en charge NetApp Volume Encryption (NVE) et si votre système de gestion des clés est correctement configuré.

Étape 1 : vérifiez si votre version de ONTAP prend en charge le chiffrement de volume NetApp

Vérifiez si votre version de ONTAP prend en charge NetApp Volume Encryption (NVE). Ces informations sont essentielles pour télécharger l'image ONTAP correcte.

1. Déterminez si votre version de ONTAP prend en charge le chiffrement en exécutant la commande suivante :

   ```
   version -v
   ```

Si le résultat de cette commande indique `1Ono-DARE`, NVE n'est pas pris en charge par la version de votre cluster.

2. Selon que NVE est pris en charge par votre système, effectuez l'une des actions suivantes :
   - Si NVE est pris en charge, téléchargez l'image ONTAP avec le chiffrement de volume NetApp.
   - Si NVE n'est pas pris en charge, téléchargez l'image ONTAP **sans** chiffrement de volume NetApp.

Étape 2 : déterminez s'il est possible d'arrêter le contrôleur en toute sécurité

Pour arrêter un contrôleur en toute sécurité, identifiez d'abord si le gestionnaire de clés externe (EKM) ou le gestionnaire de clés intégré (OKM) est actif. Ensuite, vérifiez le gestionnaire de clés en cours d'utilisation, affichez les informations de clé appropriées et prenez des mesures en fonction de l'état des clés d'authentification.

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.
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 qu'un gestionnaire de clés est configuré sur votre système, sélectionnez l'une des options suivantes.

Aucun gestionnaire de clés configuré

Vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "arrêtez le contrôleur défectueux".

Gestionnaire de clés externe ou intégré configuré

a. Entrez la commande query suivante pour afficher l'état des clés d'authentification dans votre gestionnaire de clés.

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

b. Vérifiez le résultat de la valeur dans la `Restored` colonne de votre gestionnaire de clés.

Cette colonne indique si les clés d'authentification de votre gestionnaire de clés (EKM ou OKM) ont été restaurées avec succès.

3. Selon que votre système utilise le Gestionnaire de clés externe ou intégré, sélectionnez l'une des options suivantes.

Gestionnaire de clés externe

En fonction de la valeur de sortie affichée dans la `Restored` colonne, suivez les étapes appropriées.

Valeur de sortie dans la `Restored` colonne	**Suivez ces étapes…**
`true`	Vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "arrêtez le contrôleur défectueux".
Autre que `true`	a. Restaurez les clés d'authentification de la gestion externe des clés sur tous les nœuds du cluster à l'aide de la commande suivante : `security key-manager external restore` Si la commande échoue, contactez "Support NetApp". b. Vérifiez que la `Restored` colonne affiche `true` pour toutes les clés d'authentification en saisissant la `security key-manager key query` commande. Si toutes les clés d'authentification sont `true`, vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "arrêtez le contrôleur défectueux".

Gestionnaire de clés intégré

En fonction de la valeur de sortie affichée dans la `Restored` colonne, suivez les étapes appropriées.

Valeur de sortie dans la `Restored` colonne	**Suivez ces étapes…**
`true`	Sauvegardez manuellement les informations sur OKM. a. Accédez au mode avancé en entrant, puis `Y` en entrant `set -priv advanced` lorsque vous y êtes invité. b. Entrez la commande suivante pour afficher les informations de gestion des clés : `security key-manager onboard show-backup` c. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM. d. Vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "arrêtez le contrôleur défectueux".

Valeur de sortie dans la `Restored` colonne	Suivez ces étapes…

Autre que `true`	a. Entrez la commande de synchronisation du gestionnaire de clés de sécurité intégré :
	
	`security key-manager onboard sync`
	
	b. Entrez la phrase de passe alphanumérique de gestion des clés intégrée de 32 caractères lorsque vous y êtes invité.
	
	Si la phrase de passe ne peut pas être fournie, contactez "Support NetApp".
	
	c. Vérifiez que la `Restored` colonne s'affiche `true` pour toutes les clés d'authentification :
	
	`security key-manager key query`
	
	d. Vérifiez que le `Key Manager` type s'affiche `onboard`, puis sauvegardez manuellement les informations sur OKM.
	e. Entrez la commande pour afficher les informations de sauvegarde de la gestion des clés :
	
	`security key-manager onboard show-backup`
	
	f. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal.
	
	Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.
	
	g. Vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "arrêtez le contrôleur défectueux".

Arrêtez le contrôleur défectueux - FAS2820

Arrêtez ou prenez le contrôle du contrôleur défectueux.

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.

Si le contrôleur en état de fonctionnement s'affiche…	Alors…
`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.

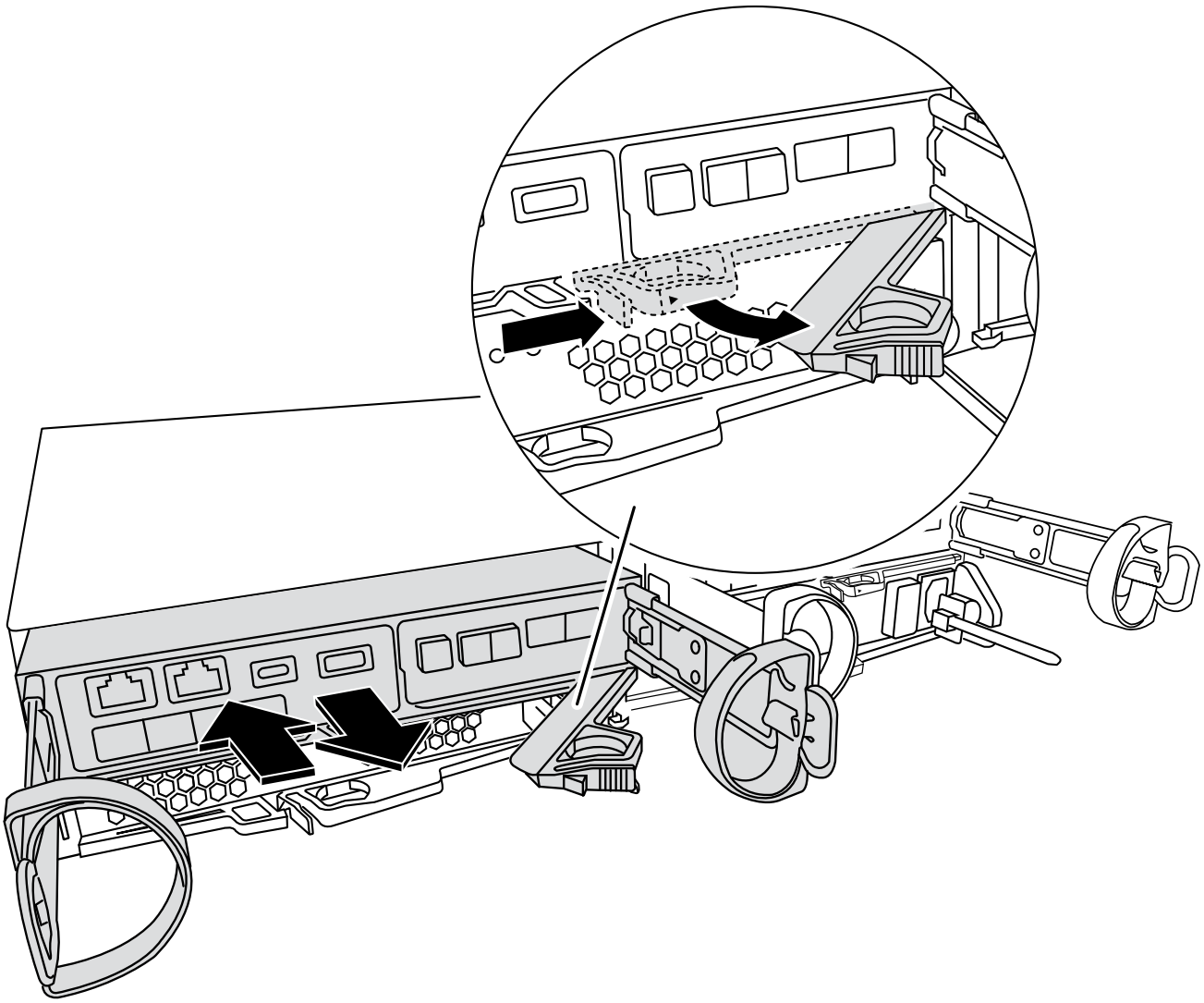
Remplacez le support de démarrage - FAS2820

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.

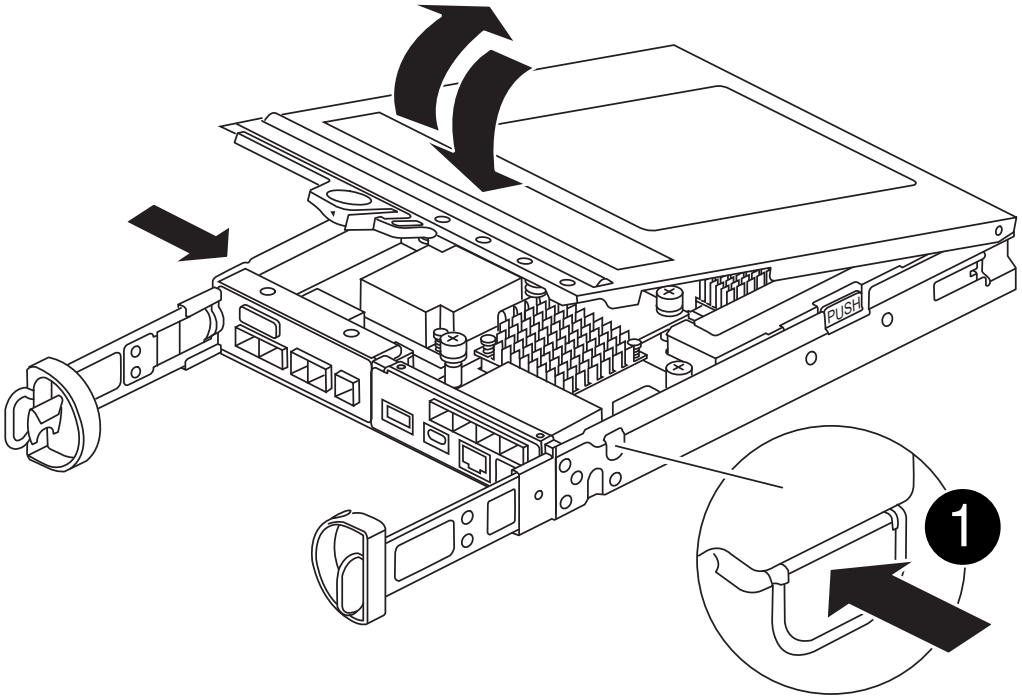
Étape 1 : retirer le module de contrôleur

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.
3. 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.



4. Retournez le module de contrôleur et placez-le sur une surface plane et stable.
5. Ouvrez le capot en appuyant sur les boutons bleus situés sur les côtés du module de contrôleur pour libérer le capot, puis faites pivoter le capot vers le haut et hors du module de contrôleur.

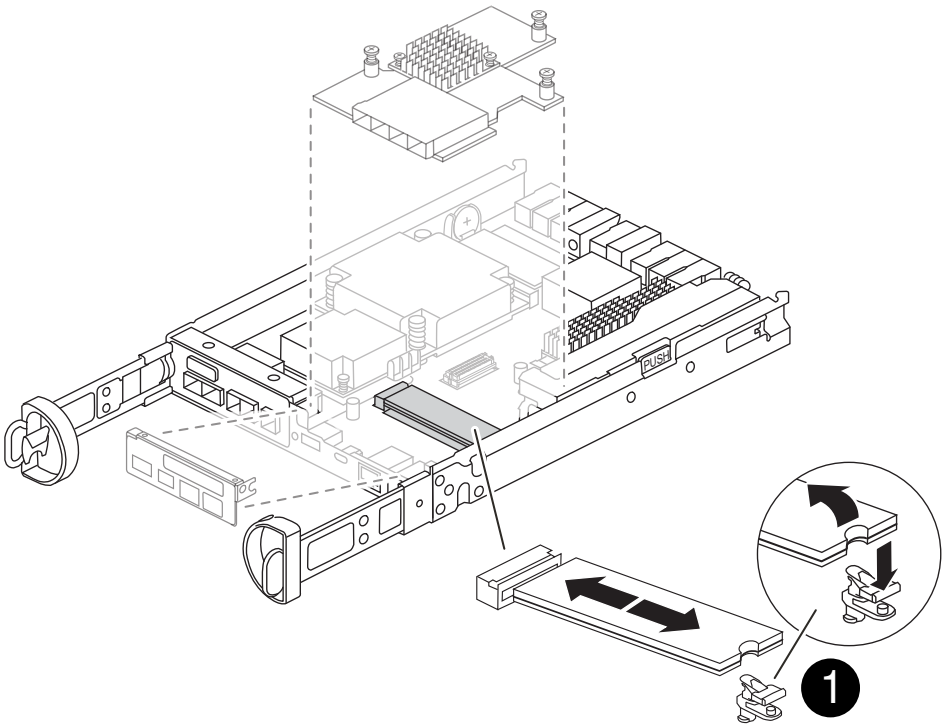


1	Bouton de déverrouillage du capot du module de contrôleur

Étape 2 : remplacer le support de démarrage

Localisez le support de démarrage dans le module de contrôleur, situé sous la carte mezzanine et suivez les instructions pour le remplacer.

Animation : remplacez le support de démarrage



1	Languette de verrouillage du support de démarrage

Étapes

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Retirez la carte mezzanine à l'aide de l'illustration suivante ou du mappage FRU sur le module de contrôleur :
   a. Retirez la plaque d'E/S en la faisant glisser hors du module de contrôleur.
   b. Desserrez les vis à molette de la carte mezzanine.

      Vous pouvez desserrer les vis moletées avec vos doigts ou un tournevis. Si vous utilisez vos doigts, vous devrez peut-être faire pivoter la batterie NV vers le haut pour obtenir un meilleur achat de doigts sur la vis à molette située à côté de celle-ci.

   c. Soulevez la carte mezzanine.
3. Remplacez le support de démarrage :
   a. Appuyez sur le bouton bleu du boîtier du support de démarrage pour libérer le support de démarrage de son logement, faites pivoter le support de démarrage vers le haut, 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.

   b. Alignez les bords du support de démarrage de remplacement avec le support de démarrage, puis poussez-le doucement dans le support. Vérifiez le support de démarrage pour vous assurer qu'il est correctement inséré dans le support et, si nécessaire, retirez le support de démarrage et réinstallez-le dans le support.
   c. Appuyez sur le bouton de verrouillage bleu, faites pivoter le support de démarrage complètement vers le bas, puis relâchez le bouton de verrouillage pour verrouiller le support de démarrage en place.
4. Réinstallez la carte mezzanine :
   a. Alignez le connecteur de la carte mère avec le connecteur de la carte mezzanine, puis insérez doucement la carte dans le support.
   b. Serrez les trois vis à molette de la carte mezzanine.
   c. Réinstallez la plaque d'E/S.
5. Réinstallez le capot du module de contrôleur et verrouillez-le en place.

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

Installez l'image système sur le support de démarrage de remplacement à l'aide d'une clé USB sur laquelle l'image est installée. Vous devez restaurer le système de fichiers var au cours de cette procédure.

Avant de commencer

- Vous devez disposer d'une clé USB, formatée en MBR/FAT32, d'une capacité minimale de 4 Go.
- Vous devez disposer d'une connexion réseau.

Étapes

1. Téléchargez la version d'image appropriée de ONTAP sur le lecteur flash USB formaté :
   a. Utiliser "Comment déterminer si la version ONTAP en cours d'exécution prend en charge NetApp Volume Encryption (NVE)" pour déterminer si le chiffrement de volume est actuellement pris en charge.
      - Si NVE est pris en charge sur le cluster, téléchargez l'image avec le chiffrement de volume NetApp.
      - Si NVE n'est pas pris en charge sur le cluster, téléchargez l'image sans chiffrement de volume NetApp. Voir "Quelle image ONTAP dois-je télécharger ? Avec ou sans chiffrement de volume ?" pour en savoir plus.
2. Décompressez l'image téléchargée.

   Si vous extrayez le contenu à l'aide de Windows, n'utilisez pas WinZip pour extraire l'image netboot. Utilisez un autre outil d'extraction, tel que 7-Zip ou WinRAR.

   Le fichier image du service décompressé contient deux dossiers :

   - `boot`
   - `efi`
     i. Copiez le `efi` Dossier dans le répertoire supérieur de la clé USB.

        Le lecteur flash USB doit avoir le dossier efi et la même version BIOS (Service image) de ce que le contrôleur douteux est en cours d'exécution.

     ii. Retirez la clé USB de votre ordinateur portable.
3. Installez le module de contrôleur :
   a. 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.
   b. Recâblage du module de contrôleur.

      Lors de la remise en état, n'oubliez pas de réinstaller les convertisseurs de support (SFP) s'ils ont été retirés.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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 - FAS2820

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 :

Option 1 : ONTAP 9.16.0 ou version antérieure

a. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `Do you want to restore the backup configuration now?`

b. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à remplacer */etc/ssh/ssh_host_ecdsa_key*.

c. Sur le contrôleur sain, définissez le contrôleur défectueux sur le niveau de privilège avancé : `set -privilege advanced`.

d. Sur le contrôleur partenaire sain, exécutez la commande restore backup : `system node restore-backup -node local -target-address impaired_node_IP_address` .

REMARQUE : si vous voyez un message autre qu'une restauration réussie, contactez "Support NetApp".

e. Sur le contrôleur partenaire sain, remettez le contrôleur défectueux au niveau admin: `set -privilege admin`.

f. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `Was the restore backup procedure successful?`.

g. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `...would you like to use this restored copy now?`.

h. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le contrôleur défectueux et appuyez sur `ctrl-c` pour accéder au menu de démarrage.

i. Si le système n'utilise pas le chiffrement, sélectionnez *option 1 démarrage normal.*, sinon, passez à "Restaurez le chiffrement".

Option 2 : ONTAP 9.16.1 ou version ultérieure

a. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à restaurer la configuration de sauvegarde.

Une fois la procédure de restauration réussie, ce message s'affiche sur la console - `syncflash_partner: Restore from partner complete`.

b. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous y êtes invité pour confirmer si la sauvegarde de restauration a réussi.

c. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à utiliser la configuration restaurée.

d. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le nœud.

e. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le contrôleur défectueux et appuyez sur `ctrl-c` pour accéder au menu de démarrage.

f. Si le système n'utilise pas le chiffrement, sélectionnez *option 1 démarrage normal.*, sinon, passez à "Restaurez le chiffrement".

4. Branchez le câble de la console au contrôleur partenaire.
5. Reaccordez le contrôleur à l'aide du `storage failover giveback -fromnode local` commande.
6. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node`

`local -auto-giveback true` commande.

7. Si AutoSupport est activé, restaurez/annulez la création automatique de cas à l'aide de la `system node autosupport invoke -node * -type all -message MAINT=END` commande.

   REMARQUE : si le processus échoue, contactez "Support NetApp".

Restaurer le chiffrement - FAS2820

Restaurez le chiffrement sur le support de démarrage de remplacement.

Vous devez effectuer les étapes spécifiques aux systèmes pour lesquels le gestionnaire de clés intégré (OKM), le chiffrement de stockage NetApp (NSE) ou le chiffrement de volume NetApp (NVE) sont activés à l'aide des paramètres capturés au début de la procédure de remplacement des supports de démarrage.

Selon le gestionnaire de clés configuré sur votre système, sélectionnez l'une des options suivantes pour le restaurer dans le menu de démarrage.

- "Option 1 : restaurez la configuration du gestionnaire de clés intégré"
- "Option 2 : restaurez la configuration du gestionnaire de clés externe"

Option 1 : restaurez la configuration du gestionnaire de clés intégré

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

Avant de commencer

- Assurez-vous de disposer des informations suivantes lors de la restauration de la configuration de OKM :
  - Phrase de passe à l'échelle du cluster entrée "tout en activant la gestion intégrée des clés".
  - "Informations de sauvegarde pour le gestionnaire de clés intégré".
- Effectuer la "Comment vérifier la sauvegarde de gestion intégrée des clés et la phrase secrète au niveau du cluster" procédure avant de continuer.

Étapes

1. Branchez le câble de la console au contrôleur cible.
2. Dans le menu de démarrage ONTAP, sélectionnez l'option appropriée dans le menu de démarrage.

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 restauration.

   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.

   Lorsque vous saisissez la phrase 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. Entrez les informations de sauvegarde.

   a. Collez l'intégralité du contenu de la ligne de DÉBUT DE SAUVEGARDE à travers la ligne de FIN DE SAUVEGARDE.

Afficher l’exemple d’invite

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

b. Appuyez deux fois sur la touche entrée à la fin de l’entrée.

   Le processus de récupération est terminé.

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 continuez pas si la sortie affichée est autre que `Successfully recovered keymanager secrets`. Effectuez le dépannage pour corriger l'erreur.

6. Sélectionnez l'option 1 dans le menu de démarrage pour poursuivre 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. Vérifier que la console du contrôleur affiche le message suivant.

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

8. Depuis le nœud partenaire, rendre le contrôleur partenaire en saisissant la commande suivante.

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

9. Après le démarrage avec uniquement l'agrégat CFO, exécutez la commande suivante.

   `security key-manager onboard sync`

10. Saisissez la phrase secrète pour l'ensemble du cluster pour le gestionnaire de clés intégré.

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. Si la synchronisation échoue, un message d'erreur s'affiche avant de revenir à l'invite du cluster. Ne continuez pas tant que l'erreur n'a pas été corrigée et que la synchronisation a réussi.

11. Vérifiez que toutes les clés sont synchronisées en saisissant la commande suivante.

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

    There are no entries matching your query.
    ```

    Aucun résultat ne doit apparaître lors du filtrage de FALSE dans le paramètre restauré.

12. Réverso le nœud du partenaire en saisissant la commande suivante.

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

13. Si vous l'avez désactivée, restaurez le rétablissement automatique en saisissant la commande suivante.

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

14. Si AutoSupport est activé, restaurez la création automatique de dossiers en saisissant la commande suivante.

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

Option 2 : restaurez la configuration du gestionnaire de clés externe

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

Avant de commencer

Vous avez besoin des informations suivantes pour restaurer la configuration du Gestionnaire de clés externe (EKM).

- Copie du fichier /cfcard/kmip/servers.cfg à partir d'un autre nœud de cluster ou des informations suivantes :

- Adresse du serveur KMIP.
- Port KMIP.

- Copie du `/cfcard/kmip/certs/client.crt` fichier d'un autre nœud de cluster ou du certificat client.
- Copie du `/cfcard/kmip/certs/client.key` fichier d'un autre nœud de cluster ou de la clé client.
- Copie du `/cfcard/kmip/certs/CA.pem` fichier d'un autre nœud de cluster ou de l'autorité de certification du serveur KMIP.

Étapes

1. Branchez le câble de la console au contrôleur cible.
2. Sélectionnez l'option 11 dans 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. Lorsque vous y êtes invité, vérifiez que vous avez recueilli les informations requises.

   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. Lorsque vous y êtes invité, entrez les informations sur le client et le serveur.

Afficher l'invite

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Montrer l'exemple

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----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-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----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
```

Une fois que vous avez saisi les informations sur le client et le serveur, le processus de récupération se termine.

Montrer l'exemple

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Sélectionnez l'option 1 dans le menu de démarrage pour poursuivre 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. Si vous l'avez désactivée, restaurez le rétablissement automatique en saisissant la commande suivante.

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

7. Si AutoSupport est activé, restaurez la création automatique de dossiers en saisissant la commande suivante.

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

Renvoyez la pièce défectueuse à NetApp - FAS2820

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.

Informations sur le copyright

Informations sur les marques commerciales