



Support de démarrage

Install and maintain

NetApp
January 10, 2025

Sommaire

- Support de démarrage 1
 - Procédure de remplacement du support de démarrage - AFF C80 1
 - Configuration requise pour le remplacement des supports de démarrage - AFF C80 1
 - Vérifiez la prise en charge et l'état de la clé de cryptage - AFF C80 2
 - Arrêter le contrôleur défectueux - AFF C80 5
 - Remplacez le support de démarrage - AFF C80 7
 - Démarrez l'image de récupération - AFF C80 11
 - Restaurer le chiffrement - AFF C80 13
 - Renvoyez la pièce défectueuse à NetApp - AFF C80 23

Support de démarrage

Procédure de remplacement du support de démarrage - AFF C80

Procédez comme suit pour remplacer votre support de démarrage.

1

"Vérifiez la configuration requise pour le support de démarrage"

Consultez les conditions requises pour le remplacement du support de démarrage.

2

"Vérifiez la prise en charge et l'état de la clé de cryptage"

Vérifiez si le gestionnaire de clés de sécurité est activé sur le système ou si des disques cryptés sont présents.

3

"Arrêtez le contrôleur défaillant"

Arrêtez ou prenez le contrôle du contrôleur défaillant pour que le contrôleur fonctionnel continue à transmettre des données à partir du stockage du contrôleur défaillant.

4

"Remplacez le support de démarrage"

Retirez le support de démarrage défectueux du module de gestion du système, installez le support de démarrage de remplacement, puis transférez une image ONTAP à l'aide d'une clé USB.

5

"Démarez l'image de récupération"

Démarez l'image ONTAP à partir du lecteur USB, restaurez le système de fichiers et vérifiez les variables d'environnement.

6

"Restaurez le chiffrement"

Restaurez la configuration du gestionnaire de clés intégré ou le gestionnaire de clés externe à partir du menu d'amorçage ONAT.

7

"Renvoyez la pièce défectueuse à NetApp"

Retournez la pièce défectueuse à NetApp, tel que décrit dans les instructions RMA (retour de matériel) fournies avec le kit.

Configuration requise pour le remplacement des supports de démarrage - AFF C80

Avant de remplacer le support de démarrage, vérifiez les conditions suivantes.

- Vous devez disposer d'une clé USB, formatée en FAT32, avec la quantité de stockage appropriée pour maintenir le `image_XXX.tgz` fichier.
- Vous devez copier le `image_XXX.tgz` fichier sur la clé USB pour pouvoir l'utiliser ultérieurement dans cette procédure.
- 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.

Vérifiez la prise en charge et l'état de la clé de cryptage - AFF C80

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

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

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

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

```
version -v
```

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

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

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

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

1. Déterminez le gestionnaire de clés activé sur votre système :

Version ONTAP	Exécutez cette commande
ONTAP 9.14.1 ou version ultérieure	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> • Si EKM est activé, EKM est répertorié dans la sortie de la commande. • Si OKM est activé, OKM est répertorié dans la sortie de la commande. • Si aucun gestionnaire de clés n'est activé, No key manager keystores configured est répertorié dans la sortie de la commande.
ONTAP 9.13.1 ou version antérieure	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • Si EKM est activé, external est répertorié dans la sortie de la commande. • Si OKM est activé, onboard est répertorié dans la sortie de la commande. • Si aucun gestionnaire de clés n'est activé, No key managers configured est répertorié dans la sortie de la commande.

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

Aucun gestionnaire de clés configuré

Vous pouvez arrêter le contrôleur défectueux en toute sécurité. Allez à "[arrêtez le contrôleur défectueux](#)".

Gestionnaire de clés externe ou intégré configuré

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

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

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

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

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

Gestionnaire de clés externe

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

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

Gestionnaire de clés intégré

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

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

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

Arrêter le contrôleur défectueux - AFF C80

Arrêtez le contrôleur défectueux en suivant la procédure appropriée à votre configuration.

Option 1 : la plupart des systèmes

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.

Description de la tâche

- Si vous disposez d'un système SAN, vous devez avoir vérifié les messages d'événement `cluster kernel-service show`) pour le serveur lame SCSI du contrôleur défectueux. ``cluster kernel-service show`` La commande (from priv mode Advanced) affiche le nom du nœud, son état de disponibilité et "état du quorum"son état de fonctionnement.

Chaque processus SCSI-Blade doit se trouver au quorum avec les autres nœuds du cluster. Tout problème doit être résolu avant de procéder au remplacement.

- 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. Si AutoSupport est activé, supprimez la création automatique de cas en appelant un message AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

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
```



Lorsque vous voyez *voulez-vous désactiver l'auto-giveback?*, entrez `y`.

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.
Attente du retour...	Appuyez sur Ctrl-C, puis répondez <code>y</code> lorsque vous y êtes invité.
Invite système ou invite de mot de passe	Prendre le contrôle défectueux ou l'arrêter à partir du contrôleur en bon état : <pre>storage failover takeover -ofnode impaired_node_name</pre> Lorsque le contrôleur douteux s'affiche en attente de rétablissement..., appuyez sur Ctrl-C et répondez <code>y</code> .

Option 2 : le contrôleur est dans un MetroCluster

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](#)".
- Vous devez avoir confirmé que l'état de configuration MetroCluster est configuré et que les nœuds sont à l'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 :

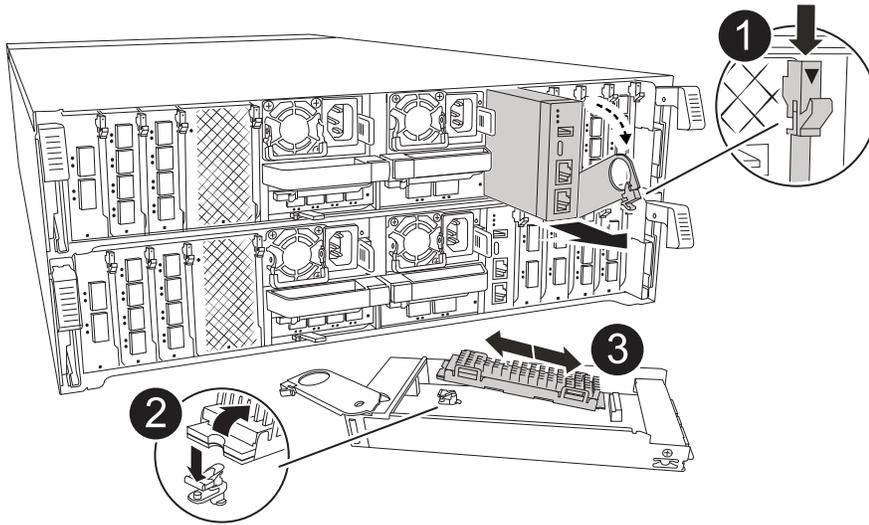
Si le contrôleur en état de fonctionnement s'affiche...	Alors...
Invite DU CHARGEUR	Passez à la section suivante.
Attente du retour...	Appuyez sur Ctrl-C, puis répondez <code>y</code> lorsque vous y êtes invité.
Invite système ou invite de mot de passe (entrer le mot de passe système)	Prendre le contrôle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

Remplacez le support de démarrage - AFF C80

Vous devez brancher le module de contrôleur, retirer le module de gestion du système à l'arrière du système, retirer le support d'amorçage défectueux et installer le support d'amorçage de remplacement dans le module de gestion du système.

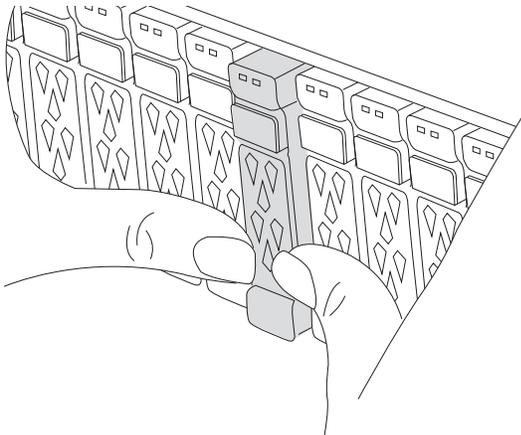
Étape 1 : remplacer le support de démarrage

Le support de démarrage se trouve à l'intérieur du module de gestion du système et est accessible en retirant le module du système.



1	Loquet de came du module de gestion du système
2	Bouton de verrouillage du support de démarrage
3	Support de démarrage

1. À l'avant du châssis, enfoncez fermement chaque disque jusqu'à ce que vous sentiez un arrêt positif. Cela permet de s'assurer que les disques sont fermement installés contre le fond de panier central du châssis.



2. Aller à l'arrière du châssis. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
3. Débranchez l'alimentation du module de contrôleur en tirant le module de contrôleur vers l'extérieur d'environ trois pouces :
 - a. Appuyez sur les deux loquets de verrouillage du module de contrôleur, puis faites pivoter les deux loquets vers le bas en même temps.

- b. Retirez le module de contrôleur d'environ 3 pouces du châssis pour le mettre hors tension.
 - c. Retirez tous les câbles connectés au module de gestion du système. Veillez à étiqueter l'emplacement de connexion des câbles afin de pouvoir les connecter aux ports appropriés lorsque vous réinstallez le module.
 - d. Faites pivoter le chemin de câbles vers le bas en tirant sur les boutons situés des deux côtés à l'intérieur du chemin de câbles, puis faites pivoter le bac vers le bas.
 - e. Appuyez sur le bouton de la came de gestion du système. Le levier de came s'éloigne du châssis.
 - f. Faites pivoter le levier de came complètement vers le bas et retirez le module de gestion du système du module de contrôleur.
 - g. Placez le module de gestion du système sur un tapis antistatique, de manière à ce que le support de démarrage soit accessible.
4. Retirez le support de démarrage du module de gestion :
 - a. Appuyez sur le bouton de verrouillage bleu.
 - b. Faites pivoter le support de démarrage vers le haut, faites-le glisser hors du support et mettez-le de côté.
 5. Installez le support de démarrage de remplacement dans le module de gestion du système :
 - a. Alignez les bords du support de coffre avec le logement de la prise, puis poussez-le doucement d'équerre dans le support.
 - b. Faites pivoter le support de démarrage vers le bas, vers le bouton de verrouillage.
 - c. Appuyez sur le bouton de verrouillage, faites pivoter le support de démarrage complètement vers le bas, puis relâchez le bouton de verrouillage.
 6. Réinstallez le module de gestion du système :
 - a. Faites pivoter le chemin de câbles vers le haut jusqu'à la position fermée.
 - b. Recâblage du module de gestion du système.

Étape 2 : transférez l'image de démarrage sur le support de démarrage

Le support de démarrage de remplacement que vous avez installé est sans image ONTAP. Vous pouvez transférer l'image ONTAP sur le support de démarrage de remplacement en téléchargeant l'image de service ONTAP appropriée du "[Site de support NetApp](#)" vers une clé USB, puis vers le support de démarrage de remplacement.

Avant de commencer

- Vous devez disposer d'une clé USB, formatée en FAT32, avec au moins 4 Go de capacité.
- Téléchargez une copie de la même version d'image de ONTAP que celle utilisée par le contrôleur défectueux. Vous pouvez télécharger l'image appropriée à partir de la section Téléchargements du site de support NetApp. Utilisez `version -v` la commande pour afficher si votre version de ONTAP prend en charge NVE. Si le résultat de la commande affiche `<10no- DARE>`, votre version de ONTAP ne prend pas en charge NVE.
 - Si NVE est pris en charge par votre version de ONTAP, téléchargez l'image avec le chiffrement de volume NetApp, comme indiqué sur le bouton de téléchargement.
 - Si NVE n'est pas pris en charge, téléchargez l'image sans chiffrement de volume NetApp, comme indiqué sur le bouton de téléchargement.
- Si votre système est une paire haute disponibilité, vous devez disposer d'une connexion réseau entre les ports de gestion des nœuds des contrôleurs (en général, les interfaces e0M).

Étapes

1. Téléchargez et copiez l'image de service appropriée du "[Site de support NetApp](#)" sur la clé USB.
 - a. Téléchargez l'image de service à partir du lien Téléchargements de la page, vers votre espace travail sur votre ordinateur portable.
 - b. Décompressez l'image du service.



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

Le lecteur flash USB doit avoir l'image ONTAP appropriée de ce que le contrôleur défectueux fonctionne.

- a. Retirez la clé USB de votre ordinateur portable.
2. Insérez la clé USB dans le port USB-A du module de gestion du système.

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

3. Rebranchez l'alimentation au module de contrôleur :
 - a. Poussez fermement le module de contrôleur dans le châssis jusqu'à ce qu'il rencontre le fond de panier central et qu'il soit bien en place.

Les loquets de verrouillage se montent lorsque le module de contrôleur est bien en place.

- b. Faites pivoter les loquets de verrouillage vers le haut en position verrouillée.

Le contrôleur commence à démarrer dès que l'alimentation est reconnectée au système.

4. 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.

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

- Si vous configurez DHCP : `ifconfig e0M -auto`



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

- Si vous configurez des connexions manuelles : `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway`
 - 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.



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

Démarrez l'image de récupération - AFF C80

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

Étapes

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

```
boot_recovery
```

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

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

Option 1 : ONTAP 9.16.0 ou version antérieure

- a. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `Do you want to restore the backup configuration now?`
- b. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à remplacer `/etc/ssh/ssh_host_ecdsa_key`.
- c. Sur le contrôleur sain, définissez le contrôleur défectueux sur le niveau de privilège avancé : `set -privilege advanced`.
- d. Sur le contrôleur partenaire sain, exécutez la commande `restore backup : system node restore-backup -node local -target-address impaired_node_IP_address`.

REMARQUE : si vous voyez un message autre qu'une restauration réussie, contactez "[Support NetApp](#)".

- e. Sur le contrôleur partenaire sain, remettez le contrôleur défectueux au niveau admin: `set -privilege admin`.
- f. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `Was the restore backup procedure successful?`.
- g. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous voyez `...would you like to use this restored copy now?`.
- h. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le contrôleur défectueux et appuyez sur `ctrl-c` pour accéder au menu de démarrage.
- i. Si le système n'utilise pas le chiffrement, sélectionnez *option 1 démarrage normal.*, sinon, passez à "[Restaurez le chiffrement](#)".

Option 2 : ONTAP 9.16.1 ou version ultérieure

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

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

- b. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous y êtes invité pour confirmer si la sauvegarde de restauration a réussi.
- c. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à utiliser la configuration restaurée.
- d. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le nœud.
- e. Sur le contrôleur défectueux, appuyez sur `Y` lorsque vous êtes invité à redémarrer le contrôleur défectueux et appuyez sur `ctrl-c` pour accéder au menu de démarrage.
- f. Si le système n'utilise pas le chiffrement, sélectionnez *option 1 démarrage normal.*, sinon, passez à "[Restaurez le chiffrement](#)".

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

`local -auto-giveback true` commande.

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

REMARQUE : si le processus échoue, contactez "[Support NetApp](#)".

Restaurer le chiffrement - AFF C80

Restaurez le chiffrement sur le support de démarrage de remplacement.

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

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

- "[Option 1 : restaurez la configuration du gestionnaire de clés intégré](#)"
- "[Option 2 : restaurez la configuration du gestionnaire de clés externe](#)"

Option 1 : restaurez la configuration du gestionnaire de clés intégré

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

Avant de commencer

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

Étapes

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

Version ONTAP	Sélectionnez cette option
ONTAP 9.8 ou version ultérieure	<p data-bbox="621 153 925 189">Sélectionnez l'option 10.</p> <p data-bbox="621 220 1161 256">Affiche un exemple de menu de démarrage</p> <div data-bbox="654 298 1456 1081" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="683 331 1294 367">Please choose one of the following:</p><ul data-bbox="683 409 1369 1008" style="list-style-type: none"><li data-bbox="683 409 971 445">(1) Normal Boot.<li data-bbox="683 451 1133 487">(2) Boot without /etc/rc.<li data-bbox="683 493 1047 529">(3) Change password.<li data-bbox="683 535 1369 604">(4) Clean configuration and initialize all disks.<li data-bbox="683 611 1153 646">(5) Maintenance mode boot.<li data-bbox="683 653 1328 688">(6) Update flash from backup config.<li data-bbox="683 695 1242 730">(7) Install new software first.<li data-bbox="683 737 977 772">(8) Reboot node.<li data-bbox="683 779 1193 848">(9) Configure Advanced Drive Partitioning.<li data-bbox="683 854 1333 924">(10) Set Onboard Key Manager recovery secrets.<li data-bbox="683 930 1317 999">(11) Configure node for external key management.<p data-bbox="683 1014 1031 1050">Selection (1-11)? 10</p></div>

Version ONTAP	Sélectionnez cette option
ONTAP 9.7 et versions antérieures	<p data-bbox="621 163 1421 195">Sélectionnez l'option cachée <code>recover_onboard_keymanager</code></p> <p data-bbox="621 233 1162 264">Affiche un exemple de menu de démarrage</p> <div data-bbox="654 306 1455 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="683 342 1369 932">Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager</pre> </div>

3. Confirmez que vous souhaitez poursuivre le processus de restauration.

Afficher l'exemple d'invite

```
This option must be used only in disaster recovery procedures. Are you
sure? (y or n):
```

4. Saisissez deux fois la phrase de passe au niveau du cluster.

Lorsque vous saisissez la phrase de passe, la console n'affiche aucune entrée.

Afficher l'exemple d'invite

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Entrez les informations de sauvegarde.

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

Afficher l'exemple d'invite

```
Enter the backup data:  
  
-----BEGIN BACKUP-----  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
34567890123456789012345678901234567890123456789012345678901234567890123456  
45678901234567890123456789012345678901234567890123456789012345678901234567  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  
-----END BACKUP-----
```

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

Le processus de récupération est terminé.

Afficher l'exemple d'invite

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```



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

6. Sélectionnez l'option 1 dans le menu de démarrage pour poursuivre le démarrage dans ONTAP.

Afficher l'exemple d'invite

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Vérifier que la console du contrôleur affiche le message suivant.

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

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

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

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

```
security key-manager onboard sync
```

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

Afficher l'exemple d'invite

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

```
All offline encrypted volumes will be brought online and the
corresponding volume encryption keys (VEKs) will be restored
automatically within 10 minutes. If any offline encrypted volumes
are not brought online automatically, they can be brought online
manually using the "volume online -vserver <vserver> -volume
<volume_name>" command.
```



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

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

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

```
There are no entries matching your query.
```



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

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

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

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

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

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

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

Option 2 : restaurez la configuration du gestionnaire de clés externe

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

Avant de commencer

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

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

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

Étapes

1. Branchez le câble de la console au contrôleur cible.
2. Sélectionnez l'option 11 dans le menu de démarrage ONTAP.

Affiche un exemple de menu de démarrage

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

3. Lorsque vous y êtes invité, vérifiez que vous avez recueilli les informations requises.

Afficher l'exemple d'invite

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

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

Afficher l'invite

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

Montrer l'exemple

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEWpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUwQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpzbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmp_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmp_init: cmd: ReleaseExtraBSDPort e0M
```

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

Montrer l'exemple

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

5. Sélectionnez l'option 1 dans le menu de démarrage pour poursuivre le démarrage dans ONTAP.

Afficher l'exemple d'invite

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

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

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

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

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

Envoyez la pièce défectueuse à NetApp - AFF C80

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

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.