Support de démarrage

Install and maintain

NetApp
September 06, 2024

Sommaire

Support de démarrage

Présentation du remplacement du support de démarrage - AFF A700s

Le support de démarrage principal stocke l'image de démarrage ONTAP que le système utilise lors du démarrage. Vous pouvez restaurer l'image du support de démarrage principal à l'aide de l'image ONTAP sur le support de démarrage secondaire ou, si nécessaire, à l'aide d'une clé USB.

Si le support d'amorçage secondaire a échoué ou s'il n'a pas le fichier image.tgz, vous devez restaurer le support d'amorçage principal à l'aide d'un lecteur flash USB. Le lecteur doit être formaté en FAT32 et avoir la quantité de stockage appropriée pour contenir le fichier image_xxx.tgz.

- Le processus de remplacement restaure le système de fichiers var du support de démarrage secondaire ou du lecteur flash USB vers le support de démarrage principal.
- 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 contrôleur approprié :
  - Le contrôleur *trouble* est le contrôleur sur lequel vous effectuez la maintenance.
  - Le contrôleur *Healthy* est le partenaire HA du contrôleur déficient.

Si vous devez remplacer le support de démarrage secondaire alors que le support de démarrage principal est installé et en bon état, contactez le support NetApp et mentionnez l'article de la "Comment remplacer le périphérique de démarrage secondaire d'un système AFF A700s" base de connaissances.

Vérifiez les clés de chiffrement intégrées - AFF A700s

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> n'est pas affiché dans la sortie de la commande et que le système exécute ONTAP 9.5, passer à Option 1 : vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.5 ou une version antérieure.
   - 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 Option 2 : vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.6 ou version ultérieure.
4. Si le contrôleur douteux est intégré à une configuration HA, désactivez le rétablissement automatique de l'état du contrôleur: `storage failover modify -node local -auto-giveback false` ou `storage failover modify -node local -auto-giveback-after-panic false`

Option 1 : vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.5 ou une version antérieure

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.

Étapes

1. Connectez le câble de la console au contrôleur pour facultés affaiblies.
2. Vérifier si NVE est configuré 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 ou non.

3. Vérifier si NSE est configuré : `storage encryption disk show`
   - Si le résultat de la commande affiche 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.
   - Si NVE et NSE ne sont pas configurés, vous pouvez arrêter le contrôleur défaillant.

Vérifiez la configuration NVE

Étapes

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager query`
   - Si le `Restored` s'affiche `yes` et tous les gestionnaires de clés s'affichent `available`, il est sûr d'arrêter le contrôleur défaillant.
   - Si le `Restored` colonne affiche tout autre élément que `yes`, ou si un gestionnaire de clés s'affiche `unavailable`, vous devez effectuer quelques étapes supplémentaires.
   - Si le message cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée, vous devez effectuer d'autres étapes supplémentaires.

2. Si le `Restored` colonne affichée autre que `yes`, ou si un gestionnaire de clés s'affiche `unavailable`:

   a. Récupérez et restaurez toutes les clés d'authentification et les ID de clé associés : `security key-manager restore -address *`

      Si la commande échoue, contactez le support NetApp.

   "mysupport.netapp.com"

   a. Vérifiez que le `Restored` s'affiche `yes` affichage de toutes les clés d'authentification et de tous les gestionnaires de clés `available`: `security key-manager query`

   b. Arrêtez le contrôleur défaillant.

3. Si vous avez vu le message, cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée, affichez les clés stockées dans le gestionnaire de clés intégré : `security key-manager key show -detail`

   a. Si le `Restored` s'affiche `yes` sauvegardez manuellement les informations de gestion intégrée des clés :

      - Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
      - Entrez la commande pour afficher les informations de sauvegarde OKM : `security key-manager backup show`
      - 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.
      - Revenir en mode admin: `set -priv admin`
      - Arrêtez le contrôleur défaillant.

   b. Si le `Restored` colonne affiche tout autre élément que `yes`:

      - Exécutez l'assistant d'installation du gestionnaire de clés : `security key-manager setup -node target/impaired node name`

        > Entrez la phrase secrète de gestion de clés intégrée du client à l'invite. Si la phrase de passe ne peut pas être fournie, contactez "mysupport.netapp.com"

      - Vérifiez que le `Restored` s'affiche `yes` pour toutes les clés d'authentification : `security key-manager key show -detail`
      - Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
      - Entrez la commande pour afficher les informations de sauvegarde OKM : `security key-manager backup show`
      - 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.
      - Revenir en mode admin: `set -priv admin`
      - Vous pouvez arrêter le contrôleur en toute sécurité.

Vérifiez la configuration NSE

Étapes

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager query`
   - Si le `Restored` s'affiche `yes` et tous les gestionnaires de clés s'affichent `available`, il est sûr d'arrêter le contrôleur défaillant.
   - Si le `Restored` colonne affiche tout autre élément que `yes`, ou si un gestionnaire de clés s'affiche `unavailable`, vous devez effectuer quelques étapes supplémentaires.
   - Si le message cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée, vous devez effectuer d'autres étapes supplémentaires
2. Si le `Restored` colonne affichée autre que `yes`, ou si un gestionnaire de clés s'affiche `unavailable`:

   a. Récupérez et restaurez toutes les clés d'authentification et les ID de clé associés : `security key-manager restore -address *`

      Si la commande échoue, contactez le support NetApp.

   "mysupport.netapp.com"

   a. Vérifiez que le `Restored` s'affiche `yes` affichage de toutes les clés d'authentification et de tous les gestionnaires de clés `available`: `security key-manager query`

   b. Arrêtez le contrôleur défaillant.
3. Si vous avez vu le message, cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée, affichez les clés stockées dans le gestionnaire de clés intégré : `security key-manager key show -detail`

   a. Si le `Restored` s'affiche `yes`, sauvegardez manuellement les informations de gestion des clés intégrées :
      - Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
      - Entrez la commande pour afficher les informations de sauvegarde OKM : `security key-manager backup show`
      - 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.
      - Revenir en mode admin: `set -priv admin`
      - Arrêtez le contrôleur défaillant.

   b. Si le `Restored` colonne affiche tout autre élément que `yes`:
      - Exécutez l'assistant d'installation du gestionnaire de clés : `security key-manager setup -node target/impaired node name`

        > Entrez la phrase de passe OKM du client à l'invite. Si la phrase de passe ne peut pas être fournie, contactez "mysupport.netapp.com"

      - Vérifiez que le `Restored` affiche la colonne `yes` pour toutes les clés d'authentification : `security`

`key-manager key show -detail`

- Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
- Entrez la commande pour sauvegarder les informations OKM : `security key-manager backup show`

> Assurez-vous que les informations OKM sont enregistrées dans votre fichier journal. Ces informations seront nécessaires dans les scénarios d'incident pour lesquels OKM peut avoir besoin d'être restauré manuellement.

- Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.
- Revenir en mode admin: `set -priv admin`
- Vous pouvez arrêter le contrôleur en toute sécurité.

Option 2 : vérifiez NVE ou NSE sur les systèmes qui exécutent ONTAP 9.6 ou version ultérieure

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 - AFF A700s

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

Étapes

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

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

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

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

Remplacez le support de démarrage - AFF A700s

Vous devez retirer le module de contrôleur du châssis, l'ouvrir, puis remplacer le support de démarrage défectueux.

Étape 1 : retirer le module de contrôleur

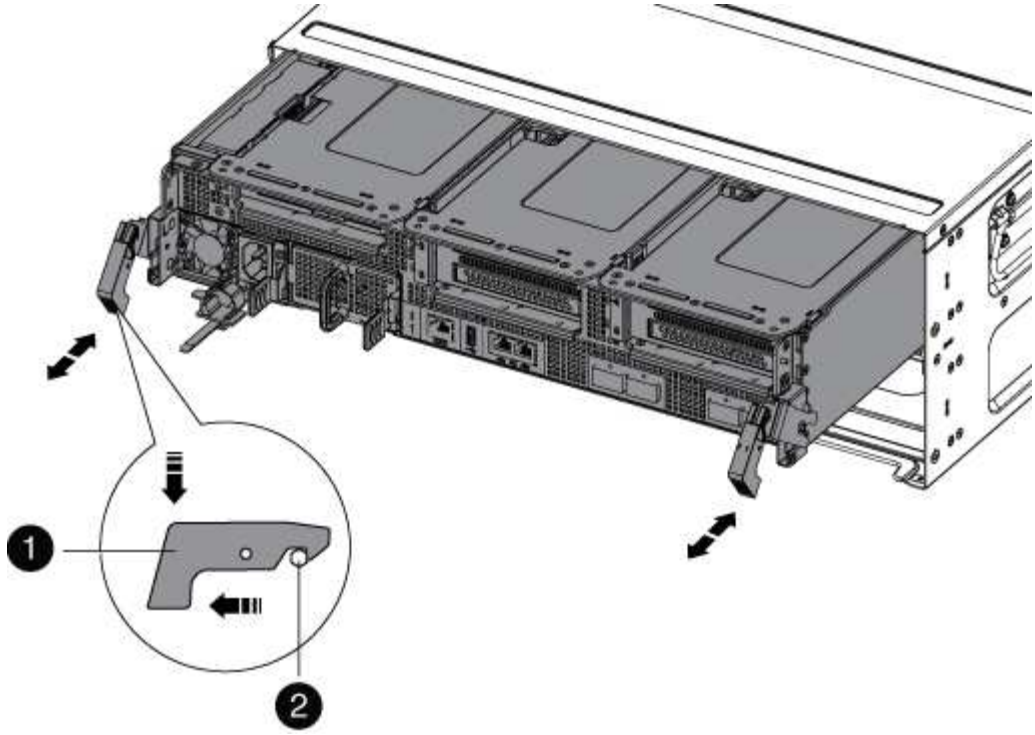
Vous devez retirer le module de contrôleur du châssis lorsque vous remplacez le module de contrôleur ou remplacez un composant dans le module de contrôleur.

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

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

3. Débranchez l'alimentation du module de contrôleur de la source, puis débranchez le câble du bloc d'alimentation.
4. Retirez le périphérique de gestion des câbles du module de contrôleur et mettez-le de côté.
5. Appuyez sur les deux loquets de verrouillage, puis faites pivoter les deux loquets vers le bas en même temps.

   Le module de contrôleur se déplace légèrement hors du châssis.

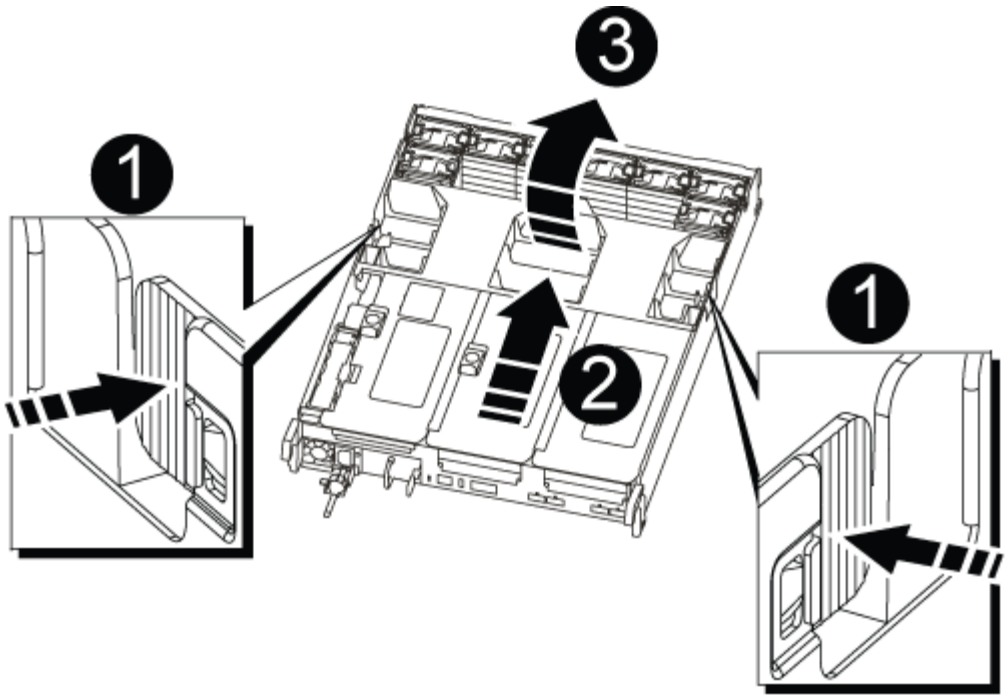


1	Loquet de verrouillage
2	Goupille de blocage

1. Faites glisser le module de contrôleur hors du châssis.

   Assurez-vous de prendre en charge la partie inférieure du module de contrôleur lorsque vous le faites glisser hors du châssis.

2. Placez le module de commande sur une surface plane et stable, puis ouvrez la conduite d'air :
   a. Appuyer sur les languettes de verrouillage situées sur les côtés du conduit d'air vers le milieu du module de contrôleur.
   b. Faites glisser le conduit d'air vers les modules de ventilateur, puis tournez-le vers le haut jusqu'à sa position complètement ouverte.



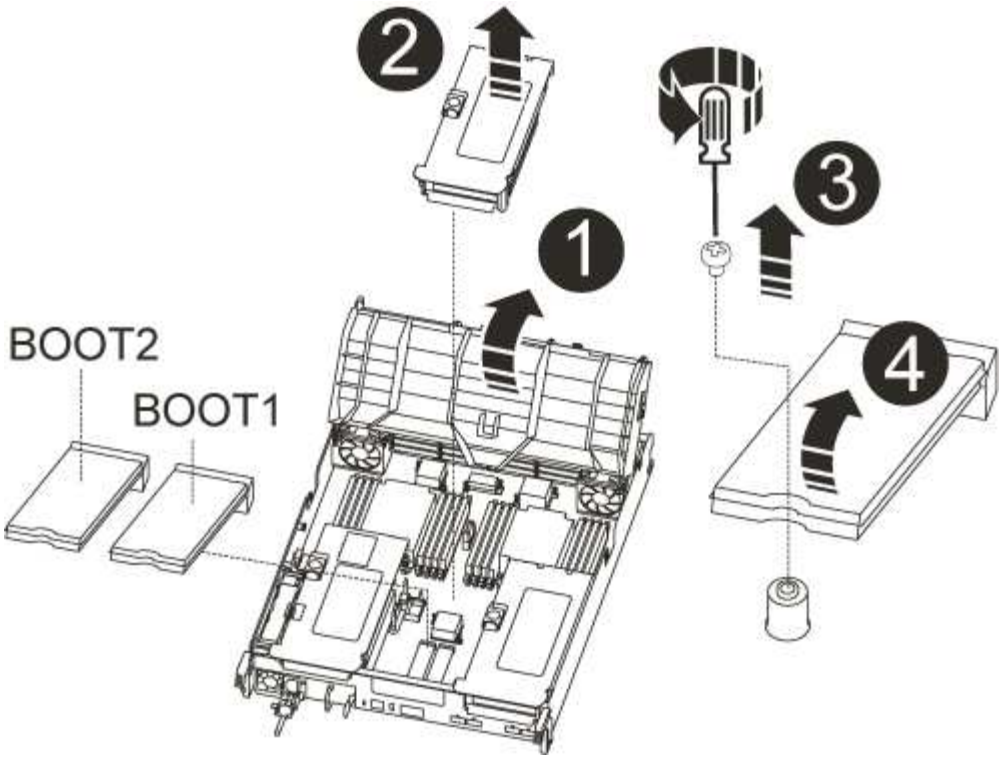
1	Pattes de verrouillage du conduit d'air
2	Redresseurs
3	Conduit d'air

Étape 2 : remplacer le support de démarrage - AFF A700s

Vous devez localiser le support de démarrage défectueux dans le module de contrôleur en retirant le module PCIe central du module de contrôleur, en localisant le support de démarrage défectueux, puis en remplaçant le support de démarrage.

Vous avez besoin d'un tournevis cruciforme pour retirer la vis qui maintient le support de démarrage en place.

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Recherchez le support de démarrage :
   a. Ouvrir le conduit d'air, si nécessaire.
   b. Si nécessaire, retirez la carte de montage 2, le module PCIe central, en déverrouillant le loquet de verrouillage, puis en retirant la carte de montage du module de contrôleur.



1	Conduit d'air
2	Carte de montage 2 (module PCIe central)
3	Vis du support de démarrage
4	Support de démarrage

3. Recherchez le support de démarrage ayant échoué.
4. Retirez le support de démarrage du module de contrôleur :
   a. À l'aide d'un tournevis cruciforme n° 1, retirez la vis qui maintient le support de démarrage et mettez la vis de côté en lieu sûr.
   b. Saisissez les côtés du support de coffre, faites pivoter doucement le support de coffre vers le haut, puis tirez le support de coffre hors du support et mettez-le de côté.
5. Alignez les bords du support de démarrage de remplacement avec le support de démarrage, puis poussez-le doucement dans le support.
6. 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.

7. Faites pivoter le support de démarrage vers le bas jusqu'à ce qu'il soit aligné sur la carte mère.
8. Fixez le support de démarrage à l'aide de la vis.

Ne serrez pas trop la vis. Cela pourrait fissurer la carte de circuit du support de démarrage.

9. Réinstallez la carte de montage dans le module de contrôleur.
10. Fermer le conduit d'air :
    a. Faire pivoter le conduit d'air vers le bas.
    b. Faites glisser le conduit d'air vers les surmontoirs jusqu'à ce qu'il s'enclenche.

Transférez l'image de démarrage vers le support de démarrage - AFF A700s

Vous pouvez installer l'image système sur le support de démarrage de remplacement à l'aide de l'image sur le second support de démarrage installé dans le module de contrôleur, la méthode principale de restauration de l'image système, Ou en transférant l'image de démarrage vers le support de démarrage à l'aide d'un lecteur flash USB lorsque le support de démarrage secondaire a échoué ou si le fichier image.tgz est introuvable sur le support de démarrage secondaire.

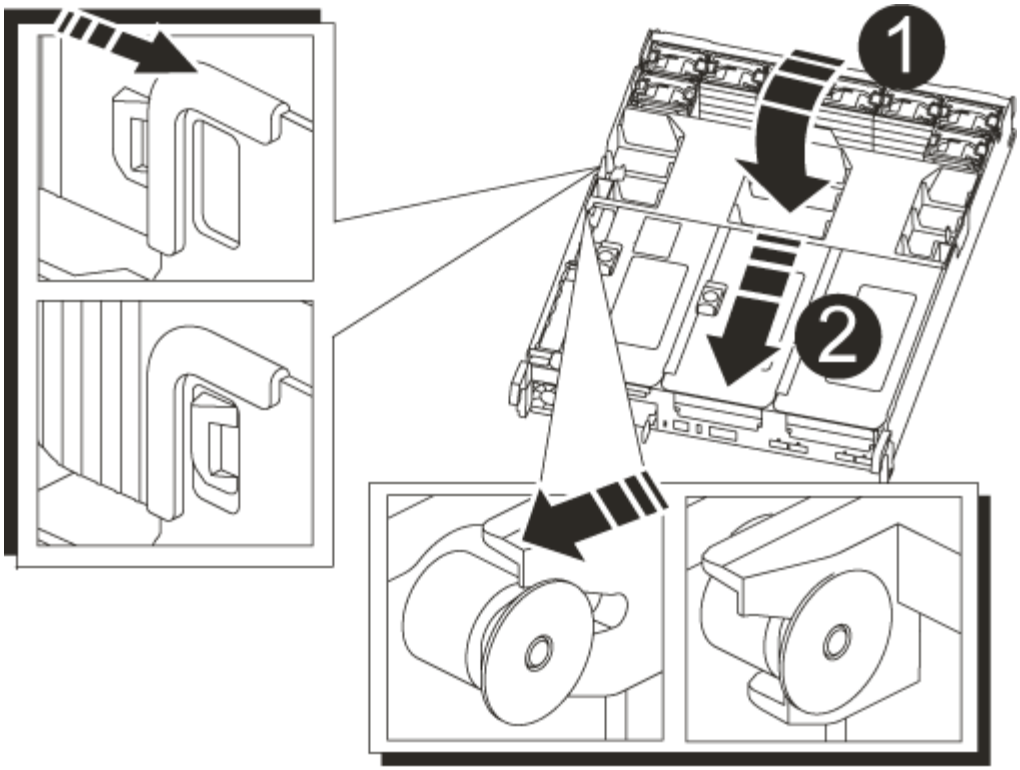
Option 1 : transférez des fichiers vers le support de démarrage à l'aide de la récupération de sauvegarde à partir du second support de démarrage

Vous pouvez installer l'image système sur le support de démarrage de remplacement à l'aide de l'image sur le second support de démarrage installé dans le module de contrôleur. Il s'agit de la méthode principale pour transférer les fichiers de support d'amorçage vers le support d'amorçage de remplacement des systèmes avec deux supports d'amorçage dans le module de contrôleur.

L'image du support de démarrage secondaire doit contenir un `image.tgz` fichier et ne doit pas être signalant des échecs. Si le fichier image.tgz est manquant ou si le support de démarrage signale des échecs, vous ne pouvez pas suivre cette procédure. Vous devez transférer l'image d'amorçage sur le support de démarrage de remplacement en suivant la procédure de remplacement du lecteur flash USB.

Étapes

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Si ce n'est déjà fait, fermer le conduit d'air :
    a. Faire basculer la conduite d'air complètement vers le bas jusqu'au module de commande.
    b. Faites glisser la conduite d'air vers les surmontoirs jusqu'à ce que les pattes de verrouillage s'enclenchent.
    c. Inspecter le conduit d'air pour s'assurer qu'il est correctement installé et verrouillé en place.



1	
Conduit d’air	
2	
Redresseurs	

3. 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.
4. Réinstallez le périphérique de gestion des câbles et recâblage du système, selon les besoins.

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

5. Recâblage du bloc d’alimentation, puis connexion à la source d’alimentation.

   Vérifiez que vous refixez le collier de verrouillage du câble d’alimentation sur le cordon d’alimentation.

6. Poussez doucement le module de contrôleur complètement dans le système jusqu’à ce que les crochets de verrouillage du module de contrôleur commencent à se lever, appuyez fermement sur les crochets de verrouillage pour terminer d’asseoir le module de contrôleur, puis faites pivoter les crochets de verrouillage dans la position verrouillée par-dessus les broches du module de contrôleur.

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

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

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.

8. Dans l'invite DU CHARGEUR, démarrez l'image de restauration à partir du support de démarrage secondaire : `boot_recovery`

   L'image est téléchargée à partir du support de démarrage secondaire.

9. Lorsque vous y êtes invité, entrez le nom de l'image ou acceptez l'image par défaut affichée entre crochets sur votre écran.
10. Une fois l'image installée, démarrez le processus de restauration :
    a. Notez l'adresse IP du contrôleur affecté qui s'affiche à l'écran.
    b. Appuyez sur `y` lorsque vous êtes invité à restaurer la configuration de sauvegarde.
    c. Appuyez sur `y` lorsque vous êtes invité à confirmer que la procédure de sauvegarde a réussi.
11. À partir du contrôleur 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`*
12. Une fois la synchronisation de la configuration terminée sans erreur, appuyez sur `y` lorsque vous êtes invité à confirmer que la procédure de sauvegarde a réussi.
13. Appuyez sur `y` lorsque vous êtes invité à utiliser la copie restaurée, puis à appuyer sur `y` lorsque vous êtes invité à redémarrer le contrôleur.
14. Quittez le niveau de privilège avancé sur le contrôleur en bon état.

Option 2 : transférez l'image d'amorçage sur le support d'amorçage à l'aide d'une clé USB

Cette procédure ne doit être utilisée que si la restauration du support de démarrage secondaire a échoué ou si le fichier image.tgz est introuvable sur le support de démarrage secondaire.

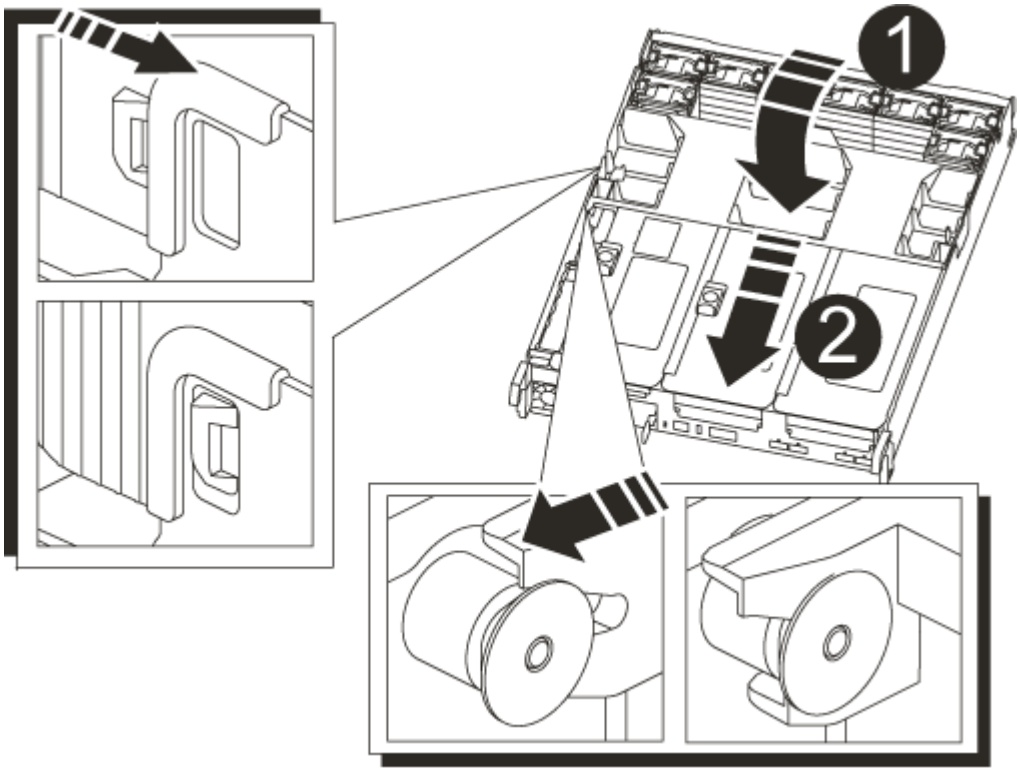
- Vous devez disposer d'une clé USB, formatée en FAT32, avec au moins 4 Go de capacité.
- Copie de la même version d'image de ONTAP que celle du contrôleur avec facultés affaiblies. Vous pouvez télécharger l'image appropriée depuis la section Downloads du site de support NetApp
  - Si NVE est activé,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

Étapes

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Si ce n'est déjà fait, fermer le conduit d'air :
   a. Faire basculer la conduite d'air complètement vers le bas jusqu'au module de commande.
   b. Faites glisser la conduite d'air vers les surmontoirs jusqu'à ce que les pattes de verrouillage

s'enclenchent.

c. Inspecter le conduit d'air pour s'assurer qu'il est correctement installé et verrouillé en place.



1	
Conduit d'air	
2	
Redresseurs	

3. 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.
4. Réinstallez le périphérique de gestion des câbles et recâblage du système, selon les besoins.

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

5. Recâblage du bloc d'alimentation, puis connexion à la source d'alimentation.

   Vérifiez que vous refixez le collier de verrouillage du câble d'alimentation sur le cordon d'alimentation.

6. 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.

7. Poussez doucement le module de contrôleur complètement dans le système jusqu'à ce que les crochets de verrouillage du module de contrôleur commencent à se lever, appuyez fermement sur les crochets de verrouillage pour terminer d'asseoir le module de contrôleur, puis faites pivoter les crochets de verrouillage dans la position verrouillée par-dessus les broches du module de contrôleur.

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

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

   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.

9. Bien que les variables d'environnement et les bootargs soient conservés, vous devez vérifier que toutes les variables d'environnement d'amorçage et les bootargs requis sont correctement définis pour votre type de système et votre configuration à l'aide de l' `printenv bootarg name` commande et corriger les erreurs à l'aide du `setenv variable-name <value>` commande.

   a. Vérifier les variables d'environnement de boot:

      - `bootarg.init.boot_clustered`
      - `partner-sysid`
      - `bootarg.init.flash_optimized` Pour AFF C190/AFF A220 (FAS 100 % Flash)
      - `bootarg.init.san_optimized` Pour les baies SAN AFF A220 et 100 % Flash
      - `bootarg.init.switchless_cluster.enable`

   b. Si le gestionnaire de clés externe est activé, vérifiez les valeurs d'amorçage répertoriées dans le `kenv` Sortie ASUP :

      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `kmip.init.interface <value>`
      - `kmip.init.ipaddr <value>`
      - `kmip.init.netmask <value>`
      - `kmip.init.gateway <value>`

   c. Si Onboard Key Manager est activé, vérifiez les valeurs de démarrage, répertoriées dans le `kenv` Sortie ASUP :

      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `bootarg.onboard_keymanager <value>`

   d. Enregistrez les variables d'environnement que vous avez modifiées à l'aide de la `savenv` commande

   e. Confirmez vos modifications à l'aide du `printenv *variable-name*` commande.

10. 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.

11. Lorsque vous y êtes invité, entrez le nom de l'image ou acceptez l'image par défaut affichée entre crochets sur votre écran.
12. Une fois l'image installée, démarrez le processus de restauration :
    a. Notez l'adresse IP du contrôleur affecté qui s'affiche à l'écran.
    b. Appuyez sur `y` lorsque vous êtes invité à restaurer la configuration de sauvegarde.
    c. Appuyez sur `y` lorsque vous êtes invité à confirmer que la procédure de sauvegarde a réussi.
13. Appuyez sur `y` lorsque vous êtes invité à utiliser la copie restaurée, puis à appuyer sur `y` lorsque vous êtes invité à redémarrer le contrôleur.
14. À partir du contrôleur 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`*
15. Une fois la synchronisation de la configuration terminée sans erreur, appuyez sur `y` lorsque vous êtes invité à confirmer que la procédure de sauvegarde a réussi.
16. Appuyez sur `y` lorsque vous êtes invité à utiliser la copie restaurée, puis à appuyer sur `y` lorsque vous êtes invité à redémarrer le contrôleur.
17. Vérifiez que les variables d'environnement sont définies comme prévu.
    a. Prenez le contrôleur vers l'invite DU CHARGEUR.

       À 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 ».

    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.
    e. Redémarre le contrôleur.
18. Le contrôleur ayant redémarré affiche le `Waiting for giveback…` message, effectuer un retour à partir du contrôleur en bon état :

Si votre système est en…	Alors…
Une paire haute disponibilité	Une fois que le contrôleur affecté affiche le `Waiting for giveback…` message, effectuer un retour à partir du contrôleur en bon état : a. Depuis le contrôleur sain : `storage failover giveback -ofnode partner_node_name` Le contrôleur affecté revient son stockage, termine son démarrage, puis redémarre et le contrôleur en bon état prend à nouveau le relais. Si le retour est vetoté, vous pouvez envisager d'ignorer les vetoes. "Gestion des paires HAUTE DISPONIBILITÉ" b. Surveiller la progression de l'opération de rétablissement à l'aide du `storage failover show-giveback` commande. c. 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. d. Restaurez le retour automatique si vous le désactivez à l'aide du `storage failover modify` commande.

19. Quittez le niveau de privilège avancé sur le contrôleur en bon état.

Démarrage de l'image de récupération - AFF A700s

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 contrôleur sain sur le niveau de privilège avancé : `set -privilege advanced` c. Exécutez la commande restore backup : `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Renvoyer le contrôleur au niveau admin : `set -privilege admin` e. Appuyez sur `y` lorsque vous êtes invité à utiliser la configuration restaurée. f. Appuyez sur `y` lorsque vous êtes invité à redémarrer le contrôleur.
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.

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

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

   Si l'une des interfaces est indiquée comme « FALSE », restaurez ces interfaces à son port d'origine à l'aide de l' `net int revert` commande.

10. Déplacez le câble de la console vers le contrôleur réparé et exécutez le `version -v` Commande pour vérifier les versions de ONTAP.
11. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

OKM, NSE et NVE si besoin : AFF A700s

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.

Déterminez la section à laquelle vous devez utiliser pour restaurer vos configurations OKM, NSE ou NVE :

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.

- Si NSE ou NVE sont activés et que le gestionnaire de clés intégré est activé, rendez-vous sur Option 1 : restaurez NVE ou NSE lorsque le gestionnaire de clés intégré est activé.
- Si NSE ou NVE sont activés pour ONATP 9.5, rendez-vous sur Option 2 : restaurez NSE/NVE sur les systèmes exécutant ONTAP 9.5 et versions antérieures.
- Si NSE ou NVE sont activés pour ONTAP 9.6, rendez-vous sur le site Option 3 : restaurez NSE/NVE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures.

Option 1 : 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`

Si la console affiche…	Alors…
Attente du retour…	a. Entrez `Ctrl-C` à l’invite b. Au message: Voulez-vous arrêter ce contrôleur 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-----------------------
   TmV0QXBwIEtleSBCbG9AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAUAAUAAUAAUAAUAAAQAAUAAUAAUAAUAAUAAUAA
   UAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUA
   AUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAU
   AAUZUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUAAUAAU
   AAUAA . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

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

   Le système démarre à `Waiting for giveback…` à l’invite.

8. Déplacez le câble de la console vers le contrôleur partenaire et connectez-vous en tant qu’administrateur.
9. Vérifiez que le contrôleur cible est prêt pour le rétablissement à l’aide du `storage failover show` commande.
10. Renvoyer uniquement les agrégats CFO avec le rétablissement du basculement du stockage `-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, 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.

11. 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.

12. Déplacez le câble de la console vers le contrôleur cible.
13. Si vous exécutez ONTAP 9.5 ou une version antérieure, exécutez l'assistant de configuration du gestionnaire de clés :
    a. Démarrez l'assistant à l'aide de `security key-manager setup -nodenodename` entrez la phrase d'authentification pour la gestion intégrée des clés lorsque vous y êtes invité.
    b. Entrez le `key-manager key show -detail` commande pour afficher une vue détaillée de toutes les clés stockées dans le gestionnaire de clés intégré et vérifier que `Restored` colonne = `yes` pour toutes les clés d'authentification.

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

    c. Attendez 10 minutes que la clé se synchronise sur l'ensemble du cluster.
14. Si vous exécutez ONTAP 9.6 ou version ultérieure :
    a. Exécutez le `security key-manager onboard sync` puis entrez la phrase de passe lorsque vous y êtes invité.
    b. 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.

    c. Attendez 10 minutes que la clé se synchronise sur l'ensemble du cluster.
15. Déplacez le câble de la console vers le contrôleur partenaire.
16. Renvoyer le contrôleur cible à l'aide du `storage failover giveback -fromnode local` commande.
17. 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.

18. 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.

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

Option 2 : restaurez NSE/NVE sur les systèmes exécutant ONTAP 9.5 et versions antérieures

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. Déplacez le câble de la console vers le contrôleur cible et exécutez la version `-v command` Pour vérifier les versions 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.

> Cette commande ne fonctionne pas si NVE (NetApp Volume Encryption) est configuré

10. Utilisez la requête Security Key-Manager pour afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés.
    - Si le `Restored` colonne = `yes` Et tous les gestionnaires clés rapportent un état disponible, allez à *compléter le processus de remplacement*.
    - Si le `Restored` colonne = tout autre élément que `yes`, et/ou un ou plusieurs gestionnaires de clés ne sont pas disponibles, utilisez le `security key-manager restore -address` Commande permettant de récupérer et de restaurer toutes les clés d'authentification (ACK) et tous les ID de clé associés à tous les nœuds à partir de tous les serveurs de gestion de clés disponibles.

      Vérifiez à nouveau la sortie de la requête du gestionnaire de clés de sécurité pour vous assurer que `Restored` colonne = `yes` et tous les responsables clés se déclarent dans un état disponible
11. Si la gestion intégrée des clés est activée :
    a. Utilisez le `security key-manager key show -detail` pour obtenir une vue détaillée de toutes les clés stockées dans le gestionnaire de clés intégré.
    b. Utilisez le `security key-manager key show -detail` et vérifiez que le `Restored` colonne = `yes` pour toutes les clés d'authentification.

       Si le `Restored` colonne = tout autre élément que `yes`, utilisez l' `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* Commande permettant de restaurer les paramètres de gestion intégrée des clés. Exécutez à nouveau le `security key-manager key show -detail` commande à vérifier `Restored` colonne = `yes` pour toutes les clés d'authentification.
12. Branchez le câble de la console au contrôleur partenaire.
13. Reaccordez le contrôleur à l'aide du `storage failover giveback -fromnode local` commande.
14. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

Option 3 : 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.

Si la console affiche…	Alors…
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. Si AutoSupport est activé, restaurez/annulez la suppression automatique de la création de cas à l'aide du `system node autosupport invoke -node * -type all -message MAINT=END`

Renvoyez la pièce défectueuse à NetApp - AFF A700s

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.