



## **Support de démarrage**

Install and maintain

NetApp  
April 19, 2024

This PDF was generated from [https://docs.netapp.com/fr-fr/ontap-systems/asa900/bootmedia\\_replace\\_overview.html](https://docs.netapp.com/fr-fr/ontap-systems/asa900/bootmedia_replace_overview.html) on April 19, 2024. Always check docs.netapp.com for the latest.

# Sommaire

- Support de démarrage ..... 1
  - Remplacer le support de démarrage - ASA A900 ..... 1
  - Contrôles avant arrêt pour les clés de chiffrement intégrées - ASA A900 ..... 1
  - Arrêter le contrôleur défectueux - ASA A900 ..... 5
  - Remplacer le support de démarrage - ASA A900 ..... 8
  - Démarrer l'image de restauration - ASA A900 ..... 13
  - Étapes de remplacement des supports après démarrage pour OKM, NSE et NVE - ASA A900..... 16
  - Renvoyer la pièce défectueuse à NetApp - ASA A900..... 20

# Support de démarrage

## Remplacer le support de démarrage - ASA A900

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 contrôleur approprié :
  - Le contrôleur *trouble* est le contrôleur sur lequel vous effectuez la maintenance.
  - Le contrôleur *Healthy* est le partenaire HA du contrôleur déficient.

## Contrôles avant arrêt pour les clés de chiffrement intégrées - ASA A900

Avant d'arrêter le contrôleur défaillant et de vérifier l'état des clés de chiffrement intégrées, vous devez vérifier l'état du contrôleur défaillant, désactiver le rétablissement automatique et vérifier quelle version de ONTAP s'exécute sur le système.

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

### Étapes

1. Vérifier l'état du contrôleur détérioré :
  - Si le contrôleur douteux se trouve à l'invite de connexion, connectez-vous en tant que `admin`.
  - Si le contrôleur associé est au niveau de l'invite DU CHARGEUR et qu'il fait partie de la configuration HA, connectez-vous en tant que `admin` sur le contrôleur sain.
  - Si le contrôleur douteux se trouve dans une configuration autonome et à l'invite DU CHARGEUR,

contactez "[mysupport.netapp.com](https://mysupport.netapp.com)".

2. Si AutoSupport est activé, supprimez la création automatique de dossier en invoquant un message

```
AutoSupport:system node autosupport invoke -node * -type all -message  
MAINT=number_of_hours_downh
```

Le message AutoSupport suivant supprime la création automatique de dossiers pendant deux heures :

```
cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h
```

3. Vérifiez la version de ONTAP que le système fonctionne sur le contrôleur défaillant, si c'est le cas, ou sur le contrôleur partenaire si le contrôleur défaillant est en panne, à l'aide du `version -v` commande :
  - Si `<lno-DARE>` ou `<1Ono-DARE>` s'affiche dans la sortie de la commande, le système ne prend pas en charge NVE, procédez à l'arrêt du contrôleur.

## ONTAP 9.6 et versions ultérieures

Avant d'arrêter le contrôleur défaillant, vérifiez si NetApp Volume Encryption (NVE) ou NetApp Storage Encryption (NSE) sont activés sur le système. Si c'est le cas, vous devez vérifier la configuration.

1. Vérifiez que NVE est utilisé pour n'importe quel volume du cluster : `volume show -is-encrypted true`

Si des volumes sont répertoriés dans le résultat, NVE est configuré et vous devez vérifier la configuration NVE. Si aucun volume n'est indiqué, vérifiez si NSE est configuré et utilisé.

2. Vérifiez si NSE est configuré et utilisé : `storage encryption disk show`
  - Si le résultat de la commande répertorie les détails du disque avec les informations relatives au mode et à l'ID de clé, NSE est configuré et vous devez vérifier la configuration NSE et son utilisation.
  - Si aucun disque n'est affiché, NSE n'est pas configuré.
  - Si NVE et NSE ne sont pas configurés, aucun disque n'est protégé avec les clés NSE, vous pouvez arrêter le contrôleur pour facultés affaiblies.

## Vérifiez la configuration NVE

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager key query`



Après la version ONTAP 9.6, il est possible que vous ayez d'autres types de gestionnaire de clés. Les types sont KMIP, AKV, et GCP. Le processus de confirmation de ces types est identique à celui de la confirmation `external` ou `onboard` types de gestionnaire de clés.

- Si le Key Manager affichage du type `external` et le `Restored` s'affiche `yes`, il est sûr d'arrêter le contrôleur défaillant.
- Si le Key Manager affichage du type `onboard` et le `Restored` s'affiche `yes`, vous devez effectuer quelques étapes supplémentaires.
- Si le Key Manager affichage du type `external` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.
- Si le Key Manager affichage du type `onboard` et le `Restored` colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.

2. Si le Key Manager affichage du type onboard et le Restored s'affiche yes, Sauvegardez manuellement les informations OKM :
  - a. Accédez au mode de privilège avancé et entrez y lorsque vous êtes invité à continuer : `set -priv advanced`
  - b. Entrez la commande pour afficher les informations de gestion des clés : `security key-manager onboard show-backup`
  - c. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.
  - d. Revenir en mode admin: `set -priv admin`
  - e. Arrêtez le contrôleur défaillant.

3. Si le Key Manager affichage du type external et le Restored colonne affiche tout autre élément que yes:

- a. Restaurer les clés d'authentification externe de gestion des clés sur tous les nœuds du cluster : `security key-manager external restore`

Si la commande échoue, contactez le support NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Vérifiez que le Restored colonne égale à yes pour toutes les clés d'authentification : `security key-manager key query`

- b. Arrêtez le contrôleur défaillant.

4. Si le Key Manager affichage du type onboard et le Restored colonne affiche tout autre élément que yes:

- a. Entrez la commande de synchronisation du gestionnaire de clés de sécurité intégré : `security key-manager onboard sync`



Saisissez la phrase de passe alphanumérique de gestion des clés intégrée de 32 caractères du client à l'invite. Si cette phrase secrète ne peut pas être fournie, contactez le support NetApp. ["mysupport.netapp.com"](https://mysupport.netapp.com)

- b. Vérifiez le Restored affiche la colonne yes pour toutes les clés d'authentification : `security key-manager key query`

- c. Vérifiez que le Key Manager s'affiche onboard, Puis sauvegardez manuellement les informations OKM.

- d. Accédez au mode de privilège avancé et entrez y lorsque vous êtes invité à continuer : `set -priv advanced`

- e. Entrez la commande pour afficher les informations de sauvegarde de la gestion des clés : `security key-manager onboard show-backup`

- f. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.

- g. Revenir en mode admin: `set -priv admin`

h. Vous pouvez arrêter le contrôleur en toute sécurité.

## Vérifiez la configuration NSE

1. Afficher les ID de clé des clés d'authentification stockées sur les serveurs de gestion des clés : `security key-manager key query -key-type NSE-AK`



Après la version ONTAP 9.6, il est possible que vous ayez d'autres types de gestionnaire de clés. Les types sont KMIP, AKV, et GCP. Le processus de confirmation de ces types est identique à celui de la confirmation `external` ou `onboard` types de gestionnaire de clés.

- Si le Key Manager affichage du type `external` et le Restored s'affiche `yes`, il est sûr d'arrêter le contrôleur défaillant.
  - Si le Key Manager affichage du type `onboard` et le Restored s'affiche `yes`, vous devez effectuer quelques étapes supplémentaires.
  - Si le Key Manager affichage du type `external` et le Restored colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.
  - Si le Key Manager affichage du type `external` et le Restored colonne affiche tout autre élément que `yes`, vous devez effectuer quelques étapes supplémentaires.
2. Si le Key Manager affichage du type `onboard` et le Restored s'affiche `yes`, Sauvegardez manuellement les informations OKM :
    - a. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
    - b. Entrez la commande pour afficher les informations de gestion des clés : `security key-manager onboard show-backup`
    - c. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.
    - d. Revenir en mode admin: `set -priv admin`
    - e. Vous pouvez arrêter le contrôleur en toute sécurité.
  3. Si le Key Manager affichage du type `external` et le Restored colonne affiche tout autre élément que `yes`:
    - a. Restaurer les clés d'authentification externe de gestion des clés sur tous les nœuds du cluster : `security key-manager external restore`  
  
Si la commande échoue, contactez le support NetApp.  
  
["mysupport.netapp.com"](https://mysupport.netapp.com)
    - a. Vérifiez que le Restored colonne égale à `yes` pour toutes les clés d'authentification : `security key-manager key query`
    - b. Vous pouvez arrêter le contrôleur en toute sécurité.
  4. Si le Key Manager affichage du type `onboard` et le Restored colonne affiche tout autre élément que `yes`:

- a. Entrez la commande de synchronisation du gestionnaire de clés de sécurité intégré : `security key-manager onboard sync`

Saisissez la phrase de passe alphanumérique de gestion des clés intégrée de 32 caractères du client à l'invite. Si cette phrase secrète ne peut pas être fournie, contactez le support NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Vérifiez le Restored affiche la colonne `yes` pour toutes les clés d'authentification : `security key-manager key query`
- b. Vérifiez que le Key Manager s'affiche `onboard`, Puis sauvegardez manuellement les informations OKM.
- c. Accédez au mode de privilège avancé et entrez `y` lorsque vous êtes invité à continuer : `set -priv advanced`
- d. Entrez la commande pour afficher les informations de sauvegarde de la gestion des clés : `security key-manager onboard show-backup`
- e. Copiez le contenu des informations de sauvegarde dans un fichier distinct ou dans votre fichier journal. Dans les scénarios d'incident, vous devrez peut-être restaurer manuellement le gestionnaire de clés intégré OKM.
- f. Revenir en mode admin: `set -priv admin`
- g. Vous pouvez arrêter le contrôleur en toute sécurité.

## Arrêter le contrôleur défectueux - ASA A900

Arrêtez ou prenez le contrôleur défaillant en suivant la procédure appropriée pour votre configuration.

## La plupart des configurations

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

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 la lame SCSI du contrôleur altérée. Le `cluster kernel-service show` commande affiche le nom du nœud, l'état quorum du nœud concerné, l'état de disponibilité de ce nœud et 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 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`



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.



Si le contrôleur en état de fonctionnement s'affiche...	Alors...
Invite système ou invite de mot de passe	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> .

### Le contrôleur réside dans un MetroCluster

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



N'utilisez pas cette procédure si votre système se trouve dans une configuration MetroCluster à deux nœuds.

Pour arrêter le contrôleur défaillant, vous devez déterminer l'état du contrôleur et, si nécessaire, prendre le contrôle de façon à ce que le contrôleur en bonne santé continue de transmettre des données provenant du stockage défaillant du contrôleur.

- Si vous avez un cluster avec plus de deux nœuds, il doit être dans le quorum. Si le cluster n'est pas au quorum ou si un contrôleur en bonne santé affiche la valeur false pour l'éligibilité et la santé, vous devez corriger le problème avant de désactiver le contrôleur défaillant ; voir "[Synchroniser un nœud avec le cluster](#)".
- Si vous disposez d'une configuration MetroCluster, vous devez avoir confirmé que l'état de configuration MetroCluster est configuré et que les nœuds sont dans un état activé et normal (`metrocluster node show`).

### Étapes

1. Si AutoSupport est activé, supprimez la création automatique de dossier en invoquant un message `AutoSupport:system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

Le message AutoSupport suivant supprime la création automatique de dossiers pendant deux heures : `cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Désactiver le rétablissement automatique depuis la console du contrôleur sain : `storage failover modify -node local -auto-giveback false`
3. Faites passer le contrôleur douteux à l'invite DU CHARGEUR :

Si le contrôleur en état de fonctionnement s'affiche...	Alors...
Invite DU CHARGEUR	Passez à l'étape suivante.
Attente du retour...	Appuyez sur Ctrl-C, puis répondez <code>y</code> lorsque vous y êtes invité.

Si le contrôleur en état de fonctionnement s'affiche...	Alors...
Invite système ou invite de mot de passe (entrer le mot de passe système)	Prendre le contrôle défectueux ou l'arrêter à partir du contrôleur en bon état : <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> .

## Remplacer le support de démarrage - ASA A900

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 contrôleur](#)



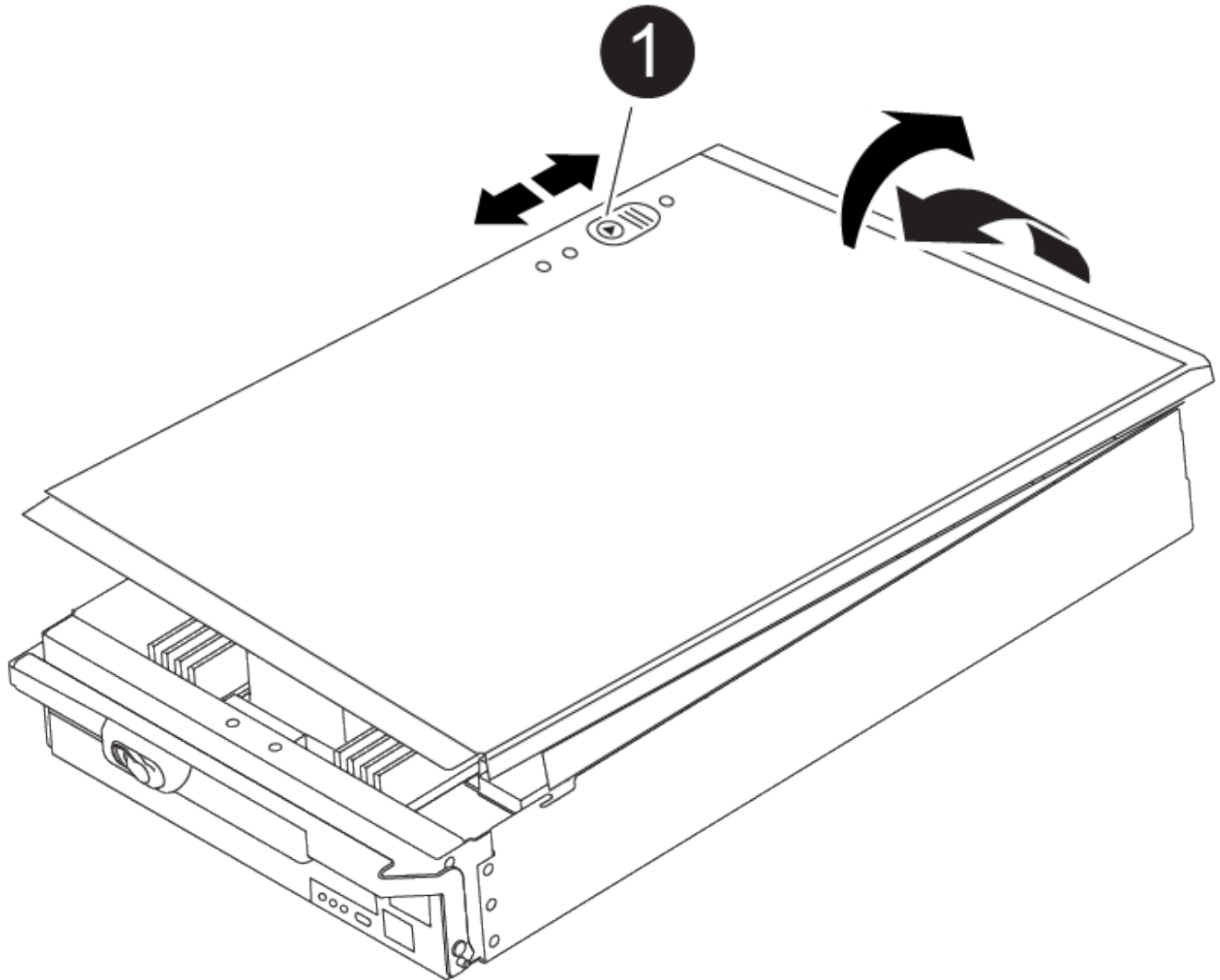
1	Bouton de déverrouillage de la poignée de came
2	Poignée de came

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.
- 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 système de fichiers var au cours de 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 contrôleur 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 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.

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

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



Le port cible que vous configurez est le port cible que vous utilisez pour communiquer avec le contrôleur doteux 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 e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
  - Filer\_addr est l'adresse IP du système de stockage.
  - Le masque de réseau est le masque de réseau du réseau de gestion connecté au partenaire haute disponibilité.
  - passerelle est la passerelle du réseau.
  - dns\_addr est l'adresse IP d'un serveur de noms sur votre réseau.
  - dns\_Domain est le nom de domaine DNS (Domain Name System).

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



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

7. Si le contrôleur est en mode MetroCluster Stretch ou Fabric-Attached, vous devez restaurer la configuration de l'adaptateur FC :
  - a. Démarrage en mode maintenance : `boot_ontap maint`
  - b. Définissez les ports MetroCluster comme initiateurs : `ucadmin modify -m fc -t initiator adapter_name`
  - c. Arrêter pour revenir en mode maintenance : `halt`

Les modifications seront mises en œuvre au démarrage du système.

## Démarrer l'image de restauration - ASA A900

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	<ul style="list-style-type: none"> <li>a. Appuyez sur <code>y</code> lorsque vous êtes invité à restaurer la configuration de sauvegarde.</li> <li>b. Appuyez sur <code>y</code> lorsque vous êtes invité à remplacer <code>/etc/ssh/ssh_host_ecdsa_key</code>.</li> <li>c. Appuyez sur <code>y</code> lorsque vous êtes invité à confirmer si la restauration de la sauvegarde a réussi.</li> <li>d. Appuyez sur <code>y</code> lorsque vous êtes invité à restaurer la copie de configuration.</li> <li>e. Réglez le contrôleur pour personnes atteintes sur le niveau de privilège avancé : <code>set -privilege advanced</code></li> <li>f. Exécutez la commande <code>restore backup</code> : <code>system node restore-backup -node local -target-address impaired_node_IP_address</code></li> <li>g. Remettre le contrôleur affecté au niveau admin : <code>set -privilege admin</code></li> <li>h. Appuyez sur <code>y</code> lorsque vous êtes invité à utiliser la configuration restaurée.</li> <li>i. Appuyez sur <code>y</code> lorsque vous êtes invité à redémarrer le contrôleur douteux.</li> </ul>
Aucune connexion réseau	<ul style="list-style-type: none"> <li>a. Appuyez sur <code>n</code> lorsque vous êtes invité à restaurer la configuration de sauvegarde.</li> <li>b. Redémarrez le système à l'invite du système.</li> <li>c. Sélectionnez l'option <b>mettre à jour Flash dans Backup config</b> (Sync flash) dans le menu affiché.</li> </ul> <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 <b>n</b> 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> <pre data-bbox="672 459 1489 1325"> 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> <p>d. Sélectionnez l'option <b>mettre à jour Flash dans Backup config</b> (Sync flash) dans le menu affiché.</p> <p>Si vous êtes invité à poursuivre la mise à jour, appuyez sur <b>y</b>.</p>

4. Assurez-vous que les variables environnementales sont définies comme prévu :
  - a. Prenez le contrôleur pour facultés affaiblies jusqu'à l'invite DU CHARGEUR.
  - b. Vérifiez les paramètres de la variable d'environnement à l'aide de la commande `printenv`.
  - c. Si une variable d'environnement n'est pas définie comme prévu, modifiez-la à l'aide de la commande `setenv Environment_variable_name changed_value`.
  - d. Enregistrez vos modifications à l'aide de la commande `saveenv`.
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 la commande `boot_ontap`.

Si vous voyez...	Alors...
Invite de connexion	Passer à l'étape suivante.
Attente du retour...	<ul style="list-style-type: none"><li>a. Connectez-vous au contrôleur partenaire.</li><li>b. Vérifiez que la cible est prête pour le rétablissement avec le <code>storage failover show</code> commande.</li></ul>

7. Branchez le câble de la console au contrôleur partenaire.

8. Renvoyer le contrôleur à l'aide de la commande locale `Storage failover giveback -fromnode`.

9. À l'invite du cluster, vérifiez les interfaces logiques avec la commande `net int -is-home false`.

Si des interfaces sont répertoriées comme « FALSE », rrestaurez ces interfaces à leur port d'origine à l'aide de la commande `net int revert`.

10. Placez le câble de la console sur l'arrêt réparé ou prenez le contrôle avec facultés affaiblies en suivant la procédure adéquate pour votre configuration. Et exécutez la commande `version -v` pour vérifier les versions de ONTAP.

11. Restaurez le rétablissement automatique si vous le avez désactivé à l'aide de la commande `Storage Failover modify -node local -auto-giveback true`.

## Étapes de remplacement des supports après démarrage pour OKM, NSE et NVE - ASA A900

Une fois les variables d'environnement vérifiées, vous devez effectuer les étapes spécifiques de restauration du gestionnaire de clés intégré (OKM), du chiffrement de stockage NetApp (NSE) et du chiffrement de volume NetApp (NVE).

Déterminez la section à utiliser pour restaurer vos configurations OKM, NSE ou NVE : si NSE ou NVE sont activés avec Onboard Key Manager, vous devez restaurer les paramètres que vous avez capturés au début de cette procédure.

- Si NSE ou NVE sont activés et que le gestionnaire de clés intégré est activé, rendez-vous sur [Restaurez NVE ou NSE lorsque le gestionnaire de clés intégré est activé](#).
- Si NSE ou NVE sont activés pour ONTAP 9.6, rendez-vous sur le site [Restaurez NSE/NVE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures](#).

### Restaurez NVE ou NSE lorsque le gestionnaire de clés intégré est activé

1. Branchez le câble de la console au contrôleur cible.
2. Utilisez la commande `boot_ontap` à l'invite DU CHARGEUR pour démarrer le contrôleur.
3. Vérifiez la sortie de la console :

Si la console affiche...	Alors...
Invite DU CHARGEUR	Démarrer le contrôleur sur le menu de démarrage : <code>boot_ontap</code> menu
En attente de retour	a. Entrez <code>Ctrl-C</code> à l'invite b. Dans le message: Voulez-vous arrêter ce nœud plutôt que d'attendre [y/n] ? , entrez : <code>y</code> c. À l'invite DU CHARGEUR, entrez le <code>boot_ontap</code> menu commande.

4. Dans le menu de démarrage, entrez la commande masquée, `recover_onboard_keymanager`, et répondre `y` à l'invite.
5. Saisissez la phrase de passe du gestionnaire de clés intégré que vous avez obtenue du client au début de cette procédure.
6. Lorsque vous êtes invité à saisir les données de sauvegarde, collez les données de sauvegarde que vous avez saisies au début de cette section, lorsque vous y êtes invité. Coller la sortie de `security key-manager backup show` OU `security key-manager onboard show-backup` commande.



Les données sont issues de l'une ou l'autre `security key-manager backup show` ou de la commande `show-backup`» intégrée avec `security key-manager`.

Exemple de données de sauvegarde :

Entrez les données de sauvegarde :

```

----- COMMENCER LA SAUVEGARDE-----
TmV0QXBwIEtleSBCbG9AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAUAAUAAUAAUAAUAAUAAUAAUAAUAAU
UAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAA
AUAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAA
AAUZUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAAUAA
AAUAA . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----- FIN DE LA SAUVEGARDE-----

```

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

Le système démarre pour attendre l'invite de rétablissement...

8. Déplacez le câble de la console vers le contrôleur partenaire et connectez-vous en tant qu'administrateur.
9. Vérifiez que le contrôleur cible est prêt pour le rétablissement à l'aide du `storage failover show` commande.

10. Renvoyer uniquement les agrégats CFO avec le `storage failover giveback -fromnode local -only-cfo-aggregates true` commande.

- Si la commande échoue en raison d'un disque en panne, désengagez physiquement le disque en panne, mais laissez le disque dans le slot jusqu'à ce qu'un disque de remplacement soit reçu.
- Si la commande échoue en raison d'une session CIFS ouverte, vérifiez auprès du client comment fermer les sessions CIFS.



L'arrêt du protocole CIFS peut entraîner la perte de données.

- Si la commande échoue car le partenaire n'est pas prêt, attendez 5 minutes pour que les systèmes NVRAM se synchronisent.
- Si la commande échoue en raison d'un processus NDMP, SnapMirror ou SnapVault, désactivez le processus. Consultez le contenu approprié pour plus d'informations.

11. Une fois le retour terminé, vérifiez l'état du basculement et du rétablissement à l'aide du `storage failover show` et `storage failover show-giveback` commandes.

Seuls les agrégats CFO (agrégats racine et agrégats de données de type CFO) seront indiqués.

12. Si vous utilisez ONTAP 9.6 ou une version ultérieure, exécutez la synchronisation intégrée du gestionnaire de clés de sécurité :

- Exécutez le `security key-manager onboard sync` puis entrez la phrase de passe lorsque vous y êtes invité.
- Entrez le `security key-manager key-query` commande pour afficher une vue détaillée de toutes les clés stockées dans le gestionnaire de clés intégré et vérifier que `Restored` colonne = `yes/true` pour toutes les clés d'authentification.



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

- Attendez 10 minutes que la clé se synchronise sur l'ensemble du cluster.

13. Déplacez le câble de la console vers le contrôleur partenaire.

14. Renvoyer le contrôleur cible à l'aide du `storage failover giveback -fromnode local` commande.

15. Vérifier le statut de rétablissement, trois minutes après la fin des rapports, à l'aide de `storage failover show` commande.

Si le retour n'est pas effectué au bout de 20 minutes, contactez le support client.

16. À l'invite `clustershell`, entrez la commande `net int show -is-home false` pour lister les interfaces logiques qui ne sont pas sur leur contrôleur et port de départ.

Si des interfaces sont répertoriées comme `false`, re restaurez ces interfaces sur leur port de départ à l'aide de la commande `net int revert`.

17. Déplacer le câble de la console vers le contrôleur cible et exécuter le `version -v` Commande pour vérifier les versions de ONTAP.

18. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

## Restaurez NSE/NVE sur les systèmes qui exécutent ONTAP 9.6 et versions ultérieures

1. Branchez le câble de la console au contrôleur cible.
2. Utilisez la commande `boot_ontap` à l'invite DU CHARGEUR pour démarrer le contrôleur.
3. Vérifiez la sortie de la console :

Si la console affiche...	Alors...
Invite de connexion	Passez à l'étape 7.
Attente du retour...	<ol style="list-style-type: none"><li>a. Connectez-vous au contrôleur partenaire.</li><li>b. Vérifiez que le contrôleur cible est prêt pour le rétablissement à l'aide du <code>storage failover show</code> commande.</li></ol>

4. Déplacez le câble de la console vers le contrôleur partenaire et redonnez le stockage du contrôleur cible à l'aide de la commande `Storage failover giveback -fromnode local -only-cfo-Aggregates` véritable commande locale.
  - Si la commande échoue en raison d'un disque en panne, désengagez physiquement le disque en panne, mais laissez le disque dans le slot jusqu'à ce qu'un disque de remplacement soit reçu.
  - Si la commande échoue en raison d'une session CIFS ouverte, vérifiez auprès du client comment fermer les sessions CIFS.



L'arrêt du protocole CIFS peut entraîner la perte de données.

- Si la commande échoue parce que le partenaire n'est pas prêt, attendez 5 minutes pour que le système NVMEMs se synchronise.
  - Si la commande échoue en raison d'un processus NDMP, SnapMirror ou SnapVault, désactivez le processus. Consultez le contenu approprié pour plus d'informations.
5. Attendez 3 minutes et vérifiez l'état du basculement à l'aide de la commande `Storage failover show`.
  6. À l'invite `clustershell`, entrez le `net int show -is-home false` commande pour lister les interfaces logiques qui ne se trouvent pas sur leur contrôleur et son port de base.

Si des interfaces sont répertoriées comme `false`, restaurez ces interfaces à leur port de départ à l'aide de l'`net int revert` commande.

7. Déplacer le câble de la console vers le contrôleur cible et exécuter le `version -v` Commande pour vérifier les versions de ONTAP.
8. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.
9. Utilisez le `storage encryption disk show` à l'invite `clustershell`, pour vérifier la sortie.
10. Utilisez le `security key-manager key-query` commande pour afficher les clés de chiffrement et d'authentification stockées sur les serveurs de gestion des clés.
  - Si le `Restored` colonne = `yes/true`, vous avez terminé et pouvez procéder à la procédure de remplacement.

- Si le `Key Manager type = external` et le `Restored` colonne = tout autre élément que `yes/true`, Utilisez la commande de restauration externe du gestionnaire de clés de sécurité pour restaurer les ID de clés des clés d'authentification.



Si la commande échoue, contactez l'assistance clientèle.

- Si le `Key Manager type = onboard` et le `Restored` colonne = tout autre élément que `yes/true`, Utilisez la commande de synchronisation intégrée du gestionnaire de clés de sécurité pour resynchroniser le type de gestionnaire de clés.

Utilisez le `security key-manager key-query` pour vérifier que le `Restored` colonne = `yes/true` pour toutes les clés d'authentification.

11. Branchez le câble de la console au contrôleur partenaire.
12. Renvoyer le contrôleur à l'aide de la commande locale `Storage failover giveback -fromnode`.
13. Restaurez le retour automatique si vous le désactivez à l'aide de `storage failover modify -node local -auto-giveback true` commande.

## Renvoyer la pièce défectueuse à NetApp - ASA A900

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

## Informations sur le copyright

Copyright © 2024 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.