



Support de démarrage

Install and maintain

NetApp
August 22, 2025

Sommaire

- Support de démarrage 1
 - Remplacez le support de démarrage - FAS9500 1
 - Vérifier la prise en charge et l'état des clés de cryptage - FAS9500 1
 - Étape 1 : vérifiez si votre version de ONTAP prend en charge le chiffrement de volume NetApp 1
 - Étape 2 : déterminez s'il est possible d'arrêter le contrôleur en toute sécurité 2
 - Arrêtez le contrôleur défaillant - FAS9500 5
 - Retirez le contrôleur, remplacez le support de démarrage et transférez l'image de démarrage - FAS9500 .. 6
 - Étape 1 : retirer le module de contrôleur 7
 - Étape 2 : remplacer le support de démarrage 9
 - Étape 3 : transférez l'image de démarrage sur le support de démarrage 11
 - Démarrez l'image de restauration - FAS9500 12
 - Restaurer le chiffrement - FAS9500 15
 - Option 1 : restaurez la configuration du gestionnaire de clés intégré 15
 - Option 2 : restaurez la configuration du gestionnaire de clés externe 21
 - Renvoyez la pièce défectueuse à NetApp - FAS9500 24

Support de démarrage

Remplacez le support de démarrage - FAS9500

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 nœud *trouble* est le nœud sur lequel vous effectuez la maintenance.
 - Le *Healthy node* est le partenaire HA du nœud douteux.

Vérifier la prise en charge et l'état des clés de cryptage - FAS9500

Pour assurer la sécurité des données sur votre système de stockage, vous devez vérifier la prise en charge et l'état de la clé de cryptage sur votre support de démarrage. Vérifiez si votre version de ONTAP prend en charge NetApp Volume Encryption (NVE) et avant d'arrêter le contrôleur, vérifiez si le gestionnaire de clés est actif.

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.

Étapes

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.

Étapes

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, <code>No key manager keystores configured</code> 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, <code>external</code> est répertorié dans la sortie de la commande.• Si OKM est activé, <code>onboard</code> est répertorié dans la sortie de la commande.• Si aucun gestionnaire de clés n'est activé, <code>No key managers configured</code> 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

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

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

- b. 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>

Arrêtez le contrôleur défaillant - FAS9500

Arrêtez ou prenez le contrôleur pour facultés affaiblies en utilisant l'une des options suivantes.

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

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 dossier en invoquant 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 retour automatique :

- a. Entrez la commande suivante depuis la console du contrôleur sain :

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

- b. Entrer y lorsque vous voyez l'invite *Voulez-vous désactiver le retour automatique ?*

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	<p>Prendre le contrôle défectueux ou l'arrêter à partir du contrôleur en bon état :</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>Le paramètre <i>-halt true</i> vous amène à l'invite Loader.</p>

Retirez le contrôleur, remplacez le support de démarrage et transférez l'image de démarrage - FAS9500

Vous devez retirer et ouvrir le module de contrôleur, localiser et remplacer le support de démarrage du contrôleur, puis transférer l'image vers le support de démarrage de remplacement.

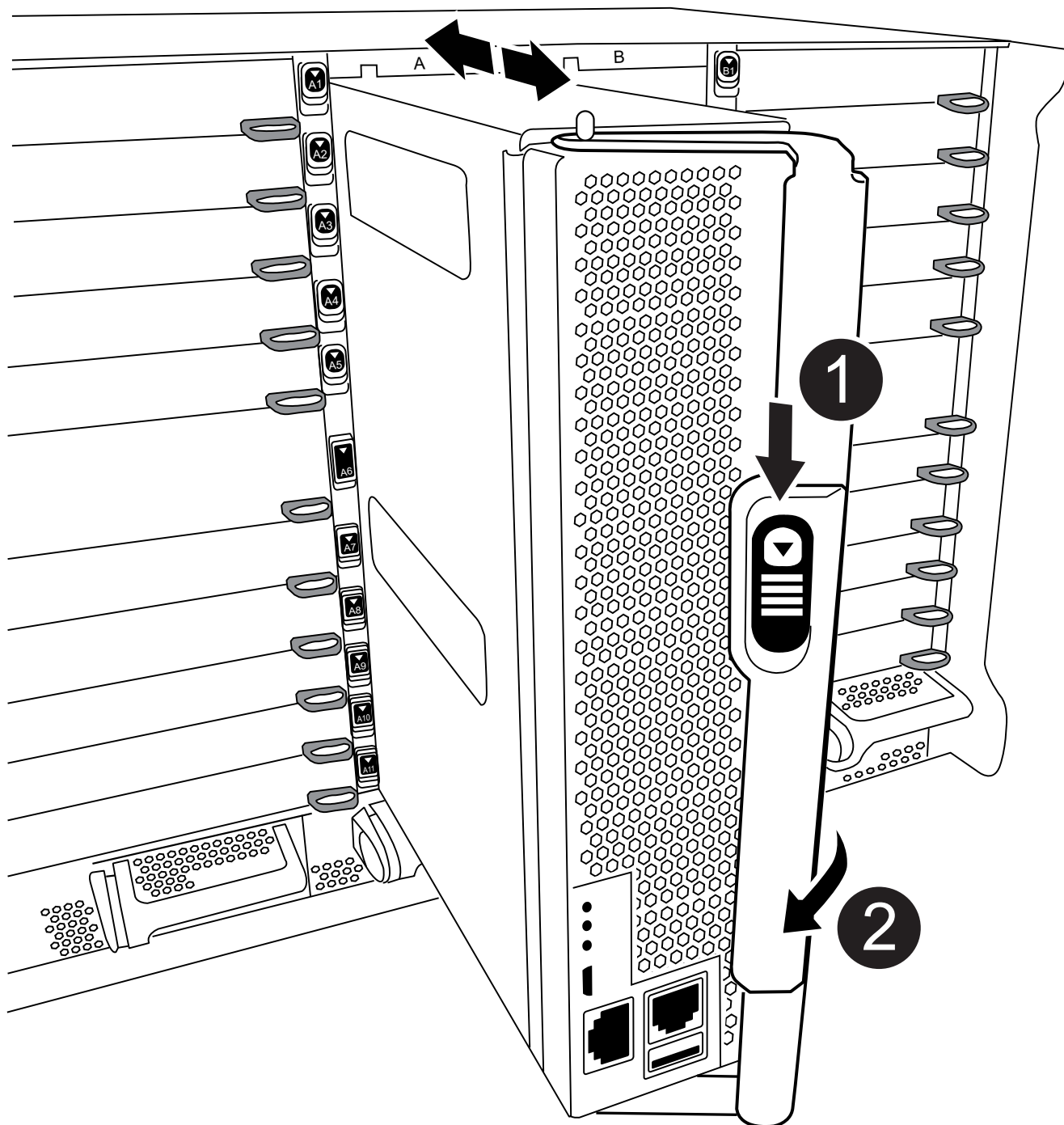
Étape 1 : retirer le module de contrôleur

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 en terre cuite de la poignée de came vers le bas jusqu'à ce qu'il se déverrouille.

[Animation - retirez le module de contrôleur](#)

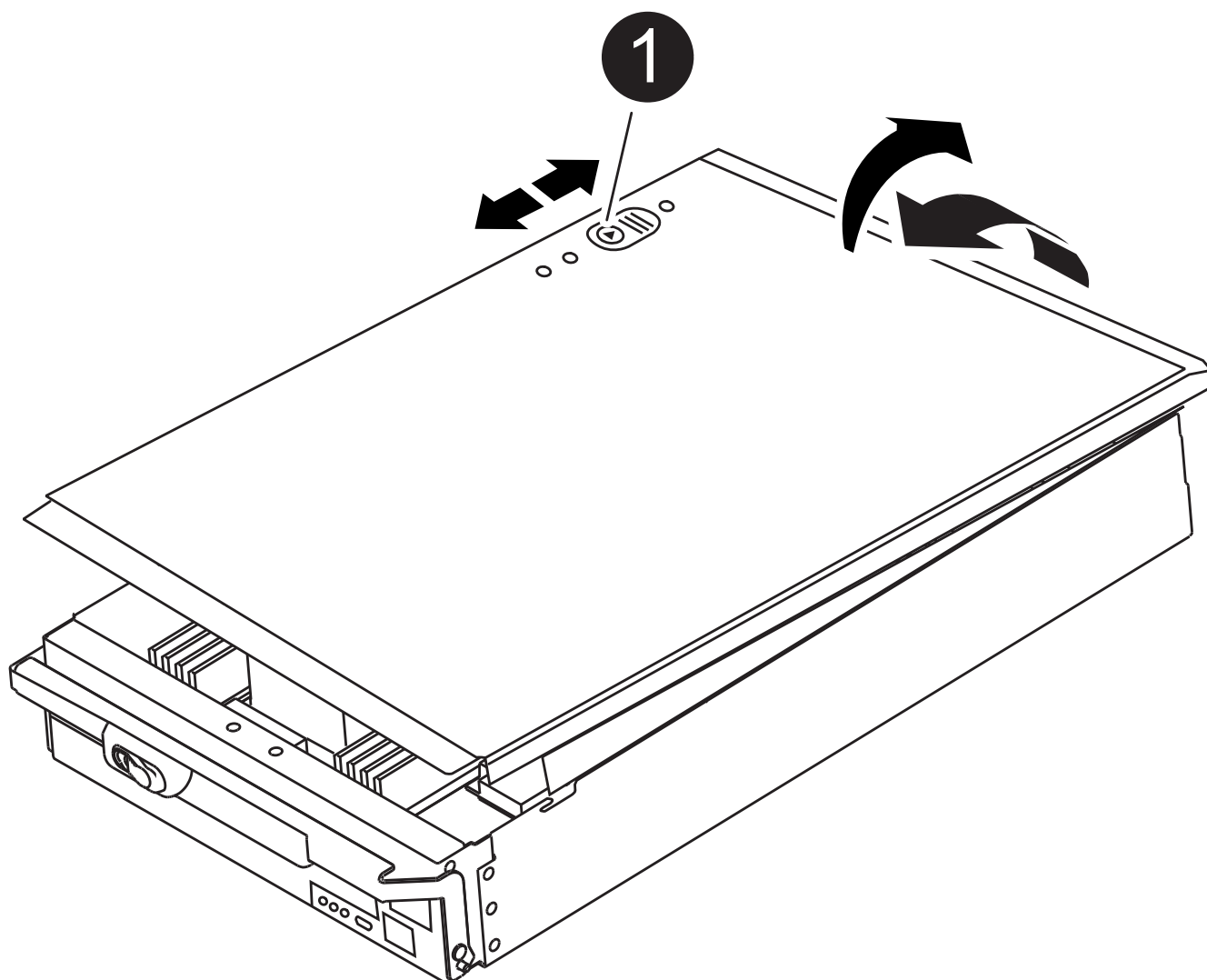


1	Bouton de déverrouillage de la poignée de came
2	Poignée de came

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

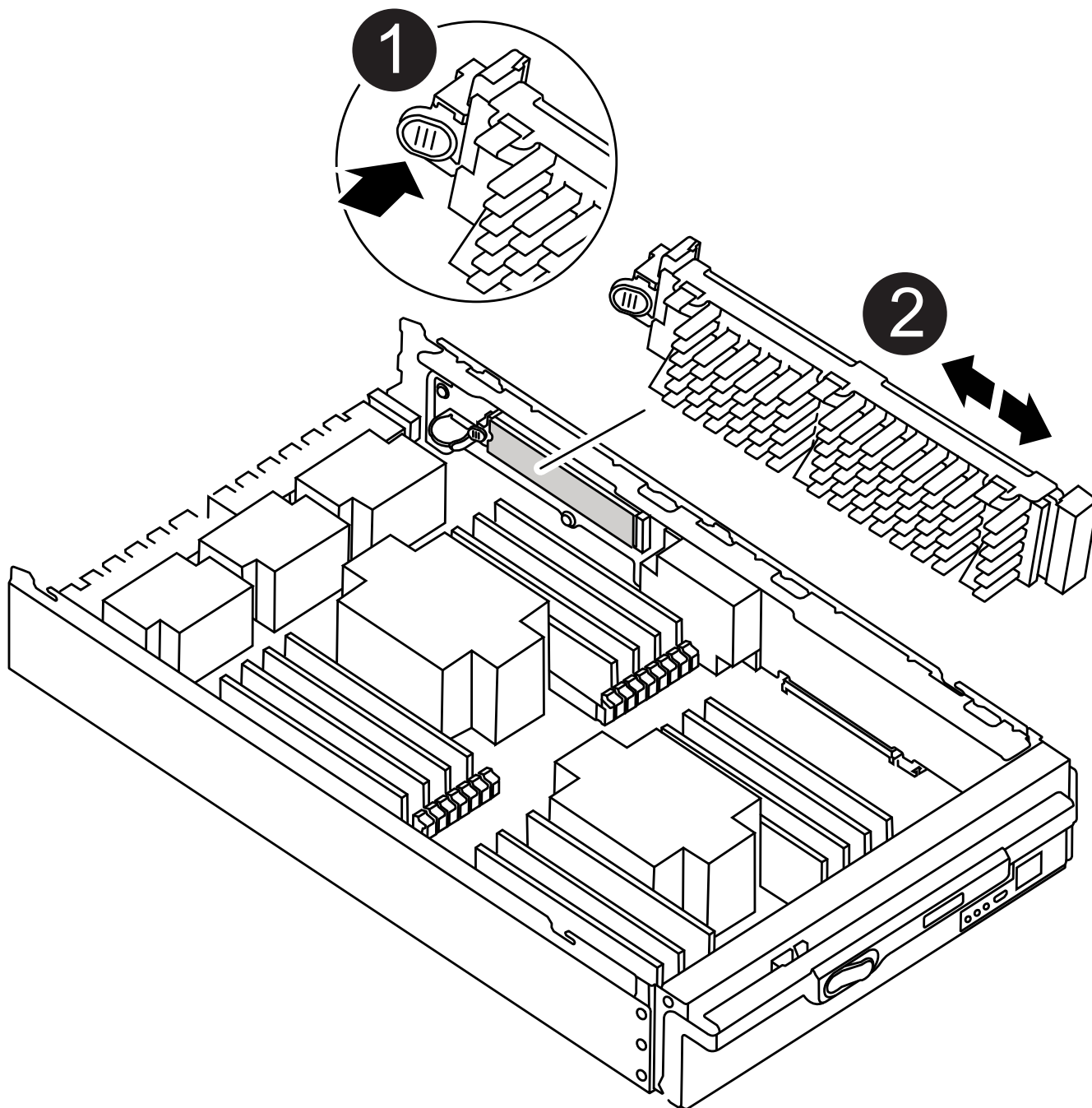
Étape 2 : remplacer le support de démarrage

Vous devez localiser le support de démarrage dans le contrôleur et suivre les instructions pour le remplacer.

Étapes

1. Soulevez le conduit d'air noir à l'arrière du module de contrôleur, puis localisez le support de démarrage à l'aide de l'illustration suivante ou de la carte FRU du module de contrôleur :

[Animation - remplacer le support d'amorçage](#)



1	Appuyez sur la languette de dégagement
2	Support de démarrage

- 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.

- Alignez les bords du support de démarrage de remplacement avec le support de démarrage, puis

poussez-le doucement dans le support.

4. 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.

5. Poussez le support de démarrage vers le bas pour engager le bouton de verrouillage sur le boîtier du support de démarrage.
6. 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.

Avant de commencer

- 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 effectuer un redémarrage supplémentaire lors de la restauration du système de fichiers var.

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

erreurs à l'aide du `setenv variable-name <value>` commande.

a. Vérifier les variables d'environnement de boot:

- `bootarg.init.boot_clustered`
- `partenaire`
- `bootarg.init.flash_optimized` pour AFF
- `bootarg.init.san_optimized` pour AFF
- `bootarg.init.switchless_cluster.enable`

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

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

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

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

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

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

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 - FAS9500

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

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

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

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

Si votre système dispose de...	Alors...
Une connexion réseau	<ol style="list-style-type: none"> a. Appuyez sur <code>y</code> lorsque vous êtes invité à restaurer la configuration de sauvegarde. b. Appuyez sur <code>y</code> lorsque vous êtes invité à remplacer <code>/etc/ssh/ssh_host_ecdsa_key</code>. c. Appuyez sur <code>y</code> lorsque vous êtes invité à confirmer si la restauration de la sauvegarde a réussi. d. Appuyez sur <code>y</code> lorsque vous êtes invité à restaurer la copie de configuration. e. Définissez le nœud sain sur le niveau de privilège avancé : <code>set -privilege advanced</code> f. Exécutez la commande <code>restore backup : system node restore-backup -node local -target-address impaired_node_IP_address</code> g. Renvoyer le nœud au niveau admin : <code>set -privilege admin</code> h. Appuyez sur <code>y</code> lorsque vous êtes invité à utiliser la configuration restaurée. i. Appuyez sur <code>y</code> lorsque vous êtes invité à redémarrer le nœud.
Aucune connexion réseau	<ol style="list-style-type: none"> a. Appuyez sur <code>n</code> 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. <p>Si vous êtes invité à poursuivre la mise à jour, appuyez sur <code>y</code>.</p>

Si votre système dispose de...	Alors...
Aucune connexion réseau et se trouve dans une configuration IP de MetroCluster	<p>a. Appuyez sur n lorsque vous êtes invité à restaurer la configuration de sauvegarde.</p> <p>b. Redémarrez le système à l'invite du système.</p> <p>c. Attendez que les connexions de stockage iSCSI se connectent.</p> <p>Vous pouvez continuer après avoir affiché les messages suivants :</p> <div data-bbox="670 459 1489 1325" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> 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).</pre> </div> <p>d. Sélectionnez l'option mettre à jour Flash dans Backup config (Sync flash) dans le menu affiché.</p> <p>Si vous êtes invité à poursuivre la mise à jour, appuyez sur y.</p>

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 `saveenv` commande.
5. Le suivant dépend de la configuration de votre système :

- Si keymanager, NSE ou NVE intégré est configuré sur votre système, rendez-vous sur [Étapes de remplacement des supports après démarrage pour OKM, NSE et NVE](#)
- Si keymanager, NSE ou NVE intégré ne sont pas configurés sur votre système, effectuez les étapes de cette section.

6. Dans l'invite DU CHARGEUR, entrez le `boot_ontap` commande.

Si vous voyez...	Alors...
Invite de connexion	Passez 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 <code>storage failover show</code> commande.

- Connectez le câble de la console au nœud partenaire.
- Renvoyer le nœud à l'aide du `storage failover giveback -fromnode local` commande.
- 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.

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

Restaurer le chiffrement - FAS9500

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>Sélectionnez l'option 10.</p> <p>Affiche un exemple de menu de démarrage</p> <div> <pre> 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 </pre> </div>

Version ONTAP	Sélectionnez cette option
ONTAP 9.7 et versions antérieures	<p>Sélectionnez l'option cachée <code>recover_onboard_keymanager</code></p> <p>Affiche un exemple de menu de démarrage</p> <div> <pre> 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-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----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/knip/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-----
<certificate_value>
-----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-----
<certificate_value>
-----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
```

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....
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. Restaurez le rétablissement automatique si vous l'avez désactivé.

```
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
```

Renvoyez la pièce défectueuse à NetApp - FAS9500

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 DÉLICTELLE (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.