Support de démarrage

Install and maintain

NetApp
September 06, 2024

Sommaire

Support de démarrage

Présentation du remplacement des supports de démarrage - FAS9000

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`.

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 ne requiert pas de connexion à un réseau pour restaurer le `var` système de fichiers. La paire HA dans un châssis unique dispose d'une connexion e0S interne, qui est utilisée pour le transfert `var` une configuration entre eux.
  - 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

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 nœud douteux est partie d'une configuration HA, désactivez le rétablissement automatique du nœud en bon état : `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 défectueux - FAS9000

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 contrôleur est dans un MetroCluster

Une fois les tâches NVE ou NSE effectuées, vous devez arrêter le nœud douteux. REMARQUE : 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`.

Option 3 : le contrôleur est intégré à un MetroCluster à deux nœuds

Une fois les tâches NVE ou NSE effectuées, vous devez arrêter le nœud douteux.

> 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 - FAS9000

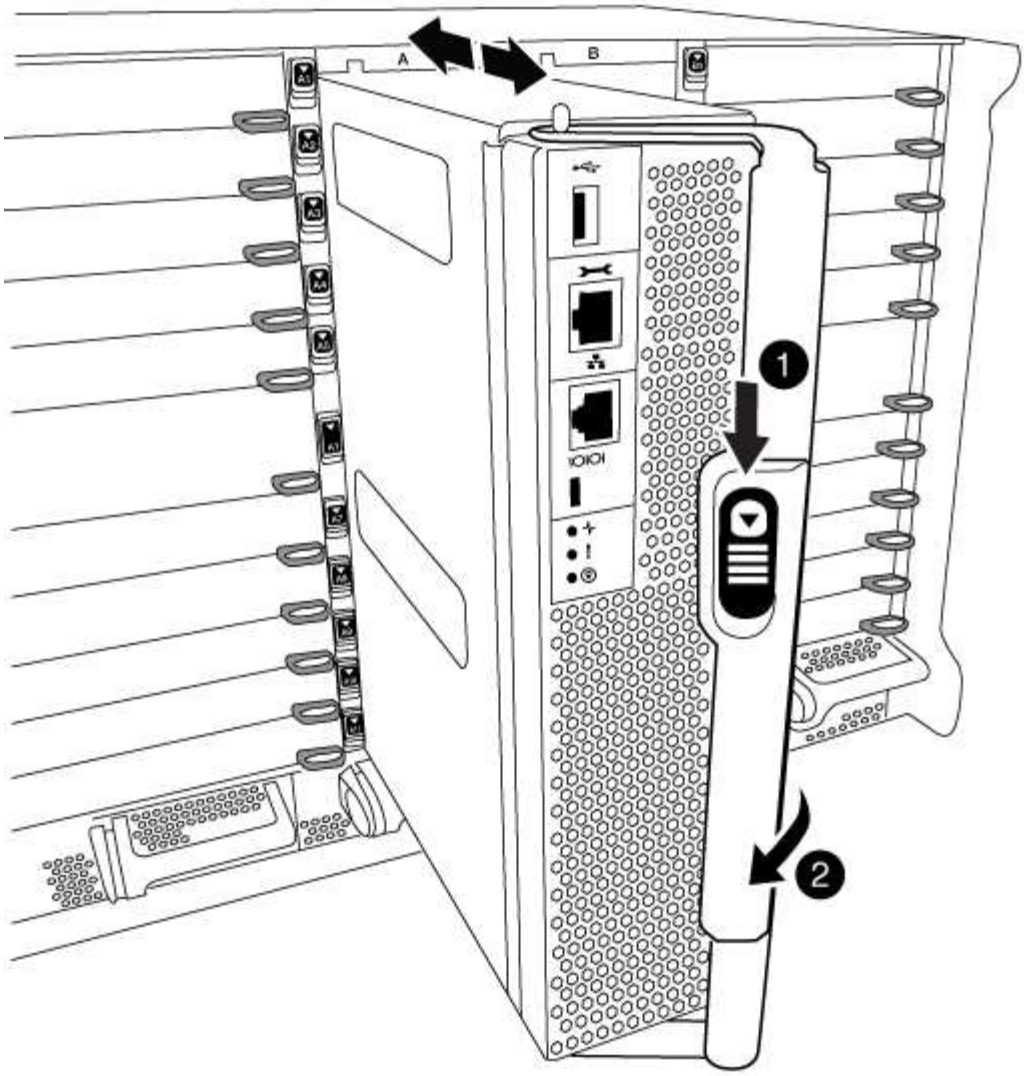
Pour remplacer le support de démarrage, vous devez retirer le module de contrôleur endommagé, installer le support de démarrage de remplacement et transférer l'image de démarrage sur une clé USB.

Étape 1 : retirer le contrôleur

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

Étapes

1. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Débranchez les câbles du module de contrôleur défaillant et suivez l'emplacement de connexion des câbles.
3. Faites glisser le bouton orange sur la poignée de came vers le bas jusqu'à ce qu'il se déverrouille.

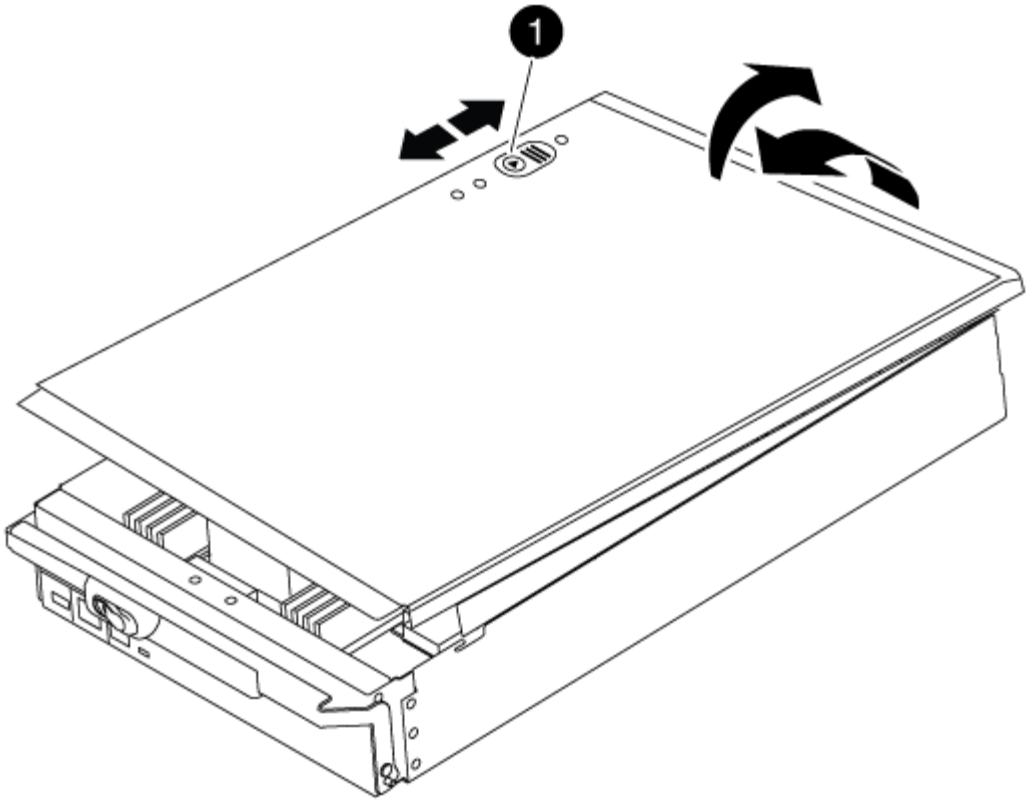


1	
Bouton de déverrouillage de la poignée de came	
2	
Poignée de came	

4. Faites pivoter la poignée de came de façon à ce qu'elle désengage complètement le module de contrôleur du châssis, puis 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.

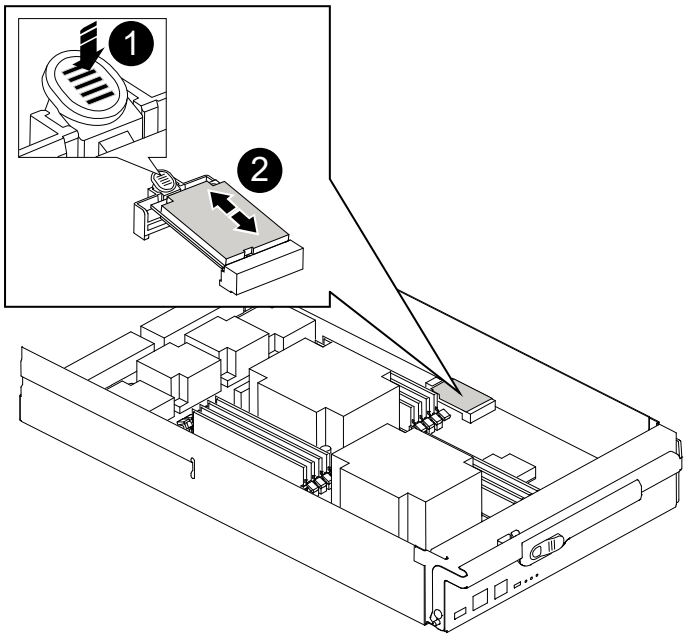
5. Placez le couvercle du module de contrôleur face vers le haut sur une surface stable et plane, appuyez sur le bouton bleu du capot, faites glisser le couvercle vers l'arrière du module de contrôleur, puis faites pivoter le couvercle vers le haut et retirez-le du module de contrôleur.



1	
Bouton de verrouillage du couvercle du module de commande	

Étape 2 : remplacer le support de démarrage

Recherchez le support de démarrage à l'aide de l'illustration suivante ou du mappage des FRU sur le module de contrôleur :



1	
Appuyez sur la languette de dégagement	
2	
Support de démarrage	

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

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

2. Alignez les bords du support de démarrage de remplacement avec le support de démarrage, puis poussez-le doucement dans le support.
3. 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.

4. Poussez le support de démarrage vers le bas pour engager le bouton de verrouillage sur le boîtier du support de démarrage.
5. Réinstallez le couvercle du module de contrôleur en alignant les broches du couvercle avec les fentes du support de carte mère, puis faites glisser le couvercle pour le mettre en place.

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

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

cette procédure.

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

Étapes

1. Alignez l'extrémité du module de contrôleur avec l'ouverture du châssis, puis poussez doucement le module de contrôleur à mi-course dans le système.
2. Recâblage du module de contrôleur, selon les besoins.
3. Insérez la clé USB dans le logement USB du module de contrôleur.

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

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

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

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

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

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

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

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

   - Si vous configurez des connexions manuelles : `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - Filer_addr est l'adresse IP du système de stockage.
     - Le masque de réseau est le masque de réseau du réseau de gestion connecté au partenaire haute disponibilité.
     - passerelle est la passerelle du réseau.

- dns_addr est l'adresse IP d'un serveur de noms sur votre réseau.
- dns_Domain est le nom de domaine DNS (Domain Name System).

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

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

7. Si le contrôleur est en mode MetroCluster Stretch ou Fabric-Attached, vous devez restaurer la configuration de l'adaptateur FC :

   a. Démarrage en mode maintenance : `boot_ontap maint`

   b. Définissez les ports MetroCluster comme initiateurs : `ucadmin modify -m fc -t` *`initiator adapter_name`*

   c. Arrêter pour revenir en mode maintenance : `halt`

   Les modifications seront mises en œuvre au démarrage du système.

Démarrez l'image de restauration - FAS9000

La procédure de démarrage du nœud douteux à partir de l'image de récupération dépend de si le système se trouve dans une configuration MetroCluster à deux nœuds.

Option 1 : démarrez l'image de récupération dans la plupart des systèmes

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

Cette procédure s'applique aux systèmes qui ne se trouvent pas dans une configuration MetroCluster à deux nœuds.

Étapes

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

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

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

3. Restaurez le `var` système de fichiers :

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 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…	Puis…*
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.

Option 2 : démarrez l'image de restauration dans une configuration MetroCluster à deux nœuds

Vous devez démarrer l'image ONTAP à partir du lecteur USB et vérifier les variables environnementales.

Cette procédure s'applique aux systèmes dotés d'une configuration MetroCluster à deux nœuds.

Étapes

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

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

2. Lorsque vous y êtes invité, entrez le nom de l'image ou acceptez l'image par défaut affichée entre crochets sur votre écran.
3. Une fois l'image installée, démarrez le processus de restauration :
   a. Appuyez sur `n` lorsque vous êtes invité à restaurer la configuration de sauvegarde.
   b. Appuyez sur `y` lorsque vous êtes invité à redémarrer le système pour commencer à utiliser le nouveau logiciel installé.

      Vous devez être prêt à interrompre le processus d'amorçage lorsque vous y êtes invité.

4. Lorsque le système démarre, appuyez sur `Ctrl-C` après que vous ayez vu le `Press Ctrl-C for Boot Menu` Message. Et lorsque le menu de démarrage est affiché, sélectionnez l'option 6.
5. Vérifiez que les variables d'environnement 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.
   e. Redémarrez le nœud.

Basculez les agrégats dans une configuration MetroCluster à deux nœuds - FAS9000

Après avoir terminé le remplacement des unités remplaçables sur site dans une configuration MetroCluster à deux nœuds, vous pouvez exécuter l'opération de rétablissement MetroCluster. Cette configuration renvoie la configuration à son état de fonctionnement normal, avec les SVM (Storage Virtual machines) source et sur le site précédemment douteux actifs et peuvent accéder aux données des pools de disques locaux.

Cette tâche s'applique uniquement aux configurations MetroCluster à deux nœuds.

Étapes

1. Vérifiez que tous les nœuds sont dans le `enabled` état : `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Vérifier que la resynchronisation est terminée sur tous les SVM : `metrocluster vserver show`
3. Vérifier que toutes les migrations LIF automatiques effectuées par les opérations de correction ont été effectuées correctement : `metrocluster check lif show`
4. Effectuez le rétablissement en utilisant le `metrocluster switchback` utilisez une commande à partir

d'un nœud du cluster survivant.

5. Vérifiez que l'opération de rétablissement est terminée : `metrocluster show`

   L'opération de rétablissement s'exécute toujours lorsqu'un cluster est dans `waiting-for-switchback` état :

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   Le rétablissement est terminé une fois les clusters dans `normal` état :

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   Si un rétablissement prend beaucoup de temps, vous pouvez vérifier l'état des lignes de base en cours en utilisant le `metrocluster config-replication resync-status show` commande.

6. Rétablir toutes les configurations SnapMirror ou SnapVault.

Restaurez OKM, NSE et NVE selon les besoins - FAS9000

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`
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-----------------------
TmV0QXBwIEtleSBCbG9AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAUAAUAAUAAUAAAQAAUAAUAAUAAUAAUAAUAA
UAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUA
AUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAU
AAUZUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUZUAAUAAUAAUAAUAAUAAUAAUAAU
AAUAA . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

------------------------- 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.
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 - FAS9000

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.