



Étape 5. Installez et démarrez Node4

Upgrade controllers

NetApp
July 05, 2024

Sommaire

- Étape 5. Installez et démarrez Node4 1
 - Présentation de la phase 5 1
 - Installez et démarrez Node4 1
 - Vérifiez l'installation du node4 11
 - Restaurez la configuration du gestionnaire de clés sur le nœud 4 17
 - Déplacement des agrégats non racines et des LIF de données NAS qui appartiennent au nœud 2 du nœud 3 vers le nœud 4 18

Étape 5. Installez et démarrez Node4

Présentation de la phase 5

Lors de la phase 5, vous installez et démarrez le nœud 4, vérifiez que le cluster et les ports de gestion des nœuds du nœud 2 sont connectés sur le nœud 4, puis vérifiez l'installation du nœud 4. Si vous utilisez NVE, restaurez la configuration du gestionnaire de clés. Vous pouvez également transférer les LIF de données NAS du nœud 2 et les agrégats non racine du nœud 3 vers le nœud 4, puis vérifier que les LIF SAN existent sur le nœud 4.

Étapes

1. ["Installez et démarrez Node4"](#)
2. ["Vérifiez l'installation du node4"](#)
3. ["Restaurez la configuration du gestionnaire de clés sur le nœud 4"](#)
4. ["Déplacement des agrégats non racines et des LIF de données NAS qui appartiennent au nœud 2 du nœud 3 vers le nœud 4"](#)

Installez et démarrez Node4

Vous installez node4 dans le rack, transférez les connexions du node2 vers le node4, amorcez le node4 et installez ONTAP. Vous réaffectez ensuite l'un des disques de spare du nœud 2, tous les disques appartenant au volume racine et tous les agrégats non racines qui n'ont pas été déplacés vers le nœud 3 plus tôt dans le processus, comme indiqué dans cette section.

Description de la tâche

L'opération de déplacement est mise en pause au début de cette étape. Ce processus est principalement automatisé. L'opération s'interrompt pour vous permettre de vérifier son état. Vous devez reprendre l'opération manuellement.

Vous devez netboot nœud4 si cette version de ONTAP 9 n'est pas installée sur le nœud 2. Une fois le nœud 4 installé, démarrez-le à partir de l'image ONTAP 9 stockée sur le serveur Web. Vous pouvez ensuite télécharger les fichiers corrects sur le périphérique de démarrage pour les démarrages suivants du système, en suivant les instructions de la section ["Préparation à la mise sur le réseau"](#).

Étapes

1. Assurez-vous que le nœud 4 dispose d'un espace de rack suffisant.

Si le nœud 4 se trouve dans un châssis distinct du nœud 2, vous pouvez placer le nœud 4 au même emplacement que le nœud 3. Si les nœuds 2 et 4 se trouvent dans le même châssis, le nœud 4 se trouve déjà dans son emplacement de rack approprié.

2. Installez le node4 dans le rack en suivant les instructions de *instructions d'installation et de configuration* pour le modèle de nœud.
3. Reliez le nœud 4, puis déplacez les connexions du nœud 2 vers le nœud 4.

Reliez les connexions suivantes à l'aide des instructions de *instructions d'installation et de configuration* ou

de *FlexArray virtualisation installation conditions requises et Reference* pour la plateforme node4, le document de tiroir disque approprié et *High Availability Management*.

Reportez-vous à la section "[Références](#)" Pour établir un lien vers les spécifications d'installation de la virtualisation et les références_ et *gestion de la haute disponibilité* de FlexArray.

- Console (port de gestion à distance)
- De clusters et de ports haute disponibilité
- Ports de données
- Ports de gestion de clusters et de nœuds
- Ports de stockage SAS (Serial-Attached SCSI) et Ethernet
- Configurations SAN : ports de switch Ethernet iSCSI, FC et NVMe/FC

Vous devrez peut-être modifier les câbles d'interconnexion entre l'ancien et le nouveau contrôleur pour assurer l'interopérabilité entre les différents modèles de contrôleur et de carte. Pour obtenir un schéma de câblage des tiroirs de stockage Ethernet de vos systèmes, reportez-vous au "[procédures d'installation du système](#)".



Pour les contrôleurs introduits dans ONTAP 9.15.1 et versions ultérieures, les interconnexions de cluster et haute disponibilité utilisent les mêmes ports. Pour les configurations connectées par commutateur, il est nécessaire de connecter des ports similaires aux mêmes commutateurs du cluster. Par exemple, lors de la mise à niveau vers un AFF A1K à partir d'un contrôleur existant, vous devez connecter les ports e1a des deux nœuds à un commutateur et les ports e7a des deux nœuds au second commutateur.

4. Mettez le nœud 4 sous tension, puis interrompez le processus de démarrage en appuyant sur `Ctrl-C` sur le terminal de la console pour accéder à l'invite de l'environnement d'initialisation.



Lors du démarrage du nœud 4, le message d'avertissement suivant peut s'afficher :

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
        because the battery is discharged but could be due to other
temporary
        conditions.
        When the battery is ready, the boot process will complete
and services will be engaged. To override this delay, press 'c'
followed
        by 'Enter'
```

5. Si le message d'avertissement s'affiche à l'étape 4, effectuez les actions suivantes :
 - a. Vérifiez s'il y a un message de console susceptible d'indiquer un problème autre que celui d'une batterie NVRAM faible et, le cas échéant, effectuez les actions correctives nécessaires.
 - b. Laissez la batterie se charger et le processus de démarrage s'achever.



Attention : ne pas outrepasser le délai; si la batterie n'est pas chargée, cela pourrait entraîner une perte de données.




Reportez-vous à la section "[Préparation à la mise sur le réseau](#)".

6. Configurez la connexion netboot en choisissant l'une des opérations suivantes.



Vous devez utiliser le port de gestion et l'IP comme connexion netboot. N'utilisez pas d'IP de la LIF de données et ne subit aucune panne pendant l'exécution de la mise à niveau.

Si le protocole DHCP (Dynamic Host Configuration Protocol) est...	Alors...
Exécution	Configurez la connexion automatiquement à l'aide de la commande suivante à l'invite de l'environnement d'initialisation : <code>ifconfig e0M -auto</code>
Non en cours d'exécution	Configurez manuellement la connexion en entrant la commande suivante à l'invite de l'environnement d'amorçage : <code>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></code> <i>filer_addr</i> Est l'adresse IP du système de stockage (obligatoire). <i>netmask</i> est le masque de réseau du système de stockage (obligatoire). <i>gateway</i> est la passerelle du système de stockage (obligatoire). <i>dns_addr</i> Est l'adresse IP d'un serveur de noms sur votre réseau (facultatif). <i>dns_domain</i> Est le nom de domaine DNS (facultatif).  D'autres paramètres peuvent être nécessaires pour votre interface. Entrez <code>help ifconfig</code> à l'invite du micrologiciel pour plus de détails.

7. Démarrage sur le nœud 4 :

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

Le <path_to_the_web-accessible_directory> vous devez indiquer où vous avez téléchargé le <ontap_version>_image.tgz À l'étape 1 de la section "[Préparation à la mise sur le réseau](#)".



N'interrompez pas l'amorçage.

8. Dans le menu de démarrage, sélectionnez option (7) `Install new software first`.

Cette option de menu permet de télécharger et d'installer la nouvelle image ONTAP sur le périphérique d'amorçage.

Ne tenez pas compte du message suivant :

This procedure is not supported for Non-Disruptive Upgrade on an HA pair

Cette remarque s'applique aux mises à niveau de ONTAP sans interruption et non aux mises à niveau des contrôleurs.



Utilisez toujours netboot pour mettre à jour le nouveau nœud vers l'image souhaitée. Si vous utilisez une autre méthode pour installer l'image sur le nouveau contrôleur, il est possible que l'image incorrecte soit installée. Ce problème s'applique à toutes les versions de ONTAP. Procédure netboot combinée avec l'option (7) `Install new software` Efface le support de démarrage et place la même version de ONTAP sur les deux partitions d'image.

9. Si vous êtes invité à poursuivre la procédure, entrez `y`. Et lorsque vous êtes invité à saisir l'URL du pack :

```
http://<web_server_ip/path_to_web-  
accessible_directory>/<ontap_version>_image.tgz
```

10. Procédez comme suit pour redémarrer le module de contrôleur :

- a. Entrez `n` pour ignorer la récupération de sauvegarde lorsque l'invite suivante s'affiche :

```
Do you want to restore the backup configuration now? {y|n}
```

- b. Redémarrez en entrant `y` lorsque vous voyez l'invite suivante :

```
The node must be rebooted to start using the newly installed  
software. Do you want to reboot now? {y|n}
```

Le module de contrôleur redémarre mais s'arrête au menu d'amorçage car le périphérique d'amorçage a été reformaté et les données de configuration doivent être restaurées.

11. Sélectionnez le mode maintenance `5` dans le menu de démarrage et entrez `y` lorsque vous êtes invité à poursuivre le démarrage.
12. Vérifiez que le contrôleur et le châssis sont configurés en tant que haute disponibilité :

```
ha-config show
```

L'exemple suivant montre la sortie du `ha-config show` commande :

```
Chassis HA configuration: ha  
Controller HA configuration: ha
```



Le système enregistre dans une PROM, qu'il soit dans une paire HA ou dans une configuration autonome. L'état doit être le même sur tous les composants du système autonome ou de la paire haute disponibilité.

13. Si le contrôleur et le châssis ne sont pas configurés comme HA, utilisez les commandes suivantes pour

corriger la configuration :

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. Vérifiez que tous les ports Ethernet utilisés pour la connexion aux tiroirs Ethernet sont configurés comme stockage :

```
storage port show
```

Le résultat affiché dépend de la configuration du système. L'exemple de sortie suivant concerne un nœud avec une seule carte de stockage dans slot11. La sortie de votre système peut être différente :

```
*> storage port show
Port Type Mode      Speed(Gb/s) State      Status  VLAN ID
---- -
e11a ENET storage 100 Gb/s   enabled  online  30
e11b ENET storage 100 Gb/s   enabled  online  30
```

15. Modifiez les ports qui ne sont pas définis sur Storage :

```
storage port modify -p <port> -m storage
```

Tous les ports Ethernet connectés aux tiroirs de stockage doivent être configurés en tant que stockage pour permettre l'accès aux disques et aux tiroirs.

16. Quitter le mode maintenance :

```
halt
```

Interrompez l'AUTOBOOT en appuyant sur Ctrl-C dans l'invite de l'environnement de démarrage.

17. sur le noeud 3, vérifiez la date, l'heure et le fuseau horaire du système :

```
date
```

18. Sur le nœud 4, vérifiez la date à l'aide de la commande suivante à l'invite de l'environnement d'initialisation :

```
show date
```

19. Si nécessaire, définissez la date sur le node4 :

```
set date <mm/dd/yyyy>
```

20. Sur le nœud 4, vérifiez l'heure à l'aide de la commande suivante à l'invite de l'environnement d'amorçage :

```
show time
```

21. Si nécessaire, définissez l'heure sur le node4 :

```
set time <hh:mm:ss>
```

22. Dans le chargeur de démarrage, définissez l'ID système partenaire sur le nœud 4 :

```
setenv partner-sysid <node3_sysid>
```

Pour node4, `partner-sysid` doit être celui du nœud 3.

Enregistrer les paramètres :

```
saveenv
```

23. Vérifiez l' `partner-sysid` pour le nœud 4 :

```
printenv partner-sysid
```

24. si des lecteurs 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>

- 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](#)".

25. Nœud de démarrage dans le menu de démarrage :

```
boot_ontap menu.
```

26. sur le node4, allez dans le menu de démarrage et, à l'aide de 22/7, sélectionnez l'option cachée `boot_after_controller_replacement`. À l'invite, entrez `node2` pour réaffecter les disques du nœud2 au nœud4, comme dans l'exemple suivant.

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 node2 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:

```



Dans l'exemple de sortie de la console ci-dessus, ONTAP vous invite à entrer le nom du nœud partenaire si le système utilise des disques du partitionnement de disque avancé.

27. à l'invite du CHARGEUR, démarrez :

boot_ontap menu

Maintenant, au démarrage, le nœud peut détecter tous les disques qui lui étaient précédemment affectés et peut démarrer comme prévu.

Lorsque les nœuds de cluster que vous remplacez utilisent le chiffrement de volume racine, ONTAP ne peut pas lire les informations de volume à partir des disques. Restaurer les clés du volume root:

Si le volume root est chiffré, restaurez les secrets de la gestion intégrée des clés afin que le système puisse trouver le volume root.

a. Revenir au menu de démarrage spécial :

```
LOADER> boot_ontap menu
```

```
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
```

b. Sélectionnez **(10) définir les secrets de récupération du gestionnaire de clés intégré**

c. Entrez **y** à l'invite suivante :

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

d. À l'invite, entrez la phrase de passe du gestionnaire de clés.

e. Entrez les données de sauvegarde lorsque vous y êtes invité.



Vous devez avoir obtenu la phrase de passe et les données de sauvegarde dans le "[Préparer les nœuds pour une mise à niveau](#)" section de cette procédure.

f. Une fois que le système a de nouveau démarré dans le menu de démarrage spécial, exécutez l'option **(1) démarrage normal**



Il se peut que vous rencontriez une erreur à ce stade. Si une erreur se produit, répétez les sous-étapes de la section [Étape 27](#) jusqu'à ce que le système démarre normalement.

Vérifiez l'installation du node4

Vous devez vérifier que les ports physiques du nœud2 sont correctement mis en correspondance avec les ports physiques du nœud4. Ainsi, le nœud4 pourra communiquer avec d'autres nœuds du cluster et avec le réseau après la mise à niveau.

Description de la tâche

Reportez-vous à la section "[Références](#)" Pour établir une liaison avec *Hardware Universe* afin de capturer des informations sur les ports des nouveaux nœuds. Vous utiliserez ces informations plus loin dans cette section.

L'organisation des ports physiques peut varier en fonction du modèle des nœuds. Au démarrage du nouveau nœud, ONTAP tente de déterminer les ports qui doivent héberger les LIFs du cluster afin de se mettre automatiquement en quorum.

Si les ports physiques du node2 ne sont pas directement mis en correspondance avec les ports physiques du node4, la section suivante [Restaurez la configuration du réseau sur le noeud 4](#) doit être utilisé pour réparer la connectivité réseau.

Après avoir installé et démarré node4, vous devez vérifier qu'il est correctement installé. Vous devez attendre que le noeud 4 rejoigne le quorum et reprendre l'opération de transfert.

À ce stade de la procédure, l'opération aura été interrompue au fur et à mesure que le noeud 4 rejoint le quorum.

Étapes

1. Vérifiez que le noeud 4 a rejoint le quorum :

```
cluster show -node node4 -fields health
```

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

2. Vérifiez que le noeud 4 fait partie du même cluster que le noeud 3 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 dans un état en pause et dans le même état qu'elle était 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. Le remplacement du contrôleur est alors mis en pause pour toute intervention incluant le message suivant :

```

Cluster::*> system controller replace show
Node                Status                Error-Action
-----
Node2(now node4) Paused-for-intervention  Follow the instructions
given in
Node2                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 *recréation des VLAN, ifgrps et des domaines de diffusion* a été renommée *Restauration de la configuration du réseau sur le nœud 4*.

7. Lorsque le remplacement du contrôleur est en pause, passez à la section suivante de ce document pour restaurer la configuration réseau sur le nœud.

Restaurez la configuration du réseau sur le nœud 4

Une fois que vous avez confirmé que le nœud4 est quorum et peut communiquer avec le nœud3, vérifiez que les VLAN, les groupes d'interface et les domaines de diffusion du nœud2 sont visibles sur le nœud4. Vérifiez également que tous les ports réseau node4 sont configurés dans leurs domaines de diffusion appropriés.

Description de la tâche

Pour plus d'informations sur la création et la recréation de VLAN, de groupes d'interfaces et de domaines de diffusion, reportez-vous à la section "[Références](#)" Pour établir un lien vers *Network Management*.

Étapes

1. Lister tous les ports physiques qui se trouvent sur le nœud mis à niveau 2 (appelé node4) :

```
network port show -node node4
```

Tous les ports réseau physiques, 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'interfaces, 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 node4 :

```
network port reachability show
```

La sortie de la commande ressemble à l'exemple suivant :

```

ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
    e0M      Default:Mgmt      ok
    e10a     Default:Default   ok
    e10b     -                 no-reachability
    e10c     Default:Default   ok
    e10d     -                 no-reachability
    e1a      Cluster:Cluster   ok
    e1b      -                 no-reachability
    e7a      Cluster:Cluster   ok
    e7b      -                 no-reachability
node2_node4
    e0M      Default:Mgmt      ok
    e10a     Default:Default   ok
    e10b     -                 no-reachability
    e10c     Default:Default   ok
    e10d     -                 no-reachability
    e1a      Cluster:Cluster   ok
    e1b      -                 no-reachability
    e7a      Cluster:Cluster   ok
    e7b      -                 no-reachability
18 entries were displayed.

```

Dans l'exemple ci-dessus, le nœud 2_node4 démarre simplement 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.

- réparer l'accessibilité pour chacun des ports du node4 avec un état d'accessibilité autre que `ok`. Exécuter la commande suivante, sur tout premier port physique, puis sur n'importe quel port VLAN, un à la fois :

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

Le résultat semble être l'exemple suivant :

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" 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 ci-dessus, est prévu 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. Si la configuration des groupes d'interfaces ne correspond pas à la nouvelle disposition des ports physiques du contrôleur, modifiez-la en procédant comme suit.

a. Vous devez d'abord supprimer les ports physiques qui doivent être des ports membres du groupe d'interfaces de leur appartenance à un domaine de diffusion. Pour ce faire, utilisez la commande suivante :

```
network port broadcast-domain remove-ports -broadcast-domain  
<broadcast_domain_name> -ports <node_name:port_name>
```

b. Ajout d'un port membre à un groupe d'interfaces :

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port  
<port_name>
```

c. Le groupe d'interface est automatiquement ajouté au domaine de diffusion environ une minute après l'ajout du premier port membre.

d. Vérifiez que le groupe d'interface a été ajouté au domaine de diffusion approprié :

```
network port reachability show -node <node_name> -port <ifgrp>
```

Si l'état de la capacité d'accessibilité du groupe d'interfaces n'est pas le cas *ok*, affectez-le au domaine de diffusion approprié :

```
network port broadcast-domain add-ports -broadcast-domain  
<broadcast_domain_name> -ports <node:port>
```

6. Attribuez les ports physiques appropriés à la *Cluster broadcast domain* :

a. Déterminez les ports qui ont la capacité de remboursement du *Cluster broadcast domain* :

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

b. Réparer n'importe quel port avec la capacité de réparation du *Cluster broadcast domain*, si son statut de accessibilité n'est pas *ok*:

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

7. Déplacez les ports physiques restants dans leurs domaines de diffusion appropriés à l'aide de l'une des commandes suivantes :

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

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Vérifiez qu'il n'y a pas de port injoignable ou inattendu. Vérifiez l'état d'accessibilité de tous les ports physiques à l'aide de la commande suivante et en examinant la sortie pour confirmer que l'état est ok:

```
network port reachability show -detail
```

8. Restaurez les VLAN qui auraient pu être déplacés à l'aide des étapes suivantes :

a. Liste des réseaux locaux virtuels déplacés :

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

Les valeurs de sortie suivantes doivent s'afficher :

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1  a0a         822, 823
      e10a         822, 823
```

b. Restaurer les VLAN déplacés de leurs ports de base précédents :

```
cluster controller-replacement network displaced-vlans restore
```

Voici un exemple de restauration des VLAN déplacés du groupe d'interface a0a vers le même groupe d'interface :

```
Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
-destination-port a0a
```

Voici un exemple de restauration de VLAN déplacés vers le port « e10a » et vers « e10b » :

```
Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
-destination-port e10b
```

Lorsqu'une restauration VLAN est réussie, les VLAN déplacés sont créés sur le port de destination spécifié. La restauration VLAN échoue si le port de destination est membre d'un groupe d'interfaces ou si le port de destination est arrêté.

Attendez environ une minute pour placer les VLAN nouvellement restaurés dans leurs domaines de

diffusion appropriés.

- a. Créez de nouveaux ports VLAN si nécessaire pour les ports VLAN qui ne sont pas dans le `cluster controller-replacement network displaced-vlans show` sortie mais doit être configurée sur d'autres ports physiques.

9. Supprimez tous les domaines de diffusion vides une fois que toutes les réparations de port ont été effectuées :

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. 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 ports, effectuez la réparation de la capacité d'accessibilité et ajoutez ou supprimez des ports de leurs domaines de diffusion comme indiqué dans [Étape 4](#).

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

```
network port show
```

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

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

13. Restaurer les ports de base LIF, en précisant les ports de base Vserver(s) et LIF, le cas échéant, à restaurer :

- a. Lister les LIFs déplacées :

```
displaced-interface show
```

- b. Restaurer les ports de base LIF :

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

14. 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 4

Si vous utilisez NetApp Volume Encryption (NVE) et NetApp Aggregate Encryption (NAE) pour le chiffrement des volumes sur le système que vous mettez à niveau, la configuration de chiffrement doit être synchronisée avec les nouveaux nœuds. Si vous ne

synchronisez pas le gestionnaire de clés, lorsque vous transférez les agrégats du nœud 2 depuis le nœud 3 vers le nœud 4 à l'aide du transfert d'agrégats, des défaillances peuvent survenir, car le nœud 4 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 4 :

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

2. Vérifier que la clé SVM-KEK est restaurée sur « true » sur le nœud4 avant de transférer les agrégats de données :

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

Exemple

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node4	svm1	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f000000000000000

Déplacement des agrégats non racines et des LIF de données NAS qui appartiennent au nœud 2 du nœud 3 vers le nœud 4

Après avoir vérifié la configuration réseau sur le nœud 4 et avant de transférer les agrégats du nœud 3 vers le nœud 4, vous devez vérifier que les LIF de données NAS appartenant au nœud 2 actuellement transférées du nœud 3 vers le nœud 4 sont bien transférées. Vous devez également vérifier que des LIFs SAN existent sur le nœud4.

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. Vous devez

vérifier que les LIF sont en bon état et situées sur les ports appropriés une fois que vous avez mis le nœud 4 en ligne.

Étapes

1. Les LIFs iSCSI trouvent automatiquement les ports home corrects à l'aide de l'analyse d'accessibilité. Les LIF FC et SAN NVMe/FC ne se déplacent pas automatiquement. Ils continuent d'afficher le port de base sur lequel ils se trouvaient avant la mise à niveau.

Vérifier les LIFs SAN sur le node4 :

- a. Modifier toute LIF SAN iSCSI signalant un état de fonctionnement « arrêté » aux nouveaux ports de données :

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. Modifier toutes les LIFs FC et SAN NVMe/FC qui home sur le nouveau contrôleur et indiquent un statut opérationnel « down » aux ports FCP sur le nouveau contrôleur :

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. 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.

3. 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 relocalise les agrégats non racines et les LIF de données NAS qui appartiennent au nœud 2 vers le nouveau contrôleur, node4. L'opération de remplacement du contrôleur s'interrompt une fois le transfert de ressources terminé.

4. 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.

5. 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 nœud4 :

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

6. 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.