Étape 3. Installez et démarrez le nœud 3

Upgrade controllers

NetApp
July 05, 2024

Sommaire

Étape 3. Installez et démarrez le nœud 3

Présentation de la phase 3

Lors de la phase 3, vous installez et démarrez le nœud 3, vérifiez que le cluster et les ports de gestion des nœuds du nœud 1 sont connectés sur le nœud 3 et vérifiez l'installation du nœud 3. Si vous utilisez NetApp Volume Encryption (NVE), vous restaurez la configuration du gestionnaire de clés. Vous pouvez également transférer les LIF de données NAS du nœud 1 et les agrégats non racine du nœud 2 vers le nœud 3, puis vérifier que les LIF SAN existent sur le nœud 3.

Étapes

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

Installez et démarrez le nœud 3

Vous installez le nœud 3 dans le rack, transférez les connexions du nœud 1 vers le nœud 3, amorcez le nœud 3 et installez ONTAP. Vous réaffectez ensuite l'un des disques de spare du nœud 1, tous les disques appartenant au volume racine et tous les agrégats non racines qui n'ont pas été déplacés vers le nœud 2 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 largement automatisé. L'opération s'interrompt pour vous permettre de vérifier son état. Vous devez reprendre l'opération manuellement. En outre, vous devez vérifier que les LIFs SAN sont bien mises en ligne et attribuées aux ports physiques FC appropriés sur le NODE3.

Vous avez besoin de netboot nœud3 si cette version de ONTAP 9 n'est pas installée sur le nœud 1. Une fois le noeud 3 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 vous disposez d'un espace rack pour node3.

   Les besoins en espace et en hauteur des nouveaux nœuds peuvent être différents des nœuds existants. Planifiez l'espace requis pour votre scénario de mise à niveau.

2. installez le noeud 3 dans le rack, en suivant les instructions *installation and Setup* de votre modèle de nœud.
3. Cable node3, déplaçant les connexions du node1 vers le node3.

   À partir de ONTAP 9.15.1, les nouveaux modèles de contrôleurs ne disposent que d'un seul port « clé »

pour le contrôleur BMC (Baseboard Management Controller) et les connexions de gestion. Planifiez les modifications de câblage en conséquence.

- 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 système sous tension vers le noeud 3, puis interrompez le processus d'amorçage en appuyant sur Ctrl-C sur le terminal de la console pour accéder à l'invite de l'environnement d'amorçage.

Lorsque vous démarrez le nœud 3, 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 vous voyez le message d'avertissement dans Étape 4, procédez comme suit :

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 actions 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 : `ifconfig e0M -auto`
Non en cours d'exécution	Configurez manuellement la connexion à l'aide de la commande suivante à l'invite de l'environnement d'initialisation : `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Est l'adresse IP du système de stockage (obligatoire). *`netmask`* est le masque de réseau du système de stockage (obligatoire). *`gateway`* est la passerelle du système de stockage (obligatoire). *`dns_addr`* Est l'adresse IP d'un serveur de noms sur votre réseau (facultatif). *`dns_domain`* Est le nom de domaine DNS (Domain Name Service) (facultatif). D'autres paramètres peuvent être nécessaires pour votre interface. Entrez `help ifconfig` à l'invite du micrologiciel pour plus de détails.

7. exécutez sur le nœud 3 :

```
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` dans 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. effectuez les sous-étapes suivantes 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. Entrez `y` pour redémarrer 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 de maintenance `5` dans le menu de démarrage et entrez `y` lorsque vous êtes invité à poursuivre le démarrage.
12. vérifier que le contrôleur et le châssis sont configurés comme 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` à l'invite de l'environnement de démarrage.

17. Sur le node2, vérifiez la date, l'heure et le fuseau horaire du système :

    ```
    date
    ```

18. Sur le node3, vérifiez la date à l'aide de la commande suivante à l'invite de l'environnement de démarrage :

    ```
    show date
    ```

19. Si nécessaire, définissez la date sur le nœud 3 :

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

20. Sur le node3, vérifiez l'heure en utilisant la commande suivante à l'invite de l'environnement de démarrage :

    ```
    show time
    ```

21. Si nécessaire, définissez l'heure sur le nœud 3 :

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

22. Dans le chargeur de démarrage, définissez l'ID système du partenaire sur le nœud 3 :

    ```
    setenv partner-sysid <node2_sysid>
    ```

    Pour le nœud 3, `partner-sysid` doit être celui du node2.

a. Enregistrer les paramètres :

```
saveenv
```

23. Vérifiez l' `partner-sysid` pour le nœud 3 :

```
printenv partner-sysid
```

24. 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	`setenv bootarg.storageencryption.support` **`true`**
NetApp non-SED FIPS	`setenv bootarg.storageencryption.support` **`false`**

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 node3, accédez au menu de démarrage et, à l'aide de 22/7, sélectionnez l'option cachée `boot_after_controller_replacement`. À l'invite, entrez node1 pour réaffecter les disques du nœud1 au nœud3, 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 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:
```

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. Si le système passe en boucle de redémarrage avec le message `no disks found`, il indique qu'il y a eu un problème avec la réaffectation de disque. Voir "Résoudre les problèmes" pour résoudre le problème.
28. Appuyez sur `Ctrl-C` pendant l'AUTOBOOT pour arrêter le nœud à `LOADER>` l'invite.
29. À l'invite du CHARGEUR, entrer en mode maintenance :

    ```
    boot_ontap maint
    ```

30. Vérifiez la connectivité du disque, le modèle de contrôleur, la configuration haute disponibilité et d'autres informations relatives à la connectivité du matériel.
31. Quitter le mode maintenance :

    ```
    halt
    ```

32. 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.

    Cela s'applique uniquement lorsque le volume racine utilise le chiffrement de volume NetApp.

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 32 jusqu'à ce que le système démarre normalement.

Vérifiez l'installation du noeud 3

Vous devez vérifier que les ports physiques du nœud1 sont correctement mis en correspondance avec les ports physiques du nœud3. Cela permettra au noeud 3 de 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 nœud1 ne sont pas directement mis en correspondance avec les ports physiques du nœud3, la section suivante Restaurez la configuration du réseau sur le noeud 3 doit être utilisé pour réparer la connectivité réseau.

Après avoir installé et démarrer node3, vous devez vérifier qu'il est correctement installé. Vous devez attendre que le noeud 3 rejoint 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 3 rejoint le quorum.

Étapes

1. Vérifiez que le noeud 3 a rejoint le quorum :

   ```
   cluster show -node node3 -fields health
   ```

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

2. Vérifiez que le noeud 3 fait partie du même cluster que le noeud 2 et qu'il est en bon état :

   ```
   cluster show
   ```

3. passer en mode de 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 1 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
---------------- ------------------------
-----------------------------------
Node1(now node3) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2                       None

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-création de VLAN, ifgrps et broadcast domain* a été renommée *Restore network configuration sur node3*.

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 noeud 3

Une fois que vous avez confirmé que le noeud 3 est dans le quorum et que vous pouvez communiquer avec le noeud 2, vérifiez que les VLAN, les groupes d'interface et les domaines de diffusion du noeud 1 sont visibles sur le noeud 3. Vérifiez également que tous les ports réseau du node3 sont configurés dans leurs domaines de diffusion appropriés.

Description de la tâche

Pour plus d'informations sur la création et la recrércréation 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. Répertoriez tous les ports physiques qui se trouvent sur le nœud mis à niveau 1 (appelé nœud 3) :

```
network port show -node node3
```

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 quels ports doivent être utilisés 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 node3 :

```
network port reachability show
```

La sortie doit s'afficher comme dans 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
          e4a      Default:Default                    ok
          e4b      -                                  no-reachability
          e4c      Default:Default                    ok
          e4d      -                                  no-reachability
          e3a      Cluster:Cluster                    ok
          e3b      Cluster:Cluster                    ok
18 entries were displayed.
```

Dans l'exemple précédent, le nœud 1_node3 démarre simplement après le remplacement du contrôleur. Certains ports n'ont pas la capacité de reachcapacité à leurs domaines de diffusion attendus et doivent être réparés.

4. réparer l'accessibilité pour chacun des ports du node3 avec un état de réabilité 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>
```

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

```
Cluster ::> reachability repair -node node1_node3 -port e4a
```

```
Warning: Repairing port "node1_node3: e4a" 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 réachbilité 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 au `Cluster` domaine de diffusion en procédant comme suit :
   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
                  e4a       822, 823
      2 entries were displayed.
      ```

   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 node1_node3 -port a0a
-destination-port a0a
```

Voici un exemple de restauration des VLAN déplacés sur le port « e9a » vers « e9d » :

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

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. vérifier 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.

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 home Vserver(s) et LIF, le cas échéant, qui doivent être restaurés 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 :

```
cluster controller-replacement network 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 noeud 3

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 1 du nœud 2 vers le nœud 3 à l'aide du transfert d'agrégats (ARL), des défaillances peuvent se produire, car le nœud 3 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 3 :

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

2. Vérifier que la clé SVM-KEK est restaurée sur « true » sur le nœud3 avant de transférer les agrégats de données :

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK
```

Exemple

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node3    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Déplacement des agrégats non racines et des LIF de données NAS qui appartiennent au nœud 1 du nœud 2 vers le nœud 3

Après avoir vérifié la configuration réseau sur le nœud 3 et avant de transférer les agrégats du nœud 2 vers le nœud 3, vous devez vérifier que les LIF de données NAS appartenant au nœud 1 actuellement sur le nœud 2 sont transférées du nœud 2 vers le nœud 3. Vous devez également vérifier que des LIFs SAN existent sur le noeud 3.

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 vérifierez que les LIFs sont saines et situées sur les ports appropriés après avoir mis le nœud3 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 node3 :

   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-racine et les LIF de données NAS qui appartiennent au nœud1 vers le nouveau contrôleur, node3. 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, restaurer le nœud de rattachement vers le nœud3 :

   `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