



Étape 6. Démarrez le nœud 2 avec les modules système de remplacement

Upgrade controllers

NetApp
February 22, 2024

Sommaire

- Étape 6. Démarrez le nœud 2 avec les modules système de remplacement 1
 - Présentation 1
 - Démarrez le nœud 2 avec les modules système de remplacement 1
 - Vérifiez l'installation du node2 6
 - Restaurez la configuration du gestionnaire de clés sur le noeud 2 10
 - Déplacement des agrégats non racines et des LIF de données NAS vers le nœud 2 11

Étape 6. Démarrez le nœud 2 avec les modules système de remplacement

Présentation

Au cours de l'étape 6, vous démarrez node2 avec des modules système mis à niveau et vérifiez l'installation du node2 mis à niveau. Si vous utilisez NetApp Volume Encryption (NVE), vous restaurez la configuration du gestionnaire de clés. Vous pouvez également transférer des agrégats non racines et des LIF de données NAS du nœud 1 vers le nœud 2 mis à niveau, puis vérifier que des LIF SAN existent sur le nœud 2.

1. ["Démarrez le nœud 2 avec les modules système de remplacement"](#)
2. ["Vérifiez l'installation du node2"](#)
3. ["Restaurez la configuration du gestionnaire de clés sur le nœud 2"](#)
4. ["Déplacement des agrégats non racines et des LIF de données NAS vers le nœud 2"](#)

Démarrez le nœud 2 avec les modules système de remplacement

Le nœud 2 avec les modules de remplacement est maintenant prêt à démarrer. La mise à niveau par permutation des modules système implique de déplacer uniquement la console et les connexions de gestion. Cette section fournit les étapes requises pour démarrer node2 avec les modules de remplacement pour les configurations de mise à niveau suivantes :

Ancien contrôleur de nœud 2	Remplacement des modules système du nœud 2
AFF A220 configuré en tant que ASA	Module de contrôleur A150 ASA
AVEC AFF A220 Solution AFF A200 Baie AFF C190	Module de contrôleur A150 AFF
FAS2620 FAS2720	Module de contrôleur FAS2820
AFF A700 configuré en tant que ASA	Contrôleur ASA A900 et modules NVRAM
AFF A700	Contrôleur AFF A900 et modules NVRAM
FAS9000	Contrôleur FAS9500 et modules NVRAM

Étapes

1. si des disques NetApp Storage Encryption (NSE) sont installés, effectuez les opérations suivantes.



Si ce n'est déjà fait, consultez l'article de la base de connaissances ["Comment savoir si un disque est certifié FIPS"](#) déterminer le type de disques à autocryptage utilisés.

a. Réglez `bootarg.storageencryption.support` à `true` ou `false`:

Si les lecteurs suivants sont utilisés...	Puis...
Disques NSE conformes aux exigences de chiffrement automatique FIPS 140-2 de niveau 2	<code>setenv bootarg.storageencryption.support true</code>
NetApp non-SED FIPS	<code>setenv bootarg.storageencryption.support false</code>



Vous ne pouvez pas combiner des disques FIPS avec d'autres types de disques sur le même nœud ou la même paire HA. Vous pouvez utiliser les disques SED avec des disques sans cryptage sur le même nœud ou une paire haute disponibilité.

b. Accédez au menu de démarrage spécial et sélectionnez option (10) Set Onboard Key Manager recovery secrets.

Saisissez la phrase de passe et les informations de sauvegarde que vous avez enregistrées lors de la procédure précédente. Voir "[Gérez le chiffrement du stockage à l'aide du gestionnaire de clés intégré](#)".

2. Démarrez le nœud dans le menu de démarrage :

```
boot_ontap menu
```

3. Réaffectez les anciens disques du nœud 2 au nœud de remplacement 2 en entrant « 22/7 » et en sélectionnant l'option cachée `boot_after_controller_replacement` lorsque le nœud s'arrête au menu de démarrage.

Après un bref délai, vous êtes invité à saisir le nom du nœud en cours de remplacement. S'il existe des disques partagés (également appelés partitionnement de disque avancé ou des disques partitionnés), vous êtes invité à saisir le nom de nœud du partenaire haute disponibilité.

Ces invites peuvent être enfouies dans les messages de la console. Si vous ne saisissez pas de nom de nœud ou si vous saisissez un nom incorrect, vous êtes invité à saisir de nouveau le nom.

```
Si [localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified
encrypting drive et, ou, [localhost:diskown.errorDuringIO:error]: error
3 (disk failed) on disk des erreurs se produisent, effectuez les opérations
suivantes :
```



- Arrêtez le nœud à l'invite DU CHARGEUR.
- Vérifiez et réinitialisez les bootargs de cryptage de stockage mentionnés dans [Étape 1](#).
- À l'invite du chargeur, démarrez :

```
boot_ontap
```

Vous pouvez utiliser l'exemple suivant comme référence :

Développez l'exemple de sortie de la console

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
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)? 22/7

(22/7)                                Print this secret List
(25/6)                                Force boot with multiple filesystem
disks missing.
(25/7)                                Boot w/ disk labels forced to clean.
(29/7)                                Bypass media errors.
(44/4a)                               Zero disks if needed and create new
flexible root volume.
(44/7)                                Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                          Clean all configuration on boot
```

```

device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)          Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.

```

The boot device has changed. System configuration information could be lost. Use option (6) to restore the system configuration, or option (4) to initialize all disks and setup a new system. Normal Boot is prohibited.

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)? boot_after_controller_replacement

```

This will replace all flash-based configuration with the last backup to disks. Are you sure you want to continue?: yes

```

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id

```

```

= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...

.
System rebooting...

.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:

```



Les ID système affichés dans l'exemple précédent sont des exemples d'ID. Les ID système réels des nœuds que vous mettez à niveau seront différents.

Entre la saisie des noms de nœud à l'invite et à l'invite de connexion, le nœud redémarre plusieurs fois pour restaurer les variables d'environnement, mettre à jour le firmware sur les cartes du système et pour d'autres mises à jour de ONTAP.

Vérifiez l'installation du nœud2

Vous devez vérifier l'installation du nœud 2 avec les modules système de remplacement. Comme il n'y a pas de modification des ports physiques, vous n'avez pas besoin d' mapper les ports physiques de l'ancien nœud 2 vers le nœud de remplacement 2.

Description de la tâche

Après avoir initialisé le nœud 1 avec le module système de remplacement, vérifiez qu'il est correctement installé. Vous devez patienter jusqu'à ce que le nœud 2 rejoigne le quorum, puis reprendre l'opération de remplacement du contrôleur.

À ce stade de la procédure, l'opération s'interrompt pendant que le nœud 2 rejoint le quorum.

Étapes

1. Vérifiez que le nœud 2 a rejoint le quorum :

```
cluster show -node node2 -fields health
```

La sortie du `health` ce champ doit être de `true`.

2. Vérifiez que le nœud 2 fait partie du même cluster que le nœud 1 et qu'il est en bon état :

```
cluster show
```

3. Passer en mode privilège avancé :

```
set advanced
```

4. Vérifier l'état de l'opération de remplacement du contrôleur et vérifier qu'elle est en pause et dans le même état qu'avant l'arrêt du nœud 2 pour effectuer les tâches physiques liées à l'installation de nouveaux contrôleurs et au déplacement des câbles :

```
system controller replace show
```

```
system controller replace show-details
```

5. Reprendre l'opération de remplacement du contrôleur :

```
system controller replace resume
```

6. L'opération de remplacement du contrôleur s'interrompt pour une intervention et affiche le message suivant :


```
Cluster::*> system controller replace show
```

Node	Status	Error-Action
Node2	Paused-for-intervention	Follow the instructions given in
Node1	None	Step Details

Step Details:

To complete the Network Reachability task, the ONTAP network configuration must be manually adjusted to match the new physical network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For detailed commands and instructions, refer to the "Re-creating VLANs, ifgrps, and broadcast domains" section of the upgrade controller hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-replacement network displaced-vlans restore" to restore the VLAN on the desired port.

2 entries were displayed.



Dans cette procédure, la section *Re-cr ation de VLAN, ifgrps et broadcast domain* a  t  renomm e *Restore network configuration sur node2*.

7. Lorsque le remplacement du contr leur est en pause, passer   [Restaurez la configuration r seau sur le n ud 2](#).

Restaurez la configuration r seau sur le n ud 2

Une fois que vous avez confirm  que le n ud2 est dans le quorum et peut communiquer avec le n ud1, v rifiez que les VLAN, les groupes d'interface et les domaines de diffusion du n ud1 sont visibles sur le n ud2. V rifiez  galement que tous les ports r seau du node2 sont configur s dans leurs domaines de diffusion appropri s.

Description de la t che

Pour plus d'informations sur la cr ation et la recr ation de VLAN, de groupes d'interfaces et de domaines de diffusion, reportez-vous   la section "[R f rences](#)" Pour cr er un lien vers le contenu *Network Management*.

 tapes

1. Lister tous les ports physiques qui se trouvent sur le n ud mis   niveau 2 :

```
network port show -node node2
```

Tous les ports réseau physique, les ports VLAN et les ports de groupe d'interfaces sur le nœud sont affichés. À partir de cette sortie, vous pouvez voir tous les ports physiques qui ont été déplacés dans le Cluster Broadcast domain par ONTAP. Vous pouvez utiliser cette sortie pour décider des ports à utiliser comme ports membres de groupe d'interface, ports de base VLAN ou ports physiques autonomes pour l'hébergement des LIFs.

2. Lister les rebroadcast domain sur le cluster :

```
network port broadcast-domain show
```

3. Lister la possibilité de port réseau de tous les ports du node2 :

```
network port reachability show -node node2
```

Vous devez voir des valeurs de sortie similaires à l'exemple suivant. Les noms de port et de diffusion varient.

```
Cluster::*> network port reachability show -node local
```

Node	Port	Expected Reachability	Reachability

Node2			
	e0M	Default:Mgmt	no-reachability
	e10a	Default:Default-3	ok
	e10b	Default:Default-4	ok
	e11a	Cluster:Cluster	no-reachability
	e11b	Cluster:Cluster	no-reachability
	e11c	-	no-reachability
	e11d	-	no-reachability
	e2a	Default:Default-1	ok
	e2b	Default:Default-2	ok
	e9a	Default:Default	no-reachability
	e9b	Default:Default	no-reachability
	e9c	Default:Default	no-reachability
	e9d	Default:Default	no-reachability

13 entries were displayed.

Dans l'exemple précédent, le nœud 2 a démarré et a rejoint le quorum après le remplacement du contrôleur. Il dispose de plusieurs ports qui n'ont pas d'accessibilité et sont en attente d'une acquisition de capacité de remboursement.

4. réparer l'accessibilité pour chacun des ports du node2 avec un état de réabilité autre que ok en utilisant la commande suivante, dans l'ordre suivant :

```
network port reachability repair -node node_name -port port_name
```

- a. Ports physiques
- b. Ports VLAN

La sortie doit s'afficher comme dans l'exemple suivant :

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Un message d'avertissement, tel qu'illustré dans l'exemple précédent, est attendu pour les ports dont l'état d'accessibilité peut être différent de l'état d'accessibilité du domaine de diffusion où il se trouve actuellement. Vérifiez la connectivité du port et la réponse *y* ou *n* selon les besoins.

Vérifier que tous les ports physiques ont leur capacité d'accessibilité attendue :

```
network port reachability show
```

Au fur et à mesure que la réparation de l'accessibilité est effectuée, ONTAP tente de placer les ports dans les domaines de diffusion appropriés. Toutefois, si la capacité de réachabilité d'un port ne peut être déterminée et n'appartient à aucun des domaines de diffusion existants, ONTAP créera de nouveaux domaines de diffusion pour ces ports.

5. Vérifiez l'accessibilité des ports :

```
network port reachability show
```

Lorsque tous les ports sont correctement configurés et ajoutés aux domaines de diffusion appropriés, le `network port reachability show` la commande doit indiquer l'état de la capacité d'accessibilité `ok` pour tous les ports connectés et l'état en tant que `no-reachability` pour les ports sans connectivité physique. Si un port signale un état autre que ces deux, effectuez la réparation de la capacité d'accès et ajoutez ou supprimez des ports de leurs domaines de diffusion comme indiqué dans [Étape 4](#).

6. Vérifier que tous les ports ont été placés dans des domaines de diffusion :

```
network port show
```

7. Vérifiez que l'unité de transmission maximale (MTU) correcte est configurée pour tous les ports des domaines de diffusion :

```
network port broadcast-domain show
```

8. Restaurer les ports de base LIF, en précisant les ports de base Vserver et LIF, le cas échéant, à restaurer à l'aide des étapes suivantes :

- a. Lister les LIFs déplacées :

```
displaced-interface show
```

b. Restaurer les home node LIF et les ports home ports :

```
displaced-interface restore-home-node -node node_name -vserver vserver_name
-lif-name LIF_name
```

9. Vérifier que toutes les LIF disposent d'un port d'origine et sont administrativement en service :

```
network interface show -fields home-port,status-admin
```

Restaurez la configuration du gestionnaire de clés sur le nœud 2

Si vous utilisez NetApp Aggregate Encryption (NAE) ou NetApp Volume Encryption (NVE) pour chiffrer les volumes sur le système que vous mettez à niveau, la configuration de chiffrement doit être synchronisée avec les nouveaux nœuds. Si vous ne resynchroniser pas le gestionnaire de clés, lorsque vous transférez les agrégats du nœud 2 depuis le nœud mis à niveau 1 vers le nœud mis à niveau 2 à l'aide du transfert d'agrégats, des pannes peuvent se produire, car le nœud 2 ne dispose pas des clés de cryptage requises pour mettre en ligne les volumes et les agrégats chiffrés.

Description de la tâche

Synchronisez la configuration de cryptage avec les nouveaux nœuds en effectuant les étapes suivantes :

Étapes

1. Exécutez la commande suivante depuis le nœud 2 :

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

2. Vérifier que la clé SVM-KEK est restaurée sur « true » sur le nœud2 avant de transférer les agrégats de données :

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK
```

Exemple

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node2	svm1	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f00000000000000000

Déplacement des agrégats non racines et des LIF de données NAS vers le nœud 2

Après avoir vérifié la configuration réseau sur le nœud 2 et avant de déplacer des agrégats du nœud 1 vers le nœud 2, vérifiez que les LIF de données NAS appartenant au nœud 2 qui se trouvent actuellement sur le nœud 1 sont déplacées du nœud 1 vers le nœud 2. Vous devez également vérifier que les LIFs SAN existent sur le nœud 2.

Description de la tâche

Les LIF distantes gèrent le trafic vers des LUN SAN pendant la procédure de mise à niveau. Le déplacement des LIF SAN n'est pas nécessaire pour assurer l'intégrité du cluster ou du service pendant la mise à niveau. Les LIF SAN ne sont pas déplacées sauf si elles doivent être mappées sur de nouveaux ports. Une fois le nœud 2 mis en ligne, vous devez vérifier que les LIF sont saines et situées sur les ports appropriés.

Étapes

1. Reprendre l'opération de relocalisation :

```
system controller replace resume
```

Le système effectue les tâches suivantes :

- Vérification du quorum du cluster
- Vérification de l'ID système
- Vérification de la version d'image
- Vérification de la plate-forme cible
- Vérification de l'accessibilité du réseau

L'opération s'interrompt à cette étape de la vérification de la capacité d'accessibilité du réseau.

2. Reprendre l'opération de relocalisation :

```
system controller replace resume
```

Le système effectue les vérifications suivantes :

- Vérification de l'état du cluster
- Vérification de l'état de la LIF de cluster

Après ces vérifications, le système replace les agrégats non racines et les LIF de données NAS sur le nœud 2, qui s'exécute désormais sur le contrôleur de remplacement.

L'opération de remplacement du contrôleur s'interrompt une fois le transfert de ressources terminé.

3. Vérifier le statut du transfert d'agrégats et du déplacement des LIF de données NAS :

```
system controller replace show-details
```

Si la procédure de remplacement du contrôleur est suspendue, vérifiez et corrigez l'erreur, le cas échéant, puis faites-la `resume` pour poursuivre l'opération.

4. Si nécessaire, restaurez et restaurez les LIF déplacées. Lister les LIFs déplacées :

```
cluster controller-replacement network displaced-interface show
```

Si des LIF sont déplacées, restaurez le nœud de rattachement vers le nœud 2 :

```
cluster controller-replacement network displaced-interface restore-home-node
```

5. Reprenez l'opération pour demander au système d'effectuer les vérifications post-requises :

```
system controller replace resume
```

Le système effectue les vérifications suivantes :

- Vérification du quorum du cluster
- Vérification de l'état du cluster
- Vérification de la reconstruction d'agrégats
- Vérification de l'état de l'agrégat
- Vérification de l'état du disque
- Vérification de l'état de la LIF de cluster
- Vérification du volume

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.