Support de démarrage

Install and maintain

NetApp
September 06, 2024

Sommaire

Support de démarrage

Présentation du remplacement du support de démarrage : AFF A320

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 : AFF A320

Avant d'arrêter le contrôleur défaillant et de vérifier l'état des clés de chiffrement intégrées, vous devez vérifier l'état du contrôleur défaillant, désactiver le rétablissement automatique et vérifier quelle version de ONTAP s'exécute sur le système.

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.
   - Si le contrôleur douteux se trouve dans une configuration autonome et à l'invite DU CHARGEUR, contactez "mysupport.netapp.com".

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 la sortie de la commande, le système ne prend pas en charge NVE, procédez à l'arrêt du contrôleur.
   - Si <lno-DARE> ne s'affiche pas dans la sortie de la commande et si le système exécute ONTAP 9.6 ou une version ultérieure, passer à la section suivante.

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 nœud : AFF A320

Une fois les tâches NVE ou NSE effectuées, vous devez arrêter le nœud douteux. Arrêtez ou prenez le contrôleur défaillant en suivant la procédure appropriée pour votre configuration.

Option 1 : la plupart des systèmes

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.

Option 2 : le système est dans un MetroCluster

> 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.

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

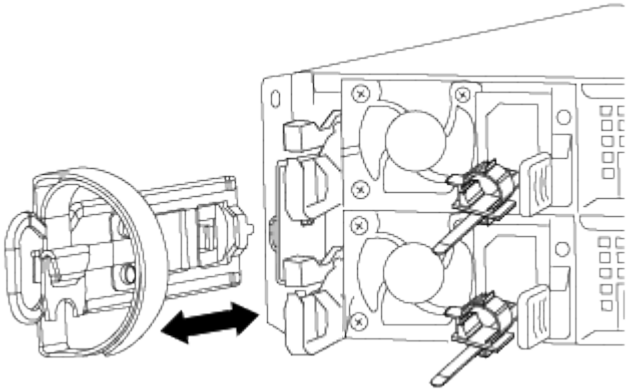
Remplacez le support de démarrage : AFF A320

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

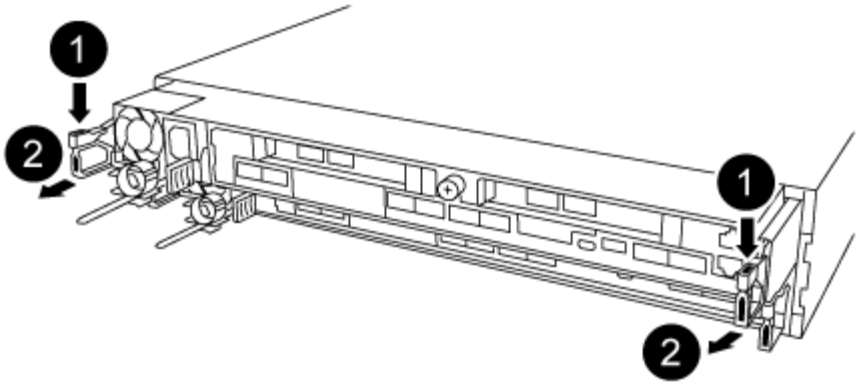
Pour accéder aux composants à l'intérieur du module de contrôleur, vous devez retirer le module de contrôleur du châssis.

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Débranchez l'alimentation du module de contrôleur de la source d'alimentation.
3. 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.

4. Retirez et mettez de côté les dispositifs de gestion des câbles des côtés gauche et droit du module de contrôleur.
5. Retirer le module de contrôleur du châssis :



a. Insérez l'index dans le mécanisme de verrouillage de chaque côté du module de contrôleur.
b. Appuyez sur la languette orange située sur la partie supérieure du mécanisme de verrouillage jusqu'à ce qu'elle se dégage de la goupille de verrouillage du châssis.

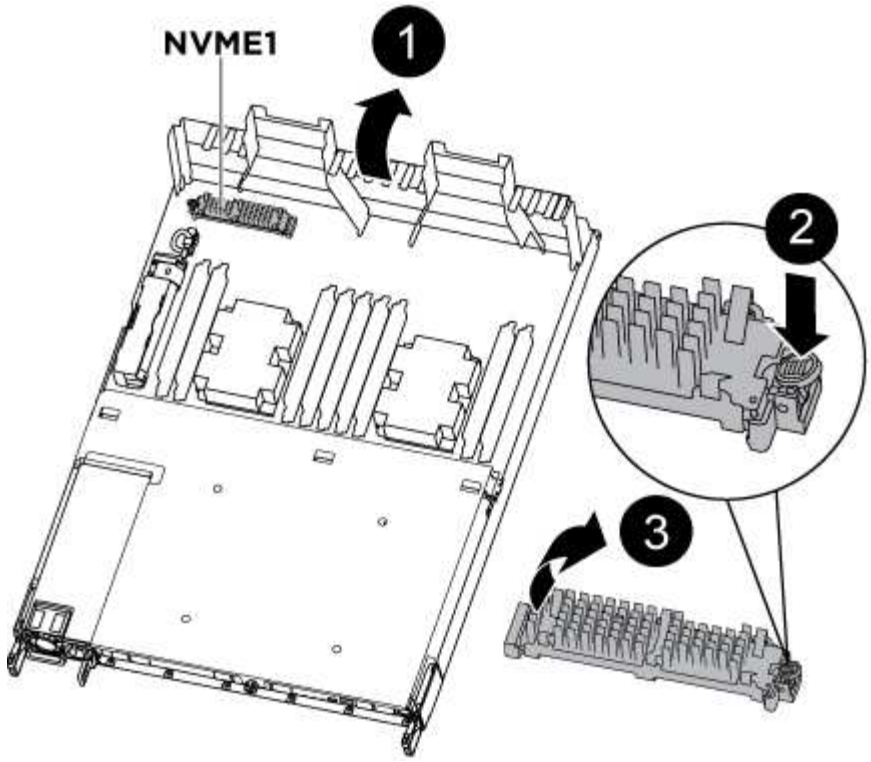
   Le crochet du mécanisme de verrouillage doit être presque vertical et doit être dégagé de l'axe du châssis.

c. Tirez doucement le module de contrôleur de quelques pouces vers vous pour pouvoir saisir les côtés du module de contrôleur.
d. A l'aide des deux mains, tirez doucement le module de contrôleur hors du châssis et posez-le sur une surface plane et stable.

Étape 2 : remplacer le support de démarrage

Vous devez localiser le support de démarrage dans le module de contrôleur, puis suivre les instructions pour le remplacer.

1. Ouvrez le conduit d'air et localisez le support de démarrage à l'aide de l'illustration ou du mappage des FRU sur le module de contrôleur :
2. Recherchez et retirez le support de démarrage du module de contrôleur :



a. Appuyez sur le bouton bleu à l'extrémité du support de démarrage jusqu'à ce que le rebord du support de démarrage disparaisse du bouton bleu.

b. Faites pivoter le support de démarrage vers le haut et retirez doucement le support de démarrage du support.

   i. 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.

3. Verrouillez le support de démarrage en place :

   a. Faites pivoter le support de démarrage vers le bas, vers la carte mère.

   b. En plaçant un doigt à l'extrémité du support de démarrage par le bouton bleu, appuyez sur l'extrémité du support de démarrage pour engager le bouton de verrouillage bleu.

   c. Tout en appuyant sur le support de démarrage, soulevez le bouton de verrouillage bleu pour verrouiller le support de démarrage en place.

4. Fermer le conduit d'air.

Étape 3 : transférez l'image d'amorçage sur le support d'amorçage à l'aide d'une clé USB

Le support de démarrage de remplacement que vous avez installé ne dispose pas d'une image d'amorçage. Vous devez donc transférer une image d'amorçage à l'aide d'un lecteur flash USB.

- Vous devez disposer d'une clé USB, formatée en MBR/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.

a. Téléchargez et copiez l'image de service appropriée depuis le site de support NetApp vers le lecteur Flash USB.

   i. Téléchargez l'image du service sur votre espace de travail sur votre ordinateur portable.

   ii. Décompressez l'image du service.

   > 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 :

   - démarrage
   - efi

   iii. Copiez le dossier efi dans le répertoire supérieur du lecteur flash 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.

   iv. Retirez la clé USB de votre ordinateur portable.

b. Si ce n'est déjà fait, fermer le conduit d'air.

c. 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.

d. Réinstallez le périphérique de gestion des câbles et recâblage du système, selon les besoins.

   Lors du retrait, n'oubliez pas de réinstaller les convertisseurs de support (SFP ou QSFP) s'ils ont été retirés.

e. Branchez le câble d'alimentation dans le bloc d'alimentation et réinstallez le dispositif de retenue du câble d'alimentation.

f. 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.

g. Terminez la réinstallation du module de contrôleur :

   i. S'assurer que les bras de verrouillage sont verrouillés en position étendue.

   ii. A l'aide des bras de verrouillage, poussez le module de contrôleur dans la baie du châssis jusqu'à ce qu'il s'arrête.

   > Ne pas pousser le mécanisme de verrouillage en haut des bras de verrouillage vers le bas. Relever le mécanisme de verrouillage et empêcher le déplacement du module de contrôleur dans le châssis.

iii. Appuyez sur les languettes orange du haut du mécanisme de verrouillage et maintenez-les enfoncées.

iv. Poussez doucement le module contrôleur dans la baie du châssis jusqu'à ce qu'il affleure les bords du châssis.

> Les bras du mécanisme de verrouillage coulissent dans le châssis.

Le module de contrôleur commence à démarrer dès qu'il est complètement inséré dans le châssis.

i. Libérer les loquets pour verrouiller le module de contrôleur en place.

ii. Si ce n'est déjà fait, réinstallez le périphérique de gestion des câbles.

   a. Interrompez le processus de démarrage en appuyant sur Ctrl-C pour vous arrêter à l'invite DU CHARGEUR.

      Si vous manquez ce message, appuyez sur Ctrl-C, sélectionnez l'option pour démarrer en mode maintenance, puis arrêtez le nœud pour démarrer le CHARGEUR.

   b. 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.

   c. Lorsque vous y êtes invité, entrez le nom de l'image ou acceptez l'image par défaut affichée entre crochets sur votre écran.

   d. Une fois l'image installée, démarrez le processus de restauration :

iii. Notez l'adresse IP du nœud douteux qui s'affiche à l'écran.

iv. Appuyez sur `y` lorsque vous êtes invité à restaurer la configuration de sauvegarde.

v. Appuyez sur `y` lorsque vous êtes invité à remplacer /etc/ssh/ssh_host_dsa_key.

   a. À partir du nœud partenaire au niveau de privilège avancé, démarrez la synchronisation de la configuration à l'aide de l'adresse IP enregistrée à l'étape précédente : `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*

   b. Si la restauration a réussi, appuyez sur `y` sur le nœud douteux, lorsque vous êtes invité à utiliser la copie restaurée ?

   c. Appuyez sur `y` lorsque vous voyez confirmer la réussite de la procédure de sauvegarde, puis appuyez sur `y` lorsque vous êtes invité à redémarrer le nœud.

   d. Vérifiez que les variables d'environnement sont définies comme prévu.

vi. Prenez le nœud vers l'invite DU CHARGEUR.

   À partir de l'invite ONTAP, vous pouvez lancer la commande system node halt -skip-lif-migration-before -shutdown true -ignore-quorum-avertissements true -Inhibit-Takeover-Takeover true.

vii. Vérifiez les paramètres de la variable d'environnement à l'aide de l' `printenv` commande.

viii. Si une variable d'environnement n'est pas définie comme prévu, modifiez-la avec le `setenv` *`environment-variable-name changed-value`* commande.

ix. Enregistrez vos modifications à l'aide du `savenv` commande.

x. Redémarrez le nœud.

a. Le nœud ayant redémarré et affichant le `Waiting for giveback…` message, effectuer un retour à partir du nœud en bon état :

Si votre système est en…	Alors…
Une paire haute disponibilité	Une fois que le nœud douteux affiche le `Waiting for giveback…` message, effectuer un retour à partir du nœud en bon état : i. Depuis le nœud sain : `storage failover giveback -ofnode partner_node_name` Le nœud défaillant reprend son stockage, termine son démarrage, puis redémarre et le nœud en bon état. Si le retour est vetoté, vous pouvez envisager d'ignorer les vetoes. "Gestion des paires HAUTE DISPONIBILITÉ" ii. Surveiller la progression de l'opération de rétablissement à l'aide du `storage failover show-giveback` commande. iii. Une fois l'opération de rétablissement terminée, vérifiez que la paire HA est saine et que le basculement est possible à l'aide du `storage failover show` commande. iv. Restaurez le rétablissement automatique si vous le avez désactivé à l'aide de la commande Storage Failover modify.

b. Quittez le niveau de privilège avancé sur le nœud en bon état.

Démarrer l'image de récupération : AFF A320

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

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 utiliser la configuration restaurée. f. 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`**.

Si votre système dispose de…	Alors…

Aucune connexion réseau et se trouve dans une configuration IP de MetroCluster	a. Appuyez sur `n` lorsque vous êtes invité à restaurer la configuration de sauvegarde.
	b. Redémarrez le système à l'invite du système.
	c. Attendez que les connexions de stockage iSCSI se connectent.
	
	Vous pouvez continuer après avoir afficher les messages suivants :
	
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	
	d. 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 nœud 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 Étapes de remplacement des supports après démarrage pour OKM, NSE et NVE
- 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 nœud partenaire. b. Vérifiez que le nœud cible est prêt pour un rétablissement à l'aide du `storage failover show` commande.

7. Connectez le câble de la console au nœud partenaire.
8. Renvoyer le nœud 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 nœud réparé et exécutez la `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.

Restaurez OKM, NSE et NVE selon les besoins : AFF A320

Une fois les variables d'environnement vérifiées, vous devez effectuer une procédure spécifique aux systèmes sur lesquels OKM (Onboard Key Manager), NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) sont activés.

1. Déterminez la section à utiliser pour restaurer vos configurations OKM, NSE ou NVE : si NSE ou NVE sont activés avec Onboard Key Manager, vous devez restaurer les paramètres que vous avez capturés au début de cette procédure.
   - Si NSE ou NVE sont activés et que le gestionnaire de clés intégré est activé, rendez-vous sur Restaurez NVE ou NSE lorsque le gestionnaire de clés intégré est activé.
   - Si NSE ou NVE sont activés pour ONTAP 9.6, rendez-vous sur le site Restaurez NSE/NVE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures.

Restaurez NVE ou NSE lorsque le gestionnaire de clés intégré est activé

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 DU CHARGEUR	Démarrer le contrôleur sur le menu de démarrage : `boot_ontap menu`
En attente de retour	a. Entrez `Ctrl-C` à l'invite b. Dans le message: Voulez-vous arrêter ce nœud plutôt que d'attendre [y/n] ? , entrez : `y` c. À l'invite DU CHARGEUR, entrez le `boot_ontap menu` commande.

4. Dans le menu de démarrage, entrez la commande masquée, `recover_onboard_keymanager` et répondre `y` à l'invite
5. Saisissez la phrase de passe du gestionnaire de clés intégré que vous avez obtenue du client au début de cette procédure.
6. Lorsque vous êtes invité à saisir les données de sauvegarde, collez les données de sauvegarde que vous avez saisies au début de cette procédure, lorsque vous y êtes invité. Coller la sortie de `security key-manager backup show` OU `security key-manager onboard show-backup` commande

> Les données sont issues de l'une ou l'autre `security key-manager backup show` ou `security key-manager onboard show-backup` commande.

Exemple de données de sauvegarde :


```
---------------------- COMMENCER LA SAUVEGARDE----------------------
TmV0QXBwIEtleSBCbG9AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAUAAUAAUAAUAAUAAAQAAUAAUAAUAAUAAUAAUAAUAA
UAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUA
AUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAU
AAUZUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUAAUAAUAAU
AAUAA . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

------------------------- FIN DE LA SAUVEGARDE------------------------
```


7. Dans le menu de démarrage, sélectionnez l'option démarrage normal.

   Le système démarre pour attendre l'invite de rétablissement…

8. Vérifiez que le contrôleur cible est prêt pour le rétablissement à l'aide du `storage failover show` commande.
9. Giveback uniquement le CFO rassemble avec le `storage failover giveback -fromnode local`

`-only-cfo-aggregates true` 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", attendre 5 minutes pour que les NVMEMs se synchronisent.
- 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.

10. Une fois le retour terminé, vérifiez l'état du basculement et du rétablissement à l'aide du `storage failover show` et ``storage failover show`commandes -giveback».

    Seuls les agrégats CFO (agrégats racine et agrégats de données de type CFO) seront indiqués.

11. Déplacez le câble de la console vers le contrôleur cible.
    a. Si vous utilisez ONTAP 9.6 ou une version ultérieure, exécutez la synchronisation intégrée du gestionnaire de clés de sécurité :
    b. Exécutez le `security key-manager onboard sync` puis entrez la phrase de passe lorsque vous y êtes invité.
    c. Entrez le `security key-manager key query` commande pour afficher une vue détaillée de toutes les clés stockées dans le gestionnaire de clés intégré et vérifier que `Restored` colonne = `yes/true` pour toutes les clés d'authentification.

       Si le `Restored` colonne = tout autre élément que `yes/true`, Contactez le support client.

    d. Attendez 10 minutes que la clé se synchronise sur l'ensemble du cluster.
12. Déplacez le câble de la console vers le contrôleur partenaire.
13. Renvoyer le contrôleur cible à l'aide du `storage failover giveback -fromnode local` commande.
14. Vérifier le statut de rétablissement, 3 minutes après la fin des rapports, à l'aide de `storage failover show` commande.

    Si le retour n'est pas effectué au bout de 20 minutes, contactez le support client.

15. 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.

16. Déplacer le câble de la console vers le contrôleur cible et exécuter le `version -v` Commande pour vérifier les versions de ONTAP.
17. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node`

`local -auto-giveback true` commande.

Restaurez NSE/NVE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures

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", attendre 5 minutes pour que les NVMEMs se synchronisent.
   - 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 le `security key-manager key query` pour vérifier que le `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.

Renvoyez la pièce défaillante en AFF A320 à NetApp

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.