Support de démarrage

Install and maintain

NetApp
September 25, 2024

Sommaire

Support de démarrage

Workflow de remplacement des supports de démarrage - FAS70 et FAS90

Procédez comme suit pour remplacer votre support de démarrage.

1. **"Vérifiez les exigences de remplacement des supports de démarrage"**

Pour remplacer le support de démarrage, vous devez répondre à certaines exigences.

2. **"Vérifiez les clés de chiffrement intégrées"**

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 défectueux.

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 sur le support de démarrage de remplacement.

5. **"Démarrez l'image de récupération"**

Démarrez 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.

Remplacement du support de démarrage requis - FAS70 et FAS90

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`.
- 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.

Vérifier les clés de chiffrement intégrées - FAS70 et FAS90

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

Si vous avez un cluster avec plus de deux nœuds, il doit être dans le quorum. Si le cluster n'est pas au quorum ou si un contrôleur en bonne santé affiche la valeur false pour l'éligibilité et la santé, vous devez corriger le problème avant de désactiver le contrôleur défaillant ; voir "Synchroniser un nœud avec le cluster".

Vérifiez NVE ou NSE

Avant d'arrêter le contrôleur défaillant, vous devez vérifier que le gestionnaire de clés de sécurité est activé ou que les disques chiffrés sont bien activés sur le système.

Vérifiez la configuration du gestionnaire de clés de sécurité

Étapes

1. Déterminez si le gestionnaire de clés est actif à l'aide de la commande *Security Key-Manager keystore show*. Pour plus d'informations, reportez-vous à la section "Page de MANUEL d'affichage du gestionnaire de clés de sécurité"

   Vous pouvez avoir d'autres types de gestionnaire de clés. Les types sont `KMIP`, , `AKV`et `GCP`. Le processus de confirmation de ces types est le même que celui de confirmation `external` ou de `onboard` gestionnaire de clés.

   - Si aucune sortie n'est affichée, passer à "arrêtez le contrôleur défectueux" pour arrêter le nœud défectueux.
   - Si la commande affiche les valeurs de sortie, le système est `security key-manager` actif et vous devez afficher le type et l' `Key Manager` état.
2. Afficher les informations pour active à l'aide de la `Key Manager` commande *Security Key-Manager key query*.

- Si le `Key Manager` type s'affiche `external` et que la `Restored` colonne affiche `true`, vous pouvez arrêter le contrôleur défectueux en toute sécurité.
- Si le `Key Manager` type s'affiche `onboard` et que la `Restored` colonne s'affiche `true`, vous devez effectuer quelques étapes supplémentaires.
- Si le `Key Manager` type s'affiche `external` et que la `Restored` colonne affiche autre chose que `true`, vous devez effectuer certaines étapes supplémentaires.
- Si le `Key Manager` type s'affiche `onboard` et que la `Restored` colonne affiche autre chose que `true`, vous devez effectuer certaines étapes supplémentaires.

3. Si le `Key Manager` type s'affiche `onboard` et que la `Restored` colonne affiche `true`, sauvegardez manuellement les informations sur OKM :
   a. 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. Vous pouvez arrêter le contrôleur défectueux en toute sécurité.
4. Si le `Key Manager` type s'affiche `onboard` et que la `Restored` colonne affiche autre chose que `true`:
   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 à l'invite. Si la phrase de passe ne peut pas être fournie, contactez le support NetApp. "mysupport.netapp.com"

   b. Vérifiez que la `Restored` colonne s'affiche `true` pour toutes les clés d'authentification : `security key-manager key query`
   c. Vérifiez que le `Key Manager` type s'affiche `onboard`, puis sauvegardez manuellement les informations sur OKM.
   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. Vous pouvez arrêter le contrôleur en toute sécurité.
5. Si le `Key Manager` type s'affiche `external` et que la `Restored` colonne affiche autre chose que `true`:
   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 à l'adresse "mysupport.netapp.com".

   b. Vérifiez que la `Restored` colonne s'affiche `true` pour toutes les clés d'authentification : *Security Key-Manager key query*
   c. Vous pouvez arrêter le contrôleur défectueux en toute sécurité.

Arrêtez le contrôleur pour facultés affaiblies - FAS70 et FAS90

Une fois les tâches NVE ou NSE terminées, vous devez arrêter le contrôleur pour cause de dysfonctionnement. Arrêtez ou prenez le contrôleur défaillant en suivant la procédure appropriée pour 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 (depuis la commande priv en mode avancé) affiche le nom du nœud, l'état de quorum de ce nœud, l'état de disponibilité de ce nœud ainsi que l'état opérationnel de ce nœud.

  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 `y` 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 : `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 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".
- 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 :

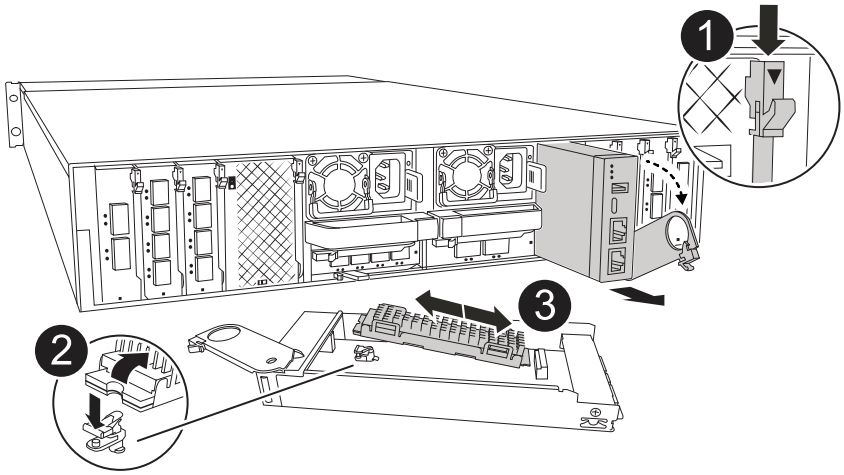
Si le contrôleur en état de fonctionnement s'affiche…	Alors…
Invite DU CHARGEUR	Passez à l'étape suivante.
Attente du retour…	Appuyez sur Ctrl-C, puis répondez `y` lorsque vous y êtes invité.
Invite système ou invite de mot de passe (entrer le mot de passe système)	Prendre le contrôle défectueux ou l'arrêter 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 - FAS70 et FAS90

Pour remplacer le support de démarrage, vous devez retirer le module de gestion du système de l'arrière du système, retirer le support de démarrage défectueux et installer le support de démarrage 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. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
2. Débranchez les câbles d'alimentation des unités d'alimentation du contrôleur.

> Si votre système de stockage est équipé d'une alimentation CC, déconnectez le bloc de câbles d'alimentation des unités d'alimentation.

a. Retirez tous les câbles connectés au module de gestion du système. Assurez-vous d'étiqueter l'emplacement de connexion des câbles afin de pouvoir les connecter aux ports appropriés lorsque vous réinstallez le module.

b. 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.

c. Appuyez sur le bouton CAM de gestion du système.

d. Faites pivoter le loquet de came le plus loin possible.

e. Retirez le module de gestion du système du boîtier en accrochant votre doigt dans l'ouverture du levier de came et en tirant le module hors du boîtier.

f. Placez le module de gestion du système sur un tapis antistatique, de manière à ce que le support de démarrage soit accessible.

3. 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.

4. 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.

5. Réinstallez le module de gestion du système.

a. Alignez le module avec les bords de l'ouverture du logement du boîtier.

b. Faites glisser doucement le module dans le logement jusqu'à l'intérieur du boîtier, puis faites pivoter le loquet de came complètement vers le haut pour verrouiller le module en place.

6. Faites pivoter le chemin de câbles vers le haut jusqu'à la position fermée.

a. Recâblage du module de gestion du système.

Étape 2 : transférez l'image ONTAP 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" sur une clé USB, puis sur le support de démarrage de remplacement.

Avant de commencer

- Vous devez disposer d'une clé USB vide, formatée en FAT32, d'une capacité minimale de 4 Go.
- Vous devez disposer d'une copie de la même version d'image de ONTAP que celle utilisée par le contrôleur défectueux. Vous pouvez télécharger l'image appropriée depuis la "Téléchargements" section du site de support NetApp
  - Si NVE est pris en charge, 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.

   c. Retirez la clé USB de votre ordinateur portable.
2. Insérez la clé USB dans le logement USB 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. Branchez les câbles d'alimentation aux blocs d'alimentation et réinstallez le dispositif de retenue du câble d'alimentation.

   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.

Démarrer l’image de restauration - FAS70 et FAS90

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

Étapes

1. À partir de l’invite du CHARGEUR, démarrez l’image de récupération à partir du lecteur flash USB : *boot_Recovery*

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

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

Si votre système est en cours d'exécution…	Alors…
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 écraser `/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 alghed_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 de chiffrement, sélectionnez *option 1 démarrage normal.*, sinon passez à "Restaurer les gestionnaires de clés". j. Branchez le câble de la console au contrôleur partenaire. k. Remettez le contrôleur en place en utilisant la commande *Storage failover giveback -fromnode local*. l. Restaurez le rétablissement automatique si vous l'avez désactivé à l'aide de la commande *Storage failover modify -node local -auto -giveback true*. m. Si AutoSupport est activé, restaurez/annulez la suppression de la création automatique de cas en utilisant le noeud système AutoSupport Invoke -node * -type all -message maint=END_ command. **REMARQUE :** si le processus échoue, contactez "Support NetApp".

Si votre système est en cours d'exécution…	Alors…
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 êtes invité à 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 de chiffrement, sélectionnez *option 1 démarrage normal.*, sinon passez à "Restaurer les gestionnaires de clés". g. Branchez le câble de la console au contrôleur partenaire. h. Remettez le contrôleur en place en utilisant la commande *Storage failover giveback -fromnode local*. i. Restaurez le rétablissement automatique si vous l'avez désactivé à l'aide de la commande *Storage failover modify -node local -auto -giveback true*. j. Si AutoSupport est activé, restaurez/annulez la suppression de la création automatique de cas en utilisant le noeud système AutoSupport Invoke -node * -type all -message maint=END_ command. **REMARQUE :** si le processus échoue, contactez "Support NetApp".

Restaurez le chiffrement - FAS70 et FAS90

Restaurez le chiffrement sur le support de démarrage de remplacement.

Étape 1 : restaurez le gestionnaire de clés intégré

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 que vous avez capturés au début de cette procédure.

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

Étapes

1. Branchez le câble de la console au contrôleur cible.
2. Sélectionnez l’une des options suivantes pour restaurer la configuration du gestionnaire de clés intégré à partir du menu d’amorçage ONAT.

Option 1 : systèmes avec configuration de serveur de gestionnaire de clés intégrée

Restaurez la configuration du gestionnaire de clés intégré à partir du menu de démarrage ONAT.

Avant de commencer

Vous avez besoin 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. Dans le menu de démarrage ONTAP, sélectionnez l'option 10 :

```
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.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 10
```

2. Confirmez la poursuite du processus. `This option must be used only in disaster recovery procedures. Are you sure? (y or n):` *y*
3. Saisissez deux fois la phrase de passe au niveau du cluster.

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

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

4. Entrez les informations de sauvegarde. Collez l'intégralité du contenu de la ligne de DÉBUT DE SAUVEGARDE à travers la ligne de FIN DE SAUVEGARDE.

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

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------END BACKUP---------------------------
```

5. Le processus de récupération sera terminé.

```
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.

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

8. Depuis le nœud partenaire, rendre le contrôleur partenaire : *Storage failover giveback -fromnode local -only-cfo-aggrégats true*
9. Une fois démarré uniquement avec l'agrégat CFO, exécutez la commande *Security Key-Manager Onboard sync* :
10. Entrez la phrase de passe au niveau du cluster pour le gestionnaire de clés intégré :

```
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.
```

11. Assurez-vous que toutes les clés sont synchronisées : *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. Rétablissement du nœud depuis le partenaire : *Storage failover giveback -fromnode local*

Option 2 : systèmes avec configuration de serveur de gestionnaire de clés externe

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

Avant de commencer

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

- Vous avez besoin d'une copie du fichier /cfcard/kmip/servers.cfg d'un autre nœud du cluster, ou des informations suivantes :
- Adresse du serveur KMIP.
- Port KMIP.
- Copie du fichier /cfcard/kmip/certs/client.crt d'un autre nœud de cluster, ou du certificat client.
- Copie du fichier /cfcard/kmip/certs/client.key à partir d'un autre nœud du cluster ou de la clé client.
- Copie du fichier /cfcard/kmip/certs/CA.pem à partir d'un autre nœud de cluster ou de l'autorité de certification du serveur KMIP.

Étapes

1. Sélectionnez l'option 11 dans le menu de démarrage ONTAP.

```
(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
```

2. Lorsque vous y êtes invité, confirmez que vous avez recueilli les informations requises :
   a. `Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}` *y*
   b. `Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}` *y*
   c. `Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}` *y*
   d. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *y*

      Vous pouvez également utiliser ces invites à la place :

   e. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *n*
      i. `Do you know the KMIP server address? {y/n}` *y*
      ii. `Do you know the KMIP Port? {y/n}` *y*
3. Fournissez les informations relatives à chacune de ces invites :
   a. `Enter the client certificate (client.crt) file contents:`
   b. `Enter the client key (client.key) file contents:`
   c. `Enter the KMIP server CA(s) (CA.pem) file contents:`
   d. `Enter the server configuration (servers.cfg) file contents:`

```
Example

Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----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....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

4. Le processus de récupération se termine :

```
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.

```
**********************************************************************
***************
* 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
```

Étape 2 : terminez le remplacement du support de démarrage

Terminez le processus de remplacement du support de démarrage après le démarrage normal en effectuant les vérifications finales et en donnant du stockage supplémentaire.

1. Vérifiez la sortie de la console :

Si la console affiche…	Alors…
Invite de connexion	Passez à l'étape 6.
Attente du retour…	a. Connectez-vous au contrôleur partenaire. b. Vérifiez que le contrôleur cible est prêt pour le rétablissement avec la commande *Storage failover show*.

2. Déplacez le câble de la console vers le contrôleur partenaire et remettez le stockage du contrôleur cible en utilisant la commande *Storage failover giveback -fromnode local -only-cfo-aggregates true*.
   - 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 parce que le partenaire est « non prêt », attendez 5 minutes que le sous-système HA se synchronise entre les partenaires.

- 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.

3. Attendez 3 minutes et vérifiez l'état du basculement à l'aide de la commande *Storage failover show*.
4. À l'invite clustershell, entrez la commande *network interface show -is-home false* pour répertorier les interfaces logiques qui ne se trouvent pas sur leur contrôleur et port de base.

   Si l'une des interfaces est répertoriée comme `false`, rétablissez le port de base de ces interfaces à l'aide de la commande *net int revert -vserver Cluster -lif _nodename* .

5. Déplacez le câble de la console vers le contrôleur cible et exécutez la commande *version -v* pour vérifier les versions de ONTAP.
6. Utilisez les `storage encryption disk show` pour vérifier la sortie.
7. Utilisez la commande *Security Key-Manager key query* 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 `Key Manager type` = `external` et la `Restored` colonne = autre que `yes/true`, utilisez la commande *Security Key-Manager external restore* pour restaurer les ID de clé des clés d'authentification.

     Si la commande échoue, contactez l'assistance clientèle.

   - Si `Key Manager type` = `onboard` et la `Restored` colonne = autre que `yes/true`, utilisez la commande *Security Key-Manager Onboard sync* pour synchroniser les clés embarquées manquantes sur le nœud réparé.

     Utilisez la commande *Security Key-Manager key query* pour vérifier que la `Restored` colonne = `yes/true` pour toutes les clés d'authentification.

8. Branchez le câble de la console au contrôleur partenaire.
9. Reaccordez le contrôleur à l'aide du `storage failover giveback -fromnode local` commande.
10. Restaurez le rétablissement automatique si vous l'avez désactivé à l'aide de la commande *Storage failover modify -node local -auto-giveback true*.
11. Si AutoSupport est activé, restaurez/annulez la suppression de la création automatique de cas en utilisant le noeud système AutoSupport Invoke -node * -type all -message maint=END_ command.

Renvoyer la pièce défectueuse à NetApp - FAS70 et FAS90

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

Informations sur les marques commerciales