Support de démarrage

Install and maintain

NetApp
April 19, 2024

Sommaire

Support de démarrage

Présentation du remplacement des supports de démarrage - FAS2800

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.

Vérifiez les clés de chiffrement intégrées - FAS2800

Avant d'arrêter le contrôleur douteux et de vérifier le statut des clés de cryptage intégrées, vous devez vérifier le statut de ce contrôleur, désactiver le giveback automatique et vérifier la version de ONTAP en cours d'exécution.

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".

Étapes

1. Vérifier l'état du contrôleur détérioré :
   - Si le contrôleur douteux se trouve à l'invite de connexion, connectez-vous en tant que `admin`.
   - Si le contrôleur associé est au niveau de l'invite DU CHARGEUR et qu'il fait partie de la configuration HA, connectez-vous en tant que `admin` sur le contrôleur sain.
2. 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`

3. Vérifiez la version de ONTAP que le système fonctionne sur le contrôleur défaillant, si c'est le cas, ou sur le contrôleur partenaire si le contrôleur défaillant est en panne, à l'aide du `version -v` commande :
   - Si <lno-DARE> ou <1Ono-DARE> s'affiche dans le résultat de la commande, le système ne prend pas en charge NVE, passez à l'étape "Arrêtez le contrôleur défaillant".
   - Si <lno-DARE> ne s'affiche pas dans le résultat de la commande et que le système exécute ONTAP 9.6 ou une version ultérieure, passez à la section suivante, Vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures.
4. Désactiver le rétablissement automatique à partir du contrôleur sain : storage failover modify -node local -auto-giveback false` ou `storage failover modify -node local -auto-giveback-after -panic false`

Vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures

Avant d'arrêter le contrôleur défaillant, vérifiez si NetApp Volume Encryption (NVE) ou NetApp Storage Encryption (NSE) sont activés sur le système. Si c'est le cas, vous devez vérifier la configuration.

1. Vérifiez que NVE est utilisé pour n'importe quel volume du cluster : `volume show -is-encrypted true`

   Si des volumes sont répertoriés dans le résultat, NVE est configuré et vous devez vérifier la configuration NVE. Si aucun volume n'est indiqué, vérifiez si NSE est configuré et utilisé.

2. Vérifiez si NSE est configuré et utilisé : `storage encryption disk show`
   - Si le résultat de la commande répertorie les détails du disque avec les informations relatives au mode et à l'ID de clé, NSE est configuré et vous devez vérifier la configuration NSE et son utilisation.
   - Si aucun disque n'est affiché, NSE n'est pas configuré.
   - Si NVE et NSE ne sont pas configurés, aucun disque n'est protégé avec les clés NSE, vous pouvez arrêter le contrôleur pour facultés affaiblies.

Vérifiez la configuration NVE

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager key query`

   > Après la version ONTAP 9.6, il est possible que vous ayez d'autres types de gestionnaire de clés. Les types sont `KMIP`, `AKV`, et `GCP`. Le processus de confirmation de ces types est identique à celui de la confirmation `external` ou `onboard` types de gestionnaire de clés.

   - Si le `Key Manager` affichage du type `external` et le `Restored` s'affiche `yes`, il est sûr d'arrêter le contrôleur défaillant.
   - Si le `Key Manager` affichage du type `onboard` et le `Restored` s'affiche `yes`, vous devez effectuer quelques étapes supplémentaires.

- Si le `Key Manager` affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.
- Si le `Key Manager` affichage du type `onboard` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.

2. Si le `Key Manager` affichage du type `onboard` et le `Restored` s'affiche `yes`, Sauvegardez manuellement les informations OKM :
   a. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
   b. Entrez la commande 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. Revenir en mode admin: `set -priv admin`
   e. Arrêtez le contrôleur défaillant.
3. Si le `Key Manager` affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`:
   a. Restaurer les clés d'authentification externe de gestion des clés sur tous les nœuds du cluster : `security key-manager external restore`

      Si la commande échoue, contactez le support NetApp.

   "mysupport.netapp.com"

   a. Vérifiez que le `Restored` colonne égale à `yes` pour toutes les clés d'authentification : `security key-manager key query`
   b. Arrêtez le contrôleur défaillant.
4. Si le `Key Manager` affichage du type `onboard` et le `Restored` colonne affiche tout autre élément que `yes`:
   a. Entrez la commande de synchronisation du gestionnaire de clés de sécurité intégré : `security key-manager onboard sync`

      > Saisissez la phrase de passe alphanumérique de gestion des clés intégrée de 32 caractères du client à l'invite. Si cette phrase secrète ne peut pas être fournie, contactez le support NetApp. "mysupport.netapp.com"

   b. Vérifiez le `Restored` affiche la colonne `yes` pour toutes les clés d'authentification : `security key-manager key query`
   c. Vérifiez que le `Key Manager` s'affiche `onboard`, Puis sauvegardez manuellement les informations OKM.
   d. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
   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. Revenir en mode admin: `set -priv admin`

h. Vous pouvez arrêter le contrôleur en toute sécurité.

Vérifiez la configuration NSE

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager key query -key-type NSE-AK`

> Après la version ONTAP 9.6, il est possible que vous ayez d'autres types de gestionnaire de clés. Les types sont `KMIP`, `AKV`, et `GCP`. Le processus de confirmation de ces types est identique à celui de la confirmation `external` ou `onboard` types de gestionnaire de clés.

   - Si le `Key Manager` affichage du type `external` et le `Restored` s'affiche `yes`, il est sûr d'arrêter le contrôleur défaillant.
   - Si le `Key Manager` affichage du type `onboard` et le `Restored` s'affiche `yes`, vous devez effectuer quelques étapes supplémentaires.
   - Si le `Key Manager` affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.
   - Si le `Key Manager` affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.

2. Si le `Key Manager` affichage du type `onboard` et le `Restored` s'affiche `yes`, Sauvegardez manuellement les informations OKM :

   a. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`

   b. Entrez la commande 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. Revenir en mode admin: `set -priv admin`

   e. Vous pouvez arrêter le contrôleur en toute sécurité.

3. Si le `Key Manager` affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`:

   a. Restaurer les clés d'authentification externe de gestion des clés sur tous les nœuds du cluster : `security key-manager external restore`

   Si la commande échoue, contactez le support NetApp.

"mysupport.netapp.com"

   a. Vérifiez que le `Restored` colonne égale à `yes` pour toutes les clés d'authentification : `security key-manager key query`

b. Vous pouvez arrêter le contrôleur en toute sécurité.

4. Si le `Key Manager` affichage du type `onboard` et le `Restored` colonne affiche tout autre élément que `yes`:

   a. Entrez la commande de synchronisation du gestionnaire de clés de sécurité intégré : `security key-manager onboard sync`

      Saisissez la phrase de passe alphanumérique de gestion des clés intégrée de 32 caractères du client à l'invite. Si cette phrase secrète ne peut pas être fournie, contactez le support NetApp.

   "mysupport.netapp.com"

   a. Vérifiez le `Restored` affiche la colonne `yes` pour toutes les clés d'authentification : `security key-manager key query`

   b. Vérifiez que le `Key Manager` s'affiche `onboard`, Puis sauvegardez manuellement les informations OKM.

   c. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`

   d. Entrez la commande pour afficher les informations de sauvegarde de la gestion des clés : `security key-manager onboard show-backup`

   e. 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.

   f. Revenir en mode admin: `set -priv admin`

   g. Vous pouvez arrêter le contrôleur en toute sécurité.

Arrêtez le contrôleur défectueux - FAS2800

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.
`Waiting for giveback…`	Appuyez sur Ctrl-C, puis répondez `y` lorsque vous y êtes invité.

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

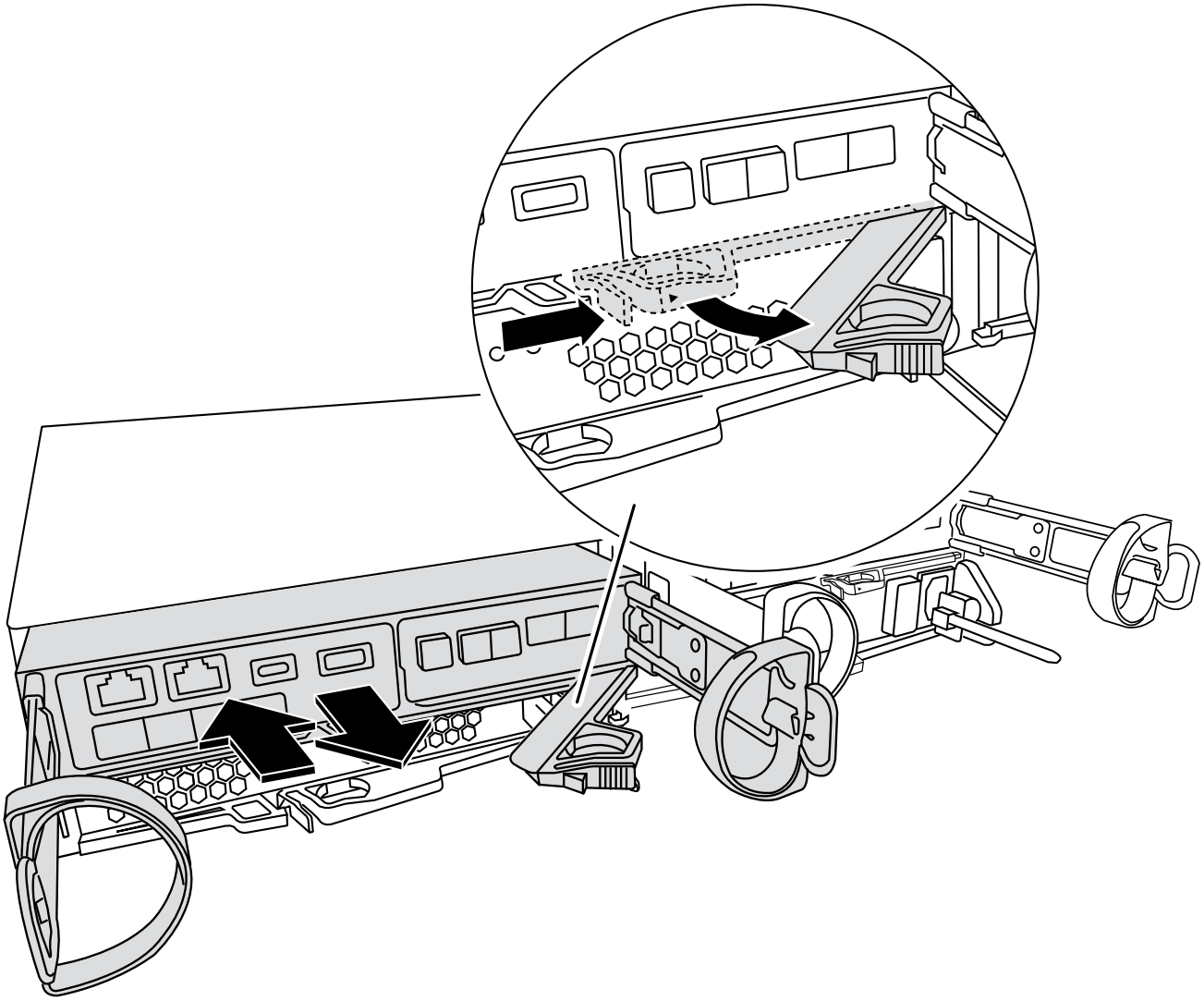
Remplacez le support de démarrage - FAS2800

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.

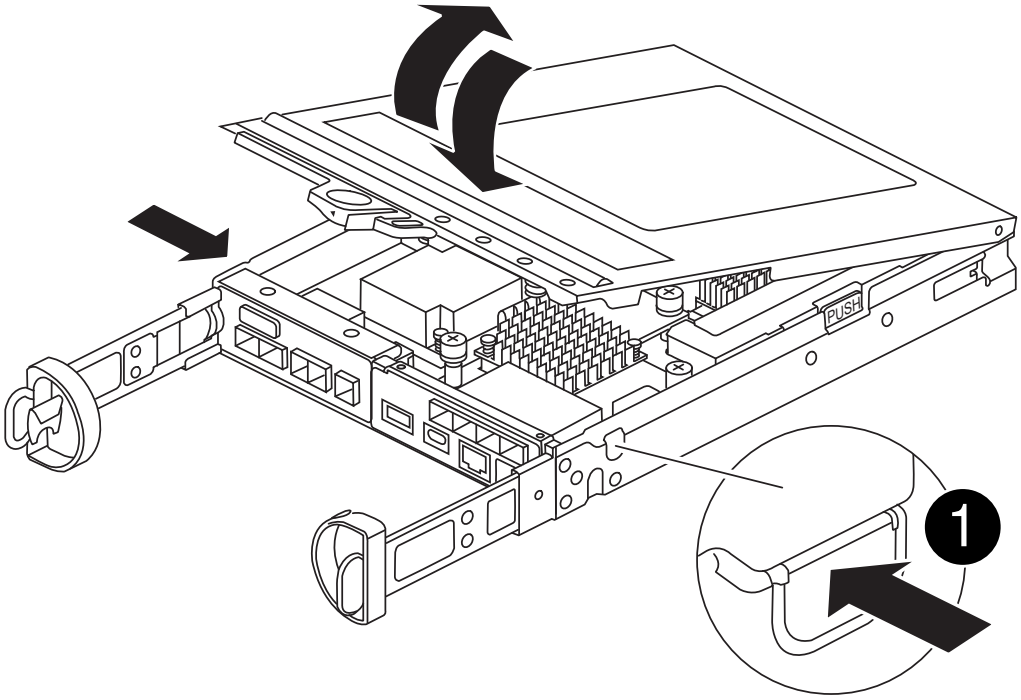
Étape 1 : retirer le module de contrôleur

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.

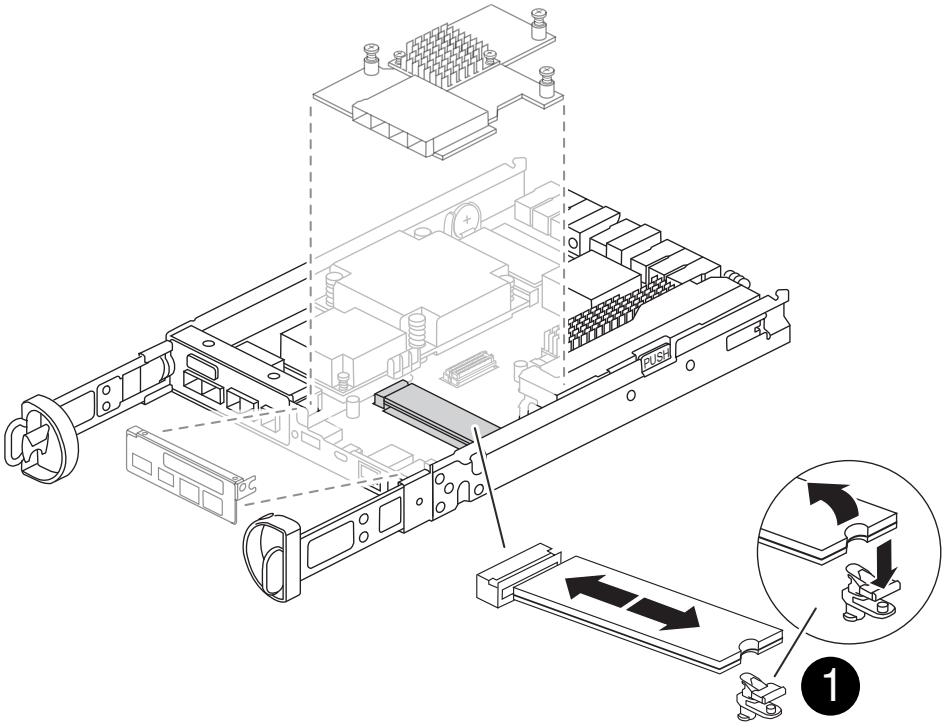


1	Bouton de déverrouillage du capot du module de contrôleur

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 le cadre de la carte mezzanine en le 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 le cadre de la mezzanine.

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 - FAS2800

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 nœud 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 nœud au niveau admin : `set -privilege admin` e. Appuyez sur `y` lorsque vous êtes invité à confirmer si la restauration de la sauvegarde a réussi. f. Appuyez sur `y` lorsque vous êtes invité à restaurer la copie de configuration. g. Appuyez sur `y` lorsque vous êtes invité à redémarrer le nœud.
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 show -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 -vserver` *`vserver_name`* `-lif` *`lif_name`* 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. Si vous n'utilisez pas le chiffrement du stockage, restaurez le rétablissement automatique et AutoSupport :

    a. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

    b. Si une fenêtre de maintenance AutoSupport a été déclenchée, mettez-la fin à l'aide du `system node autosupport invoke -node * -type all -message MAINT=END` commande.

Restaurez OKM, NSE et NVE selon les besoins - FAS2800

Une fois les variables d'environnement vérifiées, vous devez effectuer les étapes spécifiques aux systèmes sur 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 que vous avez capturés au début de cette procédure.

Si NSE ou NVE sont activés avec le gestionnaire de clés intégré, vous devez restaurer les paramètres que vous avez capturés au début de cette procédure.

Étapes

1. Branchez le câble de la console au contrôleur cible.
2. Utilisez le `boot_ontap` Commande à l'invite DU CHARGEUR pour démarrer le contrôleur.
3. Vérifiez la sortie de la console :

Si la console affiche…	Alors…
Invite de connexion	Passez à l'étape 7.
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.

4. Déplacez le câble de la console vers le contrôleur partenaire et redonnez le stockage du contrôleur cible à l'aide du `storage failover giveback -fromnode local -only-cfo-aggregates true local` commande.
   - Si la commande échoue en raison d'un disque en panne, désengagez physiquement le disque en panne, mais laissez le disque dans le slot jusqu'à ce qu'un disque de remplacement soit reçu.
   - Si la commande échoue en raison d'une session CIFS ouverte, vérifiez auprès du client comment fermer les sessions CIFS.

     L'arrêt du protocole CIFS peut entraîner la perte de données.

   - Si la commande échoue parce que le partenaire n'est pas prêt, attendez 5 minutes pour que le système NVMEMs se synchronise.
   - Si la commande échoue en raison d'un processus NDMP, SnapMirror ou SnapVault, désactivez le processus. Consultez le centre de documentation approprié pour plus d'informations.
5. Attendre 3 minutes et vérifier l'état du basculement à l'aide du `storage failover show` commande.
6. À l'invite clustershell, entrez le `net int show -is-home false` commande pour lister les interfaces logiques qui ne se trouvent pas sur leur contrôleur et son port de base.

   Si des interfaces sont répertoriées comme `false`, restaurez ces interfaces à leur port de départ à l'aide de l' `net int revert -vserver Cluster -lif` *`nodename`* commande.

7. Déplacer le câble de la console vers le contrôleur cible et exécuter le `version -v` Commande pour vérifier les versions de ONTAP.
8. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.
9. Utilisez le `storage encryption disk show` à l'invite clustershell, pour vérifier la sortie.
10. Utilisez le `security key-manager key query` Commande pour afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés.
    - Si le `Restored` colonne = `yes/true`, vous avez terminé et pouvez procéder à la procédure de

remplacement.

- Si le `Key Manager type` = `external` et le `Restored` colonne = tout autre élément que `yes/true`, utilisez l' `security key-manager external restore` Commande permettant de restaurer les ID de clé des clés d'authentification.

  Si la commande échoue, contactez l'assistance clientèle.

- Si le `Key Manager type` = `onboard` et le `Restored` colonne = tout autre élément que `yes/true`, utilisez l' `security key-manager onboard sync` Commande permettant de resynchroniser le type de gestionnaire de clés.

  Utilisez la requête de clé de sécurité du gestionnaire de clés pour vérifier que l' `Restored` colonne = `yes/true` pour toutes les clés d'authentification.

11. Branchez le câble de la console au contrôleur partenaire.
12. Reaccordez le contrôleur à l'aide du `storage failover giveback -fromnode local` commande.
13. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.
14. Restaurez AutoSupport s'il a été désactivé à l'aide de `system node autosupport invoke -node * -type all -message MAINT=END`

Renvoyer la pièce défectueuse à NetApp - FAS2800

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