Mettez à niveau, actualisez ou développez la configuration MetroCluster

ONTAP MetroCluster

NetApp
April 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-metrocluster/upgrade/concept_choosing_an_upgrade_method_mcc.html on April 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Mettez à niveau, actualisez ou développez la configuration MetroCluster . . . 1
Commencez ici : choisissez votre procédure . . . 1
Mise à niveau des contrôleurs d'une configuration IP MetroCluster à quatre nœuds via le basculement et le rétablissement à l'aide des commandes « system Controller replace » (ONTAP 9.13.1 et versions ultérieures) . . . 8
Mise à niveau des contrôleurs en une configuration MetroCluster FC à l'aide du basculement et du rétablissement . . . 30
Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 en configuration FC MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure) . . . 56
Mise à niveau des contrôleurs en une configuration FC MetroCluster à quatre nœuds via le basculement et le rétablissement avec des commandes « system contrôleur replace » (ONTAP 9.10.1 et versions ultérieures) . . . 84
Mise à niveau des contrôleurs dans une configuration MetroCluster IP à l'aide du basculement et du rétablissement (ONTAP 9.8 et versions ultérieures) . . . 101
Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 dans une configuration IP MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure) . . . 132
Mise à jour d'une configuration FC MetroCluster à quatre nœuds . . . 162
Actualisation d'une configuration IP MetroCluster à quatre ou huit nœuds (ONTAP 9.8 et versions ultérieures) . . . 164
Étendez une configuration FC MetroCluster à deux nœuds à une configuration à quatre nœuds . . . 173
Étendez une configuration FC MetroCluster à quatre nœuds à une configuration à huit nœuds . . . 212
Développement d'une configuration IP MetroCluster . . . 248
Suppression d'un groupe de reprise après incident . . . 277
Où trouver des informations complémentaires . . . 281

Mettez à niveau, actualisez ou développez la configuration MetroCluster

Commencez ici : choisissez votre procédure

Commencez ici : vous avez le choix entre une mise à niveau du contrôleur, une mise à jour du système ou une extension

En fonction du périmètre de la mise à niveau de l'équipement, le client choisit une procédure de mise à niveau du contrôleur, de mise à jour du système ou d'extension.

- Les procédures de mise à niveau du contrôleur s'appliquent uniquement aux modules de contrôleur. Les contrôleurs sont remplacés par un nouveau modèle de contrôleur.

  Les modèles de tiroirs de stockage ne sont pas mis à niveau.

  - Dans le cadre des procédures de basculement et de rétablissement, le basculement MetroCluster est utilisé pour fournir aux clients un service sans interruption pendant la mise à niveau des modules de contrôleur sur le cluster partenaire.
  - Dans le cadre d'une procédure de mise à niveau du contrôleur basée sur le transfert d'agrégats, les opérations de transfert d'agrégats servent à déplacer des données de l'ancienne configuration vers la nouvelle configuration mise à niveau, et ce sans interruption.
- Les procédures de mise à jour s'appliquent aux contrôleurs et aux tiroirs de stockage.

  Dans les procédures de mise à jour, de nouveaux contrôleurs et tiroirs sont ajoutés à la configuration MetroCluster, créant un deuxième groupe de reprise sur incident. Ensuite, les données sont migrées sans interruption vers les nouveaux nœuds.

  Les contrôleurs d'origine sont ensuite retirés du cluster.
- Les procédures d'extension permettent d'ajouter des contrôleurs et des tiroirs à la configuration MetroCluster sans supprimer aucun.

  La procédure que vous utilisez dépend du type de MetroCluster et du nombre de contrôleurs existants.

Type de mise à niveau	Aller à…
Mise à niveau du contrôleur	"Choisir la procédure de mise à niveau du contrôleur"
Mise à jour du système	"Choisir une procédure de rafraîchissement du système"
De développement	• "MetroCluster à deux nœuds à quatre nœuds" • "MetroCluster FC à quatre nœuds à huit" • "MetroCluster IP à quatre nœuds sur huit"

Choisir la procédure de mise à niveau du contrôleur

La procédure de mise à niveau du contrôleur que vous utilisez dépend du modèle de plate-forme et du type de configuration MetroCluster.

Dans le cadre d'une procédure de mise à niveau, les contrôleurs sont remplacés par un nouveau modèle de contrôleur. Les modèles de tiroirs de stockage ne sont pas mis à niveau.

- Dans le cadre des procédures de basculement et de rétablissement, le basculement MetroCluster est utilisé pour fournir aux clients un service sans interruption pendant la mise à niveau des modules de contrôleur sur le cluster partenaire.
- Dans le cadre d'une procédure de mise à niveau du contrôleur basée sur le transfert d'agrégats, les opérations de transfert d'agrégats servent à déplacer des données de l'ancienne configuration vers la nouvelle configuration mise à niveau, et ce sans interruption.

Sélection de la procédure utilisant le processus de basculement et de rétablissement

Sélectionnez votre plateforme actuelle dans le tableau FC ou IP ci-dessous. Si l'intersection de la ligne de plateforme actuelle et de la colonne de plateforme cible est vide, la mise à niveau n'est pas prise en charge.

Mises à niveau du contrôleur IP MetroCluster prises en charge

Si votre plate-forme n'est pas répertoriée, aucune combinaison de mise à niveau du contrôleur n'est prise en charge.

Lorsque vous effectuez une mise à niveau du contrôleur, l'ancien et le nouveau type de plate-forme **doivent** correspondent.

- Vous pouvez mettre à niveau un système FAS vers un système FAS ou un système AFF A-Series vers un système AFF A-Series.
- Vous ne pouvez pas mettre à niveau un système FAS vers un système AFF A-Series ou un système AFF A-Series vers un système AFF C-Series.

Par exemple, si la plateforme que vous souhaitez mettre à niveau est un système FAS8200, vous pouvez effectuer une mise à niveau vers un système FAS9000. Vous ne pouvez pas mettre à niveau un système FAS8200 vers un système AFF A700.

		Target MetroCluster IP platform									
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150										
	FAS2750 AFF A220										
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250										
	FAS8200 AFF A300										Note 2
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										Note 2
	FAS8700										Note 2
	FAS9000 AFF A700										Note 1
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

- Remarque 1 : pour cette mise à niveau, utilisez la procédure "Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 dans une configuration IP MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure)"
- Remarque 2 : les mises à niveau des contrôleurs sont prises en charge sur les systèmes exécutant ONTAP 9.13.1 ou version ultérieure.
- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, les nouveaux contrôleurs doivent exécuter la même version ONTAP que les anciens.

Mises à niveau prises en charge du contrôleur MetroCluster FC

Si votre plate-forme n'est pas répertoriée, aucune combinaison de mise à niveau du contrôleur n'est prise en charge.

Lorsque vous effectuez une mise à niveau du contrôleur, l'ancien et le nouveau type de plate-forme **doivent** correspondent.

- Vous pouvez mettre à niveau un système FAS vers un système FAS ou un système AFF A-Series vers un système AFF A-Series.
- Vous ne pouvez pas mettre à niveau un système FAS vers un système AFF A-Series ou un système AFF A-Series vers un système AFF C-Series.

Par exemple, si la plateforme que vous souhaitez mettre à niveau est un système FAS8200, vous pouvez effectuer une mise à niveau vers un système FAS9000. Vous ne pouvez pas mettre à niveau un système FAS8200 vers un système AFF A700.

		Target MetroCluster FC platform											
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1			Note 1				
	AFF8020		Note 1		Note 1		Note 1			Note 1			
	FAS8040 FAS8060 FAS8080												
	AFF8040 AFF8060 AFF8080												
	FAS8200					Note 2			Note 2		Note 4		
	AFF A300						Note 2			Note 2		Note 4	
	FAS8300										Note 4		
	AFF A400											Note 4	
	ASA A400												Note 5
	FAS9000										Note 3		
	AFF A700											Note 3	
	FAS9500												
	AFF A900												
	ASA A900												

- Remarque 1 : pour mettre à niveau les contrôleurs lorsque des connexions FCVI sur les nœuds FAS8020 ou AFF8020 existants utilisent les ports 1c et 1D, voir ci-dessoushttps://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/MetroCluster/Upgrading_controllers_when_FCVI_connections_on_existing_FAS8020_or_AFF8020_nodes_use_ports_1c_and_1d["Article de la base de connaissances"^].
- Remarque 2 : les mises à niveau des contrôleurs depuis des plateformes AFF A300 ou FAS8200 à l'aide des ports intégrés 0e et 0f en tant que connexions FC-VI sont prises en charge uniquement sur les systèmes suivants :
  - ONTAP 9.9.1 et versions antérieures
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1GA
  - ONTAP 9.13.1 et versions ultérieures

  Pour plus d'informations, consultez la "Rapport public".
- Remarque 3 : pour cette mise à niveau, voir "Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 en configuration FC MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure)"
- Remarque 4 : les mises à niveau des contrôleurs sont prises en charge sur les systèmes exécutant ONTAP 9.13.1 ou version ultérieure.
- Remarque 5 : les mises à niveau des contrôleurs sont prises en charge sur les systèmes exécutant ONTAP 9.14.1 ou version ultérieure.
- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, les nouveaux contrôleurs doivent exécuter la même version ONTAP que les anciens.

Type de MetroCluster	Méthode de mise à niveau	Version ONTAP	Procédure

IP	Mise à niveau par les commandes « System Controller replace »	9.13.1 et versions ultérieures	"Lien vers la procédure"
FC	Mise à niveau par les commandes « System Controller replace »	9.10.1 et versions ultérieures	"Lien vers la procédure"
FC	Mise à niveau manuelle avec les commandes de l'interface de ligne de commande (AFF A700/FAS9000 vers AFF A900/FAS9500 uniquement)	9.10.1 et versions ultérieures	"Lien vers la procédure"
IP	Mise à niveau manuelle avec les commandes de l'interface de ligne de commande (AFF A700/FAS9000 vers AFF A900/FAS9500 uniquement)	9.10.1 et versions ultérieures	"Lien vers la procédure"
FC	Mise à niveau manuelle avec les commandes CLI	9.8 et versions ultérieures	"Lien vers la procédure"
IP	Mise à niveau manuelle avec les commandes CLI	9.8 et versions ultérieures	"Lien vers la procédure"

Choix d'une procédure à l'aide du transfert d'agrégats

Dans le cadre d'une procédure de mise à niveau du contrôleur basée sur le transfert d'agrégats, les opérations de transfert d'agrégats servent à déplacer des données de l'ancienne configuration vers la nouvelle configuration mise à niveau, et ce sans interruption.

Type de MetroCluster	Transfert d'agrégats	Version ONTAP	Procédure
FC	Utilisation des commandes « system Controller replace » pour la mise à niveau des modèles de contrôleurs dans le même châssis	9.10.1 et versions ultérieures	"Lien vers la procédure"
FC	À l'aide de `system controller replace` commandes	9.8 et versions ultérieures	"Lien vers la procédure"
FC	À l'aide de `system controller replace` commandes	9.5 à 9.7	"Lien vers la procédure"
FC	À l'aide des commandes ARL manuelles	9.8	"Lien vers la procédure"
FC	À l'aide des commandes ARL manuelles	9.7 et versions antérieures	"Lien vers la procédure"

Choix d'une méthode de renouvellement du système

La procédure de mise à jour du système que vous utilisez dépend du modèle de plate-forme et du type de configuration MetroCluster. Les procédures de mise à jour s'appliquent aux contrôleurs et aux tiroirs de stockage. Dans les procédures de mise à jour, de nouveaux contrôleurs et tiroirs sont ajoutés à la configuration MetroCluster, créant un deuxième groupe de reprise sur incident. Ensuite, les données sont migrées sans interruption vers les nouveaux nœuds. Les contrôleurs d'origine sont ensuite retirés du cluster.

Combinaisons de mise à jour technologique MetroCluster FC prises en charge

		Target MetroCluster FC platform									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8200	■	■	■	■	■	■	■	■	■	■
	AFF A300	■	■	■	■	■	■	■	■	■	■
	FAS8300			■	■	■	■	■	■	■	■
	AFF A400			■	■	■	■	■	■	■	■
	ASA A400			■	■	■	■	■	■	■	■
	FAS9000						■	■	■	■	■
	AFF A700						■	■	■	■	■
	FAS9500								■	■	■
	AFF A900								■	■	■
	ASA A900								■	■	■

- Vous devez terminer la procédure de mise à jour technologique avant d'ajouter un nouveau chargement.
- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, si vous avez une configuration à huit nœuds, les huit nœuds doivent exécuter la même version de ONTAP.

- Ne dépassez pas les limites d'objet du « bas » des plates-formes de la combinaison. Appliquez la limite inférieure des objets des deux plates-formes.
- Si les limites de la plateforme cible sont inférieures aux limites de la MetroCluster, vous devez reconfigurer la MetroCluster pour qu'elle se situe au niveau ou en dessous des limites de la plateforme cible avant d'ajouter les nouveaux nœuds.
- Reportez-vous à la "Hardware Universe" pour les limites de plateforme.

Combinaisons de mise à jour technologique MetroCluster IP prises en charge

		Target MetroCluster IP platform									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150 ASA A150	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS2750 AFF A220	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										
	FAS8700										
	FAS9000 AFF A700										
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

Note 1: cette combinaison nécessite ONTAP 9.13.1 ou une version ultérieure.

- Vous devez terminer la procédure de mise à jour technologique avant d'ajouter un nouveau chargement.
- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, si vous avez une configuration à huit nœuds, les huit nœuds doivent exécuter la même version de ONTAP.
- Ne dépassez pas les limites d'objet du « bas » des plates-formes de la combinaison. Appliquez la limite inférieure des objets des deux plates-formes.
- Si les limites de la plateforme cible sont inférieures aux limites MetroCluster, vous devez reconfigurer le MetroCluster pour qu'il atteigne ou dépasse les limites de la plateforme cible avant d'ajouter les nouveaux nœuds.
- Reportez-vous à la "Hardware Universe" pour les limites de plateforme.

Méthode de rafraîchissement	Type de configuration	Version ONTAP	Procédure
• Méthode : développez la configuration MetroCluster, puis supprimez les anciens nœuds	FC à quatre nœuds	9.6 et versions ultérieures	"Lien vers la procédure"

Méthode de rafraîchissement	Type de configuration	Version ONTAP	Procédure
• Méthode : développez la configuration MetroCluster, puis supprimez les anciens nœuds	IP à quatre nœuds	9.8 et versions ultérieures	"Lien vers la procédure"

Choisissez une procédure d'extension

La procédure d'extension que vous utilisez dépend du type de configuration MetroCluster et de la version de ONTAP.

Une procédure d'extension implique l'ajout de nouveaux contrôleurs et de nouveaux espaces de stockage à la configuration MetroCluster. L'extension doit maintenir un nombre pair de contrôleurs sur chaque site et la procédure que vous utilisez dépend du nombre de nœuds de la configuration MetroCluster d'origine.

Méthode d'expansion	Type de configuration	Version ONTAP	Procédure
Méthode : développez un MetroCluster FC à deux nœuds sur quatre	FC à deux nœuds	ONTAP 9 et versions ultérieures (les plateformes doivent être prises en charge dans ONTAP 9.2 et versions ultérieures)	"Lien vers la procédure"
Méthode : développez un MetroCluster FC à quatre nœuds sur huit	FC à quatre nœuds	ONTAP 9 ou version ultérieure	"Lien vers la procédure"
Méthode : développez une adresse IP MetroCluster à quatre nœuds sur huit	IP à quatre nœuds	ONTAP 9.9.1 et versions ultérieures	"Lien vers la procédure"

Mise à niveau des contrôleurs d'une configuration IP MetroCluster à quatre nœuds via le basculement et le rétablissement à l'aide des commandes « system Controller replace » (ONTAP 9.13.1 et versions ultérieures)

Vous pouvez utiliser cette opération de basculement automatisé MetroCluster guidée pour effectuer une mise à niveau sans interruption du contrôleur sur une configuration IP MetroCluster à quatre nœuds. Dans le cadre de cette procédure, d'autres composants (tels que des tiroirs de stockage ou des commutateurs) ne peuvent pas être mis à niveau.

Combinaisons de plateformes prises en charge

Cette procédure prend en charge les mises à niveau de contrôleur suivantes sur les systèmes exécutant ONTAP 9.13.1 et versions ultérieures.

Ancien contrôleur	Remplacement du contrôleur
AFF A300	AFF A900
FAS8200	FAS9500

Vous pouvez effectuer les mises à niveau de contrôleur répertoriées dans le tableau ci-dessus sur les systèmes exécutant ONTAP 9.12.1 ou 9.11.1 en suivant la procédure de mise à niveau manuelle décrite "ici".

Pour plus d'informations sur les combinaisons de mise à niveau de plate-forme, consultez le tableau de mise à niveau IP MetroCluster dans "Choisir la procédure de mise à niveau du contrôleur".

Reportez-vous à la section "Choisissez une méthode de mise à niveau ou de rafraîchissement" pour les procédures supplémentaires.

Description de la tâche

- Cette procédure ne peut être utilisée que pour la mise à niveau du contrôleur.

  Les autres composants de la configuration, tels que les tiroirs de stockage ou les commutateurs, ne peuvent pas être mis à niveau simultanément.

- Cette procédure s'applique aux modules de contrôleur dans une configuration IP MetroCluster à quatre nœuds exécutant ONTAP 9.13.1 ou une version ultérieure.

  "NetApp Hardware Universe"

- Les systèmes MetroCluster doivent exécuter la même version de ONTAP sur les deux sites.
- Vous pouvez utiliser cette procédure pour mettre à niveau les contrôleurs d'une configuration IP MetroCluster à quatre nœuds à l'aide du basculement et du rétablissement automatisés basés sur NSO.

  Une mise à niveau avec transfert d'agrégats (ARL) à l'aide de commandes « remplacement du contrôleur système » n'est pas prise en charge dans une configuration IP MetroCluster à quatre nœuds.

- Vous devez utiliser la procédure de mise à niveau automatisée du contrôleur NSO pour mettre à niveau les contrôleurs dans l'ordre sur les deux sites.
- Cette procédure de mise à niveau automatisée du contrôleur NSO-5 vous permet de lancer le remplacement du contrôleur sur un site de reprise après incident MetroCluster. Vous pouvez effectuer le remplacement d'un contrôleur uniquement sur un site à la fois.
- Pour lancer un remplacement du contrôleur sur le site A, vous devez exécuter la commande de démarrage du remplacement du contrôleur depuis le site B. L'opération vous guide à remplacer les contrôleurs des deux nœuds sur le site A uniquement. Pour remplacer les contrôleurs sur le site B, vous devez exécuter la commande de démarrage de remplacement du contrôleur depuis le site A. Un message indique le site sur lequel les contrôleurs sont remplacés.

Les exemples de noms suivants sont utilisés dans cette procédure :

- Site_A
  - Avant la mise à niveau :
    - Node_A_1-Old
    - Node_A_2-Old
  - Après la mise à niveau :
    - Node_A_1-New
    - Node_A_2-New
- Site_B
  - Avant la mise à niveau :
    - Node_B_1-Old
    - Node_B_2-Old
  - Après la mise à niveau :
    - Node_B_1-New
    - Node_B_2-New

Préparation à la mise à niveau

Pour préparer la mise à niveau du contrôleur, vous devez effectuer des contrôles préalables du système et collecter les informations de configuration.

Avant le démarrage des contrôles préalables, si le Mediator ONTAP est installé, il est automatiquement détecté et supprimé. Pour confirmer la suppression, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Lorsque vous avez terminé la mise à niveau, ou si les contrôles préalables échouent ou si vous choisissez de ne pas poursuivre la mise à niveau, vous devez Reconfigurer manuellement le médiateur ONTAP.

À n'importe quel stade de la mise à niveau, vous pouvez exécuter le `system controller replace show` ou `system controller replace show-details` Commande du site A pour vérifier le statut. Si les commandes renvoient une sortie vide, attendez quelques minutes et exécutez à nouveau la commande.

Étapes

1. Lancer la procédure de remplacement automatisé du contrôleur depuis le site A pour remplacer les contrôleurs du site B :

   ```
   system controller replace start -nso true
   ```

   L'opération automatisée exécute les contrôles préalables. Si aucun problème n'est trouvé, l'opération s'interrompt pour que vous puissiez collecter manuellement les informations relatives à la configuration.

- Si vous n'exécutez pas le `system controller replace start -nso true` La procédure de mise à niveau du contrôleur choisit le basculement et le rétablissement automatisés basés sur NSO comme procédure par défaut sur les systèmes IP MetroCluster.
- Le système source actuel et tous les systèmes cible compatibles sont affichés. Si vous avez remplacé le contrôleur source par un contrôleur possédant une version ONTAP différente ou une plateforme non compatible, l'opération d'automatisation s'arrête et signale une erreur après le démarrage des nouveaux nœuds. Pour rétablir l'état sain du cluster, il est nécessaire de suivre la procédure de restauration manuelle.

  Le `system controller replace start` la commande peut signaler l'erreur de vérification préalable suivante :

  ```
  Cluster-A::*>system controller replace show
  Node        Status         Error-Action
  ----------- --------------
  ------------------------------------
  Node-A-1    Failed         MetroCluster check failed.
  Reason : MCC check showed errors in component aggregates
  ```

  Vérifiez si cette erreur s'est produite parce que vous avez des agrégats non mis en miroir ou en raison d'un autre problème d'agrégat. Vérifiez que tous les agrégats en miroir sont sains et ne sont pas dégradés ou ne sont pas dégradés. Si cette erreur est due uniquement aux agrégats non mis en miroir, vous pouvez annuler cette erreur en sélectionnant le `-skip-metrocluster-check true` sur le `system controller replace start` commande. Si le stockage distant est accessible, les agrégats sans miroir sont connectés après le basculement. En cas de défaillance de la liaison de stockage distante, les agrégats non mis en miroir ne parviennent pas à se mettre en ligne.

2. Collectez manuellement les informations de configuration en se connectant sur le site B et en suivant les commandes répertoriées dans le message de la console sous le `system controller replace show` ou `system controller replace show-details` commande.

Collecte des informations avant la mise à niveau

Avant de procéder à la mise à niveau, si le volume racine est chiffré, vous devez vous fournir la clé de sauvegarde ainsi que d'autres informations permettant de démarrer les nouveaux contrôleurs avec les anciens volumes root chiffrés.

Description de la tâche

Cette tâche est effectuée sur la configuration IP MetroCluster existante.

Étapes

1. Etiqueter les câbles pour les contrôleurs existants afin de faciliter l'identification des câbles lors de la configuration des nouveaux contrôleurs.
2. Afficher les commandes pour capturer la clé de sauvegarde et d'autres informations :

   `system controller replace show`

Exécutez les commandes répertoriées sous le `show` commande provenant du cluster partenaire.

Le `show` Le résultat des commandes affiche trois tableaux contenant les adresses IP de l'interface MetroCluster, les ID système et les UUID du système. Ces informations sont requises plus tard dans la procédure pour définir les bootargs lorsque vous démarrez le nouveau noeud.

3. Collectez les ID système des nœuds de la configuration MetroCluster :

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Au cours de la procédure de mise à niveau, vous remplacerez ces anciens ID système par les ID système des nouveaux modules de contrôleur.

   Dans cet exemple, pour une configuration IP MetroCluster à quatre nœuds, les anciens ID de système suivants sont récupérés :

   - Node_A_1-Old : 4068741258
   - Node_A_2-Old : 4068741260
   - Node_B_1-Old : 4068741254
   - Node_B_2-Old : 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

   Dans cet exemple, pour une configuration IP MetroCluster à deux nœuds, les anciens ID de système suivants sont récupérés :

   - Node_A_1 : 4068741258
   - Node_B_1 : 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Collecte des informations relatives aux ports et aux LIF pour chaque ancien nœud.

   Vous devez collecter les valeurs de sortie des commandes suivantes pour chaque nœud :

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node-name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`

5. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés :

   `security key-manager backup show`

7. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les informations concernant les clés et les clés de phrase secrète.

   Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

   a. Si le gestionnaire de clés intégré est configuré :

```
security key-manager onboard show-backup
```

Vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

```
security key-manager external show -instance
```

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

8. Une fois que vous avez terminé de collecter les informations de configuration, reprenez l'opération :

```
system controller replace resume
```

Suppression de la configuration existante du logiciel disjoncteur d'attache ou autre logiciel de surveillance

Si la configuration existante est contrôlée avec la configuration MetroCluster Tiebreaker ou d'autres applications tierces (telles que ClusterLion) capables d'effectuer un basculement, vous devez supprimer la configuration MetroCluster du logiciel disjoncteur d'attache ou autre logiciel avant de remplacer l'ancien contrôleur.

Étapes

1. "Supprimez la configuration MetroCluster existante" À partir du logiciel disjoncteur d'attache.
2. Supprimez la configuration MetroCluster existante de toute application tierce pouvant effectuer le basculement.

   Reportez-vous à la documentation de l'application.

Remplacement des anciens contrôleurs et démarrage des nouveaux contrôleurs

Une fois que vous avez recueilli des informations et que vous reprenez l'opération, l'automatisation procède à l'opération de basculement.

Description de la tâche

L'opération d'automatisation lance les opérations de basculement. Une fois ces opérations terminées, l'opération s'interrompt à **interrompu pour l'intervention de l'utilisateur**. Vous pouvez ainsi installer les contrôleurs, démarrer les contrôleurs partenaires et réaffecter les disques d'agrégat racine au nouveau module de contrôleur à partir de la sauvegarde flash à l'aide de `sysids` rassemblés plus tôt.

Avant de commencer

Avant de lancer le basculement, l'automatisation s'interrompt pour que vous puissiez vérifier manuellement que toutes les LIF sont « en service » sur le site B. Si nécessaire, apportez toutes les LIF « propres » à « UP » et reprenez l'opération d'automatisation à l'aide du `system controller replace resume` commande.

Préparation de la configuration réseau des anciens contrôleurs

Pour assurer la reprise du réseau correctement sur les nouveaux contrôleurs, vous devez déplacer les LIF vers un port commun, puis supprimer la configuration réseau des anciens contrôleurs.

Description de la tâche

- Cette tâche doit être effectuée sur chacun des anciens nœuds.

- Vous utiliserez les informations recueillies dans Préparation à la mise à niveau.

Étapes

1. Démarrez les anciens nœuds, puis connectez-vous aux nœuds :

   `boot_ontap`

2. Assignez le port de base de toutes les LIFs de données de l'ancien contrôleur à un port commun identique sur les anciens et les nouveaux modules de contrôleur.

   a. Afficher les LIFs :

      `network interface show`

      Toutes LES LIF de données, y compris SAN et NAS, seront admin « up » et « possède » des opérations, car celles-ci se trouvent sur le site de basculement (cluster_A).

   b. Vérifiez le résultat de cette commande pour trouver un port réseau physique commun identique sur l'ancien et le nouveau contrôleur qui n'est pas utilisé comme port du cluster.

      Par exemple, « e0d » est un port physique des anciens contrôleurs et est également présent sur les nouveaux contrôleurs. « e0d » n'est pas utilisé comme port de cluster ou autre sur les nouveaux contrôleurs.

      Pour l'utilisation des ports pour les modèles de plate-forme, reportez-vous à la section "NetApp Hardware Universe"

   c. Modifier toutes LES LIFS de données pour utiliser le port commun comme port de base :

      `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

      Dans l'exemple suivant, il s'agit de ""e0d"".

      Par exemple :

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modifier les domaines de diffusion pour supprimer les VLAN et les ports physiques qui doivent être supprimés :

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Répétez cette étape pour tous les réseaux VLAN et les ports physiques.

4. Supprimez tous les ports VLAN utilisant des ports de cluster comme ports membres et groupes d'interfaces utilisant des ports de cluster comme ports membres.

   a. Supprimer les ports VLAN :

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Par exemple :

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Supprimez les ports physiques des groupes d'interface :

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Par exemple :

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Supprimer les ports VLAN et group d'interface de broadcast domain :

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modifiez les ports du groupe d'interface pour utiliser d'autres ports physiques comme membre :

`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

5. Arrêter les nœuds :

`halt -inhibit-takeover true -node node-name`

Cette étape doit être effectuée sur les deux nœuds.

Configuration des nouveaux contrôleurs

Vous devez installer et câbler les nouveaux contrôleurs.

Étapes

1. Planifiez le positionnement des nouveaux modules de contrôleur et tiroirs de stockage en fonction des besoins.

   L'espace rack dépend du modèle de plateforme des modules de contrôleur, des types de switchs et du nombre de tiroirs de stockage de votre configuration.

2. Mettez-vous à la terre.
3. Installez les modules de contrôleur sur le rack ou l'armoire.

   "Documentation des systèmes matériels ONTAP"

4. Si les nouveaux modules de contrôleur ne sont pas livrés avec eux-mêmes des cartes FC-VI et si les cartes FC-VI des anciens contrôleurs sont compatibles avec les nouveaux contrôleurs, remplacez les cartes FC-VI et installez-les dans les connecteurs appropriés.

   Voir la "NetApp Hardware Universe" Pour les informations sur les slots pour les cartes FC-VI.

5. Reliez les connexions d'alimentation, de console série et de gestion des contrôleurs, comme décrit dans les *MetroCluster - Guides d'installation et de configuration*.

Ne connectez pas d'autres câbles ayant été débranchés des anciens contrôleurs à l'heure actuelle.

"Documentation des systèmes matériels ONTAP"

6. Mettez les nouveaux nœuds sous tension et appuyez sur Ctrl-C lorsque vous êtes invité à afficher l'invite DU CHARGEUR.

Démarrage réseau des nouveaux contrôleurs

Une fois les nouveaux nœuds installés, vous devez démarrage sur le réseau pour vous assurer que la version des nouveaux nœuds exécute la même version de ONTAP que les nœuds d'origine. Le terme netboot signifie que vous êtes en cours de démarrage à partir d'une image ONTAP stockée sur un serveur distant. Lorsque vous vous préparez à netboot, vous devez placer une copie de l'image de démarrage ONTAP 9 sur un serveur web auquel le système peut accéder.

Cette tâche est effectuée sur chacun des nouveaux modules de contrôleur.

Étapes

1. Accédez au "Site de support NetApp" pour télécharger les fichiers utilisés pour effectuer le démarrage sur le réseau du système.
2. Téléchargez le logiciel ONTAP approprié depuis la section de téléchargement de logiciels du site du support NetApp et stockez le fichier ontap-version_image.tgz dans un répertoire accessible en ligne.
3. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.

   Votre liste de répertoires doit contenir un dossier netboot avec un fichier noyau : ontap-version_image.tgz

   Il n'est pas nécessaire d'extraire le fichier ontap-version_image.tgz.

4. À l'invite DU CHARGEUR, configurez la connexion netboot pour les LIF de gestion :
   - Si l'adressage IP est DHCP, configurez la connexion automatique :

     ```
     ifconfig e0M -auto
     ```

   - Si l'adressage IP est statique, configurez la connexion manuelle :

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Effectuer la démarrage sur le réseau.
   - Si la plate-forme est un système de la série 80xx, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Si la plateforme est un autre système, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Dans le menu de démarrage, sélectionnez l'option **(7) installer le nouveau logiciel en premier** pour télécharger et installer la nouvelle image logicielle sur le périphérique d'amorçage.

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
. Si vous êtes invité à poursuivre la procédure, entrez `y`, Et lorsque
vous êtes invité à saisir l'URL du fichier image :
`\http://web_server_ip/path_to_web-accessible_directory/ontap-
version_image.tgz`
```

```
Enter username/password if applicable, or press Enter to continue.
```

7. Assurez-vous d'entrer `n` pour ignorer la restauration de la sauvegarde lorsque vous voyez une invite similaire à la suivante :

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

8. Redémarrez en entrant `y` lorsque vous voyez une invite similaire à la suivante :

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

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   ```
   halt
   ```

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   ```
   set-defaults
   ```

3. Enregistrez l'environnement :

   ```
   saveenv
   ```

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   ```
   boot_ontap menu
   ```

5. À l'invite du menu de démarrage, effacez la configuration :

`wipeconfig`

Répondez `yes` à l'invite de confirmation.

Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

   Répondez `yes` à l'invite de confirmation.

Restauration de la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :

   a. Vérifiez les paramètres actuels des ports : `ucadmin show`

   b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Cible FC	`fcadmin config -t target` *`adapter-name`*
Initiateur FC	`fcadmin config -t initiator` *`adapter-name`*

2. Quitter le mode Maintenance :

   `halt`

   Une fois que vous avez exécuté la commande, attendez que le nœud s'arrête à l'invite DU CHARGEUR.

3. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet :

   `boot_ontap maint`

4. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`

FC	`fcadmin show`

Définissez l'état de haute disponibilité sur les nouveaux contrôleurs et châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état de haute disponibilité de tous les composants doit être `mccip`.

2. Si l'état système affiché du contrôleur ou du châssis n'est pas correct, définissez l'état HA :

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

3. Arrêter le nœud : `halt`

   Le nœud doit s'arrêter au niveau du `LOADER>` à l'invite.

4. Sur chaque nœud, vérifiez la date, l'heure et le fuseau horaire du système : `show date`
5. Si nécessaire, définissez la date en UTC ou GMT : `set date <mm/dd/yyyy>`
6. Vérifiez l'heure à l'aide de la commande suivante à l'invite de l'environnement d'amorçage : `show time`
7. Si nécessaire, définissez l'heure en UTC ou GMT : `set time <hh:mm:ss>`
8. Enregistrer les paramètres : `saveenv`
9. Collecter les variables d'environnement : `printenv`

Mettre à jour les fichiers RCF de commutateur afin de s'adapter aux nouvelles plateformes

Vous devez mettre à jour les commutateurs vers une configuration prenant en charge les nouveaux modèles de plate-forme.

Description de la tâche

Vous pouvez effectuer cette tâche sur le site contenant les contrôleurs en cours de mise à niveau. Dans les exemples présentés dans cette procédure, nous mettons d'abord à niveau site_B.

Les commutateurs du site_A seront mis à niveau lorsque les contrôleurs du site_A sont mis à niveau.

Étapes

1. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

   Suivez les étapes de la section correspondant à votre fournisseur de commutateur dans la section *MetroCluster IP installation and Configuration*.

"Installation et configuration de MetroCluster IP"

- "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
- "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

2. Téléchargez et installez les fichiers RCF.

   Suivez les étapes de la section correspondant au fournisseur de votre commutateur du "Installation et configuration de MetroCluster IP".

   - "Téléchargement et installation des fichiers RCF Broadcom"
   - "Téléchargement et installation des fichiers Cisco IP RCF"

Définissez les variables bootarg IP MetroCluster

Certaines valeurs d'amorçage MetroCluster IP doivent être configurées sur les nouveaux modules de contrôleur. Les valeurs doivent correspondre à celles configurées sur les anciens modules de contrôleur.

Description de la tâche

Dans cette tâche, vous utiliserez les UUID et les ID système identifiés précédemment dans la procédure de mise à niveau de "Collecte des informations avant la mise à niveau".

Étapes

1. Au `LOADER>` À l'invite, définissez les bootargs suivants sur les nouveaux nœuds à site_B :

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   L'exemple suivant définit les valeurs de node_B_1 en utilisant VLAN 120 pour le premier réseau et VLAN 130 pour le second réseau :

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   L'exemple suivant définit les valeurs de node_B_2 en utilisant VLAN 120 pour le premier réseau et VLAN 130 pour le second réseau :

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. Dans les nouveaux nœuds » `LOADER` À l'invite, définissez les UUID :

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID
```

a. Définissez les UUID sur node_B_1.

L'exemple suivant montre les commandes permettant de définir les UUID sur node_B_1 :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Définissez les UUID sur node_B_2 :

L'exemple suivant montre les commandes permettant de définir les UUID sur node_B_2 :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Si les systèmes d'origine ont été configurés pour ADP, à l'invite DU CHARGEUR des nœuds de remplacement, activez ADP :

```
setenv bootarg.mcc.adp_enabled true
```

4. Définissez les variables suivantes :

```
setenv bootarg.mcc.local_config_id original-sys-id

setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

Le `setenv bootarg.mcc.local_config_id` La variable doit être définie sur l'ID système du module de contrôleur **Original**, node_B_1.

a. Définissez les variables sur node_B_1.

L'exemple suivant montre les commandes permettant de définir les valeurs sur node_B_1 :

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Définissez les variables sur node_B_2.

L'exemple suivant montre les commandes permettant de définir les valeurs sur node_B_2 :

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Si vous utilisez le chiffrement avec un gestionnaire de clés externe, définissez les paramètres d'amorçage requis :

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Réaffectation des disques de l'agrégat racine

Réallouer les disques de l'agrégat racine vers le nouveau module de contrôleur, à l'aide du `sysids` rassemblés plus tôt

Description de la tâche

Cette tâche est effectuée en mode Maintenance.

Les anciens ID système ont été identifiés dans "Collecte des informations avant la mise à niveau".

Les exemples de cette procédure utilisent des contrôleurs avec les ID système suivants :

Nœud	Ancien ID système	Nouvel ID système
Nœud_B_1	4068741254	1574774970

Étapes

1. Reliez toutes les autres connexions aux nouveaux modules de contrôleur (FC-VI, stockage, interconnexion de cluster, etc.).
2. Arrêtez le système et démarrez en mode maintenance à partir de l'invite DU CHARGEUR :

```
boot_ontap maint
```

3. Afficher les disques détenus par le nœud_B_1-Old :

   `disk show -a`

   Le résultat de la commande affiche l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (4068741254). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers le nouveau contrôleur :

   `disk reassign -s old-sysid -d new-sysid`

   > Si votre système MetroCluster IP est configuré avec le partitionnement de disque avancé, vous devez inclure l'identifiant système partenaire de reprise sur incident en exécutant `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid` commande.

   L'exemple suivant montre la réaffectation de disques :

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Vérifier que tous les disques sont réaffectés comme prévu :

`disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                     POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------             -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Afficher le statut de l'agrégat :

   `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Répétez les étapes ci-dessus sur le nœud partenaire (node_B_2-New).

Démarrage des nouveaux contrôleurs

Vous devez redémarrer les contrôleurs à partir du menu de démarrage pour mettre à jour l'image flash du contrôleur. Des étapes supplémentaires sont nécessaires si le chiffrement est configuré.

Vous pouvez reconfigurer les VLAN et les groupes d'interface. Si nécessaire, modifier manuellement les ports des LIFs de cluster et des détails de broadcast domain avant de reprendre l'opération en utilisant le `system controller replace resume` commande.

Description de la tâche

Cette tâche doit être effectuée sur tous les nouveaux contrôleurs.

Étapes

1. Arrêter le nœud :

   `halt`

2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Afficher le menu de démarrage :

   `boot_ontap menu`

4. Si le cryptage racine est utilisé, sélectionnez l'option de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…

Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

5. Dans le menu de démarrage, exécutez l'option « 6 ».

   L'option « 6 » redémarre le nœud deux fois avant de terminer.

   Répondez « y » aux invites de changement d'ID système. Attendez les deuxième messages de redémarrage :

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

   Au cours de l'un des redémarrages après l'option « 6 », l'invite de confirmation `Override system ID? {y|n}` s'affiche. Entrez `y`.

6. Si le cryptage racine est utilisé, sélectionnez à nouveau l'option de menu d'amorçage pour la configuration de votre gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

   Selon le paramètre du gestionnaire de clés, effectuez la procédure de récupération en sélectionnant l'option « 10 » ou « 11 », suivie de l'option « 6 » à la première invite du menu d'amorçage. Pour démarrer complètement les nœuds, il est possible que vous deviez répéter la procédure de restauration suite à l'option « 1 » (démarrage normal).

7. Démarrez les nœuds :

`boot_ontap`

8. Attendez que les nœuds remplacés démarrent.

   Si l'un des nœuds est en mode basculement, exécutez un retour à l'aide du `storage failover giveback` commande.

9. Vérifier que tous les ports se trouvent dans un broadcast domain :

   a. Afficher les domaines de diffusion :

      `network port broadcast-domain show`

   b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

      "Ajout ou suppression de ports d'un broadcast domain"

   c. Ajoutez le port physique qui hébergera les LIFs intercluster sur le broadcast domain correspondant.

   d. Modifier les LIFs intercluster de façon à utiliser le nouveau port physique en tant que port de départ.

   e. Une fois les LIFs intercluster configurées, vérifiez le statut des clusters et redéfinissez le peering de cluster si nécessaire.

      Vous devrez peut-être reconfigurer le peering de cluster.

      "Création d'une relation entre clusters"

   f. Recréez les VLAN et les groupes d'interfaces selon les besoins.

      L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

      "Création d'un VLAN"

   "Combinaison de ports physiques pour créer des groupes d'interfaces"

   a. Vérifier que le cluster partenaire est accessible et que la configuration a été resynchronisée sur le cluster partenaire :

      `metrocluster switchback -simulate true`

10. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…
Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

11. Avant de reprendre l'opération, vérifiez que le MetroCluster est configuré correctement. Vérifier l'état du nœud :

    ```
    metrocluster node show
    ```

    Vérifiez que les nouveaux nœuds (site_B) sont dans **en attente de l'état de rétablissement** à partir de site_A.

12. Reprendre l'opération :

    ```
    system controller replace resume
    ```

Fin de la mise à niveau

L'automatisation exécute des vérifications du système, puis s'interrompt pour que vous puissiez vérifier la capacité d'accès au réseau. Une fois la vérification terminée, la phase de récupération des ressources est lancée, et l'opération d'automatisation exécute le rétablissement sur le site A et s'interrompt après les vérifications de mise à niveau. Une fois que vous avez rétabli l'opération d'automatisation, il effectue les vérifications post-mise à niveau et, si aucune erreur n'est détectée, marque la mise à niveau comme terminée.

Étapes

1. Vérifiez l'accessibilité du réseau en suivant le message de la console.
2. Une fois la vérification terminée, reprendre l'opération :

    ```
    system controller replace resume
    ```

3. L'opération d'automatisation est effectuée `heal-aggregate`, `heal-root-aggregate`, Et les opérations de rétablissement sur le site A, et les vérifications post-mise à niveau. Lorsque l'opération s'interrompt, vérifier manuellement le statut LIF SAN et vérifier la configuration du réseau en suivant le message de la console.
4. Une fois la vérification terminée, reprendre l'opération :

    ```
    system controller replace resume
    ```

5. Vérifier l'état des vérifications post-mise à niveau :

    ```
    system controller replace show
    ```

    Si les vérifications post-mise à niveau n'ont pas signalé d'erreurs, la mise à niveau est terminée.

6. Une fois la mise à niveau du contrôleur terminée, connectez-vous au site B et vérifiez que les contrôleurs remplacés sont configurés correctement.

Reconfigurer le médiateur ONTAP

Configurez manuellement le médiateur ONTAP qui a été automatiquement supprimé avant de commencer la mise à niveau.

1. Suivez les étapes de la section "Configurez le service Mediator ONTAP à partir d'une configuration IP MetroCluster".

Restauration du contrôle disjoncteur d'attache

Si le logiciel disjoncteur d'attache a déjà été configuré pour la surveillance de la configuration MetroCluster, vous pouvez restaurer la connexion ce dernier.

1. Suivez les étapes de la section "Ajout des configurations MetroCluster".

Mise à niveau des contrôleurs en une configuration MetroCluster FC à l'aide du basculement et du rétablissement

Il est possible d'utiliser le basculement MetroCluster pour fournir un service sans interruption aux clients pendant la mise à niveau des modules de contrôleur du cluster partenaire. Dans le cadre de cette procédure, d'autres composants (tels que des tiroirs de stockage ou des commutateurs) ne peuvent pas être mis à niveau.

Combinaisons de plateformes prises en charge

Vous pouvez mettre à niveau certaines plateformes en utilisant l'opération de basculement et de rétablissement dans une configuration MetroCluster FC.

Pour en savoir plus sur les combinaisons de mise à niveau de plateforme prises en charge, consultez le tableau des mises à niveau FC MetroCluster dans "Choisir la procédure de mise à niveau du contrôleur".

Reportez-vous à la section "Choisissez une méthode de mise à niveau ou de rafraîchissement" pour les procédures supplémentaires.

Description de la tâche

- Cette procédure ne peut être utilisée que pour la mise à niveau du contrôleur.

  Les autres composants de la configuration, tels que les tiroirs de stockage ou les commutateurs, ne peuvent pas être mis à niveau simultanément.

- Vous pouvez utiliser cette procédure avec certaines versions de ONTAP :
  - Les configurations à deux nœuds sont prises en charge par ONTAP 9.3 et versions ultérieures.
  - Les configurations à quatre et huit nœuds sont prises en charge dans ONTAP 9.8 et versions ultérieures.

    N'utilisez pas cette procédure pour des configurations à quatre ou huit nœuds exécutant les versions ONTAP antérieures à 9.8.

- Vos plateformes d'origine et nouvelles doivent être compatibles et prises en charge.

  "NetApp Hardware Universe"

  Si les plateformes d'origine ou nouvelles sont des systèmes FAS8020 ou AFF8020 utilisant les ports 1c et 1D en mode FC-VI, consultez l'article de la base de connaissances "Mise à niveau des contrôleurs lors des connexions FCVI sur les nœuds FAS8020 ou AFF8020 existants utilisent les ports 1c et 1D."

- Les licences des deux sites doivent correspondre. Vous pouvez obtenir de nouvelles licences à partir de "Support NetApp".
- Cette procédure s'applique aux modules de contrôleur dans une configuration MetroCluster FC (MetroCluster extensible à deux nœuds ou une configuration MetroCluster à deux, quatre ou huit nœuds).
- Tous les contrôleurs d'un même groupe de reprise sur incident doivent être mis à niveau pendant la même période de maintenance.

  L'exploitation de la configuration MetroCluster avec différents types de contrôleurs dans le même groupe de reprise sur incident n'est pas prise en charge en dehors de cette activité de maintenance. Pour les configurations MetroCluster à 8 nœuds, les contrôleurs d'un groupe de reprise après incident doivent être identiques, mais les deux groupes de reprise après incident peuvent utiliser différents types de contrôleur.
- Le mappage anticipé des connexions de stockage, FC et Ethernet entre les nœuds d'origine et les nouveaux nœuds est recommandé.
- Si la nouvelle plate-forme comporte moins de slots que le système d'origine ou si elle comporte moins ou différents types de ports, vous devrez peut-être ajouter un adaptateur au nouveau système.

  Pour plus d'informations, reportez-vous à la section "NetApp Hardware Universe"

Les exemples de noms suivants sont utilisés dans cette procédure :

- Site_A
  - Avant la mise à niveau :
    - Node_A_1-Old
    - Node_A_2-Old
  - Après la mise à niveau :
    - Node_A_1-New
    - Node_A_2-New
- Site_B
  - Avant la mise à niveau :
    - Node_B_1-Old
    - Node_B_2-Old
  - Après la mise à niveau :
    - Node_B_1-New
    - Node_B_2-New

Préparation de la mise à niveau

Avant d'apporter des modifications à la configuration MetroCluster existante, vous devez vérifier l'état de santé de la configuration, préparer les nouvelles plateformes et effectuer d'autres tâches diverses.

Vérification de l'état de santé de la configuration MetroCluster

Vous devez vérifier l'état de santé et la connectivité de la configuration MetroCluster avant d'effectuer la mise à niveau.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :

   a. Vérifiez si les nœuds sont multipathed :
   `node run -node node-name sysconfig -a`

      Vous devez exécuter cette commande pour chaque nœud de la configuration MetroCluster.

   b. Vérifier qu'il n'y a aucun disque défectueux dans la configuration :

      `storage disk show -broken`

      Vous devez exécuter cette commande sur chaque nœud de la configuration MetroCluster.

   c. Vérifiez si des alertes d'intégrité sont émises :

      `system health alert show`

      Vous devez exécuter cette commande sur chaque cluster.

   d. Vérifier les licences sur les clusters :

      `system license show`

      Vous devez exécuter cette commande sur chaque cluster.

   e. Vérifiez les périphériques connectés aux nœuds :

      `network device-discovery show`

      Vous devez exécuter cette commande sur chaque cluster.

   f. Vérifiez que le fuseau horaire et l'heure sont correctement définis sur les deux sites :

      `cluster date show`

   Vous devez exécuter cette commande sur chaque cluster. Vous pouvez utiliser le `cluster date` commandes permettant de configurer le fuseau horaire et le fuseau horaire.

2. Vérifier la présence d'alertes d'intégrité sur les commutateurs (le cas échéant) :

   `storage switch show`

   Vous devez exécuter cette commande sur chaque cluster.

3. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.
   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

      `metrocluster show`

   b. Vérifiez que tous les nœuds attendus s'affichent :

      `metrocluster node show`

   c. Exécutez la commande suivante :

```
metrocluster check run
```

d. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

4. Vérifiez le câblage MetroCluster à l'aide de l'outil Config Advisor.

a. Téléchargez et exécutez Config Advisor.

"Téléchargement NetApp : Config Advisor"

b. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.

Mappage des ports des anciens nœuds sur les nouveaux nœuds

Vous devez planifier le mappage des LIFs sur les ports physiques des anciens nœuds sur les ports physiques des nouveaux nœuds.

Description de la tâche

Une fois le nouveau nœud démarré au cours du processus de mise à niveau, la configuration la plus récente de l'ancien nœud qu'il remplace est retraitée. Lorsque vous démarrez node_A_1-New, ONTAP tente d'héberger les LIFs sur les mêmes ports qui ont été utilisés sur node_A_1-Old. Par conséquent, dans le cadre de la mise à niveau, vous devez ajuster la configuration du port et de la LIF afin qu'elle soit compatible avec celle de l'ancien nœud. Durant la procédure de mise à niveau, vous effectuez les étapes des anciens et nouveaux nœuds afin d'assurer une configuration correcte du cluster, de la gestion et de la LIF de données.

Le tableau suivant présente des exemples de modifications de configuration liées aux exigences de port des nouveaux nœuds.

Ports physiques d'interconnexion de cluster		
Ancien contrôleur	Nouveau contrôleur	Action requise
e0a, e0b	e3a, e3b	Aucun port correspondant. Après la mise à niveau, vous devez recréer les ports du cluster."Préparation des ports de cluster sur un module de contrôleur existant"
e0c, e0d	e0a,e0b,e0c,e0d	e0c et e0d sont des ports correspondants. Vous n'avez pas à modifier la configuration, mais après une mise à niveau, vous pouvez répartir les LIF de cluster entre les ports disponibles.

Étapes

1. Identifiez les ports physiques disponibles sur les nouveaux contrôleurs et les LIFs peuvent être hébergées sur les ports.

   L'utilisation des ports du contrôleur dépend du module de plate-forme et des commutateurs que vous utiliserez dans la configuration IP de MetroCluster. Vous pouvez collecter l'utilisation des ports des nouvelles plates-formes à partir du "NetApp Hardware Universe".

   Identifier également l'utilisation du slot de carte FC-VI.

2. Planifiez l'utilisation de vos ports et, le cas échéant, remplissez les tableaux suivants pour vous y référer

pour chacun des nouveaux nœuds.

Vous vous référez au tableau lors de la procédure de mise à niveau.

	Node_A_1-Old			Node_A_1-New		
LIF	Ports	Les IPspaces	Les domaines de diffusion	Ports	Les IPspaces	Les domaines de diffusion
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestion de nœuds						
Gestion du cluster						
Données 1						
Données 2						
Données 3						
Données 4						
SAN						
Port intercluster						

Collecte des informations avant la mise à niveau

Avant de procéder à la mise à niveau, vous devez recueillir des informations pour chacun des anciens nœuds et, si nécessaire, ajuster les domaines de diffusion réseau, supprimer les VLAN et les groupes d'interface et collecter des informations de chiffrement.

Description de la tâche

Cette tâche s'effectue sur la configuration FC MetroCluster existante.

Étapes

1. Etiqueter les câbles pour les contrôleurs existants, afin de faciliter l'identification des câbles lors de la configuration des nouveaux contrôleurs.

2. Collectez les ID système des nœuds de la configuration MetroCluster :

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Au cours de la procédure de mise à niveau, vous remplacerez ces anciens ID système par les ID système des nouveaux modules de contrôleur.

   Dans cet exemple de configuration FC MetroCluster à quatre nœuds, les anciens ID système suivants sont récupérés :

   - Node_A_1-Old : 4068741258
   - Node_A_2-Old : 4068741260
   - Node_B_1-Old : 4068741254
   - Node_B_2-Old : 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                        node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------- ------------------
-------------                  --------------------
--------------------             ----------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                        4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                        4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                         4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                        4068741260
4068741258
4 entries were displayed.
```

   Dans cet exemple de configuration FC MetroCluster à deux nœuds, les anciens ID système suivants sont récupérés :

   - Node_A_1 : 4068741258
   - Node_B_1 : 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Collecte des informations relatives aux ports et aux LIF pour chaque ancien nœud.

   Vous devez collecter les valeurs de sortie des commandes suivantes pour chaque nœud :

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node-name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`

4. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés :

   `security key-manager backup show`

6. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les informations concernant les clés et les clés de phrase secrète.

   Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

   a. Si le gestionnaire de clés intégré est configuré :

```
security key-manager onboard show-backup
```

Vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

```
security key-manager external show -instance
```

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

Suppression de la configuration existante du logiciel disjoncteur d'attache ou autre logiciel de surveillance

Si la configuration existante est contrôlée avec la configuration MetroCluster Tiebreaker ou d'autres applications tierces (telles que ClusterLion) capables d'effectuer un basculement, vous devez supprimer la configuration MetroCluster du logiciel disjoncteur d'attache ou d'autres logiciels avant la transition.

Étapes

1. Supprimer la configuration MetroCluster existante du logiciel disjoncteur d'attache

   "Suppression des configurations MetroCluster"

2. Supprimez la configuration MetroCluster existante de toute application tierce pouvant effectuer le basculement.

   Reportez-vous à la documentation de l'application.

Envoi d'un message AutoSupport personnalisé avant la maintenance

Avant d'effectuer la maintenance, vous devez envoyer un message AutoSupport pour informer le support technique de NetApp que la maintenance est en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Pour éviter la génération automatique de dossiers de demande de support, envoyez un message AutoSupport pour indiquer que la maintenance est en cours.

   a. Exécutez la commande suivante :

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   `maintenance-window-in-hours` spécifie la durée de la fenêtre de maintenance, avec un maximum de 72 heures. Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Répétez la commande sur le cluster partenaire.

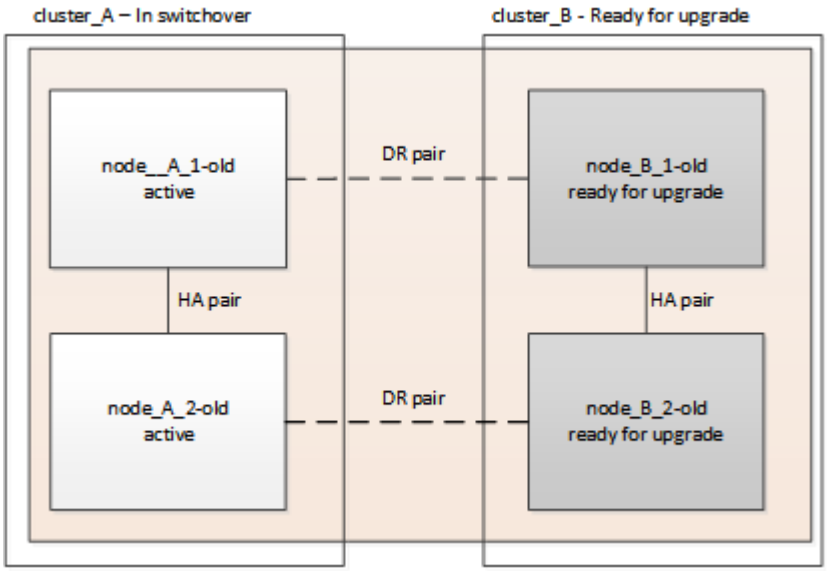
Commutation de la configuration MetroCluster

Vous devez basculer la configuration vers site_A afin de pouvoir mettre à niveau les plateformes du site_B.

Description de la tâche

Cette tâche doit être effectuée sur site_A.

Une fois cette tâche terminée, cluster_A est actif et assure le service des données des deux sites. Cluster_B est inactif et prêt à démarrer le processus de mise à niveau, comme illustré ci-dessous.



Étapes

1. Basculer la configuration MetroCluster sur site_A afin de mettre à niveau les nœuds site_B :
   a. Sélectionnez l'option qui correspond à votre configuration et exécutez la commande appropriée sur cluster_A :

      Option 1 : configuration FC à quatre ou huit nœuds exécutant ONTAP 9.8 ou une version ultérieure

      Lancer la commande : `metrocluster switchover -controller-replacement true`

      Option 2 : configuration FC à deux nœuds exécutant ONTAP 9.3 et versions ultérieures

      Lancer la commande : `metrocluster switchover`

      L'opération peut prendre plusieurs minutes.

   b. Surveiller le fonctionnement du basculement :

      ```
      metrocluster operation show
      ```

   c. Une fois l'opération terminée, vérifiez que les nœuds sont en état de basculement :

      ```
      metrocluster show
      ```

   d. Vérifier l'état des nœuds MetroCluster :

```
metrocluster node show
```

2. Corriger les agrégats de données.
   a. Réparation des agrégats de données :

   ```
   metrocluster heal data-aggregates
   ```

   b. Vérifiez que l'opération de correction est terminée en exécutant le `metrocluster operation show` commande sur le cluster sain :

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-aggregates
         State: successful
    Start Time: 7/29/2020 20:54:41
      End Time: 7/29/2020 20:54:42
        Errors: -
   ```

3. Corriger les agrégats racine.
   a. Réparation des agrégats de données :

   ```
   metrocluster heal root-aggregates
   ```

   b. Vérifiez que l'opération de correction est terminée en exécutant le `metrocluster operation show` commande sur le cluster sain :

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2020 20:58:41
      End Time: 7/29/2020 20:59:42
        Errors: -
   ```

Préparation de la configuration réseau des anciens contrôleurs

Pour assurer la reprise du réseau correctement sur les nouveaux contrôleurs, vous devez déplacer les LIF vers un port commun, puis supprimer la configuration réseau des anciens contrôleurs.

Description de la tâche

- Cette tâche doit être effectuée sur chacun des anciens nœuds.
- Vous utiliserez les informations recueillies dans "Mappage des ports des anciens nœuds sur les nouveaux nœuds".

Étapes

1. Démarrez les anciens nœuds, puis connectez-vous aux nœuds :

   ```
   boot_ontap
   ```

2. Assignez le port de base de toutes les LIFs de données de l'ancien contrôleur à un port commun identique sur les anciens et les nouveaux modules de contrôleur.

   a. Afficher les LIFs :

      `network interface show`

      Toutes LES LIF de données, y compris SAN et NAS, seront administrative et hors service, car celles-ci fonctionnent sur le site basculement (cluster_A).

   b. Vérifiez le résultat de cette commande pour trouver un port réseau physique commun identique sur l'ancien et le nouveau contrôleur qui n'est pas utilisé comme port du cluster.

      Ainsi, le port e0d est un port physique des anciens contrôleurs et il est également présent sur les nouveaux contrôleurs. e0d n'est pas utilisé comme port de cluster ou autre sur les nouveaux contrôleurs.

      Pour l'utilisation des ports pour les modèles de plate-forme, reportez-vous à la section "NetApp Hardware Universe"

   c. Modifier toutes LES LIFS de données pour utiliser le port commun comme port de base :

      `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

      Dans l'exemple suivant, il s'agit de « e0d ».

      Par exemple :

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modifier les domaines de diffusion pour supprimer les vlan et les ports physiques qui doivent être supprimés :

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Répétez cette étape pour tous les réseaux VLAN et les ports physiques.

4. Retirez tous les ports VLAN utilisant les ports de cluster comme ports membres et ifgrps utilisant les ports de cluster comme ports membres.

   a. Supprimer les ports VLAN :

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Par exemple :

```
network port vlan delete -node node1 -vlan-name e1c-80
```

   b. Supprimez les ports physiques des groupes d'interface :

```
network port ifgrp remove-port -node node-name -ifgrp interface-group-name
-port portid
```

Par exemple :

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Supprimer les ports VLAN et group d'interface de broadcast domain :

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Modifiez les ports du groupe d'interface pour utiliser d'autres ports physiques comme membre :

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Arrêter les nœuds :

```
halt -inhibit-takeover true -node node-name
```

Cette étape doit être effectuée sur les deux nœuds.

Retrait des anciennes plates-formes

Les anciens contrôleurs doivent être supprimés de la configuration.

Description de la tâche

Cette tâche est effectuée sur site_B.

Étapes

1. Se connecter à la console série des anciens contrôleurs (node_B_1-Old et node_B_2-Old) au site_B et vérifier qu'il affiche l'invite DU CHARGEUR.
2. Déconnectez les connexions de stockage et de réseau du nœud_B_1-Old et du nœud_B_2-Old et étiquetez les câbles pour qu'ils puissent être reconnectés aux nouveaux nœuds.
3. Déconnectez les câbles d'alimentation du nœud_B_1-Old et du nœud_B_2-Old.
4. Retirez le rack des contrôleurs node_B_1-Old et node_B_2-Old.

Configuration des nouveaux contrôleurs

Vous devez installer et installer les contrôleurs, effectuer la configuration requise en mode maintenance, puis démarrer les contrôleurs, et vérifier la configuration LIF sur les contrôleurs.

Configuration des nouveaux contrôleurs

Vous devez installer et câbler les nouveaux contrôleurs.

Étapes

1. Planifiez le positionnement des nouveaux modules de contrôleur et tiroirs de stockage en fonction des besoins.

L'espace rack dépend du modèle de plateforme des modules de contrôleur, des types de switchs et du nombre de tiroirs de stockage de votre configuration.

2. Mettez-vous à la terre.
3. Installez les modules de contrôleur sur le rack ou l'armoire.

   "Documentation des systèmes matériels ONTAP"

4. Si les nouveaux modules de contrôleur ne sont pas livrés avec eux-mêmes des cartes FC-VI et si les cartes FC-VI des anciens contrôleurs sont compatibles avec les nouveaux contrôleurs, remplacez les cartes FC-VI et installez-les dans les connecteurs appropriés.

   Voir la "NetApp Hardware Universe" Pour les informations sur les slots pour les cartes FC-VI.

5. Reliez les connexions d'alimentation, de console série et de gestion des contrôleurs, comme décrit dans les *MetroCluster - Guides d'installation et de configuration*.

   Ne connectez pas d'autres câbles ayant été débranchés des anciens contrôleurs à l'heure actuelle.

   "Documentation des systèmes matériels ONTAP"

6. Mettez les nouveaux nœuds sous tension et appuyez sur Ctrl-C lorsque vous êtes invité à afficher l'invite DU CHARGEUR.

Démarrage réseau des nouveaux contrôleurs

Une fois les nouveaux nœuds installés, vous devez démarrage sur le réseau pour vous assurer que la version des nouveaux nœuds exécute la même version de ONTAP que les nœuds d'origine. Le terme netboot signifie que vous êtes en cours de démarrage à partir d'une image ONTAP stockée sur un serveur distant. Lorsque vous vous préparez à netboot, vous devez placer une copie de l'image de démarrage ONTAP 9 sur un serveur web auquel le système peut accéder.

Cette tâche est effectuée sur chacun des nouveaux modules de contrôleur.

Étapes

1. Accédez au "Site de support NetApp" pour télécharger les fichiers utilisés pour effectuer le démarrage sur le réseau du système.
2. Téléchargez le logiciel ONTAP approprié depuis la section de téléchargement de logiciels du site du support NetApp et stockez le fichier ontap-version_image.tgz dans un répertoire accessible en ligne.
3. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.

Si le modèle de plateforme est…	Alors…
Systèmes de la gamme FAS/AFF8000	Extrayez le contenu d'ontap-version_image.tgzfile dans le répertoire cible : tar -zxvf ontap-version_image.tgz REMARQUE : si vous extrayez le contenu sous Windows, utilisez 7-Zip ou WinRAR pour extraire l'image netboot. Votre liste de répertoires doit contenir un dossier netboot avec un fichier de noyau:netboot/kernel

Tous les autres systèmes	Votre liste de répertoires doit contenir un dossier netboot avec un fichier du noyau : ontap-version_image.tgz vous n'avez pas besoin d'extraire le fichier ontap-version_image.tgz.

4. À l'invite DU CHARGEUR, configurez la connexion netboot pour les LIF de gestion :
   - Si l'adressage IP est DHCP, configurez la connexion automatique :

     ```
     ifconfig e0M -auto
     ```

   - Si l'adressage IP est statique, configurez la connexion manuelle :

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Effectuer la démarrage sur le réseau.
   - Si la plate-forme est un système de la série 80xx, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Si la plateforme est un autre système, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
     ```

6. Dans le menu de démarrage, sélectionnez l'option **(7) installer le nouveau logiciel en premier** pour télécharger et installer la nouvelle image logicielle sur le périphérique d'amorçage.

   ```
    Disregard the following message: "This procedure is not supported for Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive upgrades of software, not to upgrades of controllers.
   . Si vous êtes invité à poursuivre la procédure, entrez `y`, Et lorsque vous êtes invité à saisir l'URL du fichier image : `\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Assurez-vous d'entrer `n` pour ignorer la restauration de la sauvegarde lorsque vous voyez une invite similaire à la suivante :

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

8. Redémarrez en entrant `y` lorsque vous voyez une invite similaire à la suivante :

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

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   `halt`

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   `set-defaults`

3. Enregistrez l'environnement :

   `saveenv`

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   `boot_ontap menu`

5. À l'invite du menu de démarrage, effacez la configuration :

   `wipeconfig`

   Répondez `yes` à l'invite de confirmation.

   Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

   Répondez `yes` à l'invite de confirmation.

Restauration de la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :

   a. Vérifiez les paramètres actuels des ports : `ucadmin show`

   b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator adapter-name`
Ethernet CNA	`ucadmin modify -mode cna adapter-name`
Cible FC	`fcadmin config -t target adapter-name`
Initiateur FC	`fcadmin config -t initiator adapter-name`

2. Quitter le mode Maintenance :

   `halt`

   Une fois que vous avez exécuté la commande, attendez que le nœud s'arrête à l'invite DU CHARGEUR.

3. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet :

   `boot_ontap maint`

4. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`
FC	`fcadmin show`

Configuration de l'état haute disponibilité sur les nouveaux contrôleurs et le châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état HA pour tous les composants doit être mcc.

Si la configuration MetroCluster a…	L'état de la HA doit être…
Deux nœuds	mcc-2n
Quatre ou huit nœuds	mcc

2. Si l'état du système affiché du contrôleur n'est pas correct, définissez l'état HA pour le module de contrôleur et le châssis :

Si la configuration MetroCluster a…	Lancer ces commandes…

Deux nœuds	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Quatre ou huit noeuds	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Réaffectation des disques de l'agrégat racine

Réaffectez les disques de l'agrégat racine au nouveau module de contrôleur, en utilisant les sysids réunis précédemment

Description de la tâche

Cette tâche est effectuée en mode Maintenance.

Les anciens ID système ont été identifiés dans "Collecte des informations avant la mise à niveau".

Les exemples de cette procédure utilisent des contrôleurs avec les ID système suivants :

Nœud	Ancien ID système	Nouvel ID système
Nœud_B_1	4068741254	1574774970

Étapes

1. Reliez toutes les autres connexions aux nouveaux modules de contrôleur (FC-VI, stockage, interconnexion de cluster, etc.).
2. Arrêtez le système et démarrez en mode maintenance à partir de l'invite DU CHARGEUR :

   ```
   boot_ontap maint
   ```

3. Afficher les disques détenus par le nœud_B_1-Old :

   ```
   disk show -a
   ```

   Le résultat de la commande affiche l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (4068741254). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers le nouveau contrôleur :

   `disk reassign -s old-sysid -d new-sysid`

   L'exemple suivant montre la réaffectation de disques :

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Vérifier que tous les disques sont réaffectés comme prévu :

   `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                     POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------             -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Afficher le statut de l'agrégat :

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status            Options
   aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                              mirrored
   mirror_resync_priority=high(fixed)
                              fast zeroed
                              64-bit
   ```

7. Répétez les étapes ci-dessus sur le nœud partenaire (node_B_2-New).

Démarrage des nouveaux contrôleurs

Vous devez redémarrer les contrôleurs à partir du menu de démarrage pour mettre à jour l'image flash du contrôleur. Des étapes supplémentaires sont nécessaires si le chiffrement est configuré.

Description de la tâche

Cette tâche doit être effectuée sur tous les nouveaux contrôleurs.

Étapes

1. Arrêter le nœud :

   ```
   halt
   ```

2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Afficher le menu de démarrage :

   ```
   boot_ontap menu
   ```

4. Si le cryptage racine est utilisé, en fonction de la version de ONTAP que vous utilisez, sélectionnez l'option du menu de démarrage ou lancez la commande du menu de démarrage pour votre configuration de gestion des clés.

ONTAP 9.8 et versions ultérieures

Depuis ONTAP 9.8, sélectionnez l'option de menu de démarrage.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

ONTAP 9.7 et versions antérieures

Pour ONTAP 9.7 et les versions antérieures, exécutez la commande boot menu.

Si vous utilisez…	Exécutez cette commande à l'invite du menu de démarrage…
Gestion intégrée des clés	`recover_onboard_keymanager`
Gestion externe des clés	`recover_external_keymanager`

5. Si AUTOBOOT est activé, interrompez l'AUTOBOOT en appuyant sur CTRL-C.
6. Dans le menu de démarrage, exécutez l'option « 6 ».

   L'option « 6 » redémarre le nœud deux fois avant de terminer.

   Répondez « y » aux invites de changement d'ID système. Attendez les deuxième messages de redémarrage :

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Vérifiez que le partenaire-sysid est correct :

   ```
   printenv partner-sysid
   ```

   Si le partenaire-sysid n'est pas correct, définissez-le :

```
setenv partner-sysid partner-sysID
```

8. Si le cryptage racine est utilisé, en fonction de la version de ONTAP que vous utilisez, sélectionnez l'option du menu de démarrage ou exécutez de nouveau la commande du menu de démarrage pour la configuration de la gestion des clés.

ONTAP 9.8 et versions ultérieures

Depuis ONTAP 9.8, sélectionnez l'option de menu de démarrage.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

Selon le paramètre du gestionnaire de clés, effectuez la procédure de récupération en sélectionnant l'option « 10 » ou « 11 », suivie de l'option « 6 » à la première invite du menu d'amorçage. Pour démarrer complètement les nœuds, il est possible que vous deviez répéter la procédure de restauration suite à l'option « 1 » (démarrage normal).

ONTAP 9.7 et versions antérieures

Pour ONTAP 9.7 et les versions antérieures, exécutez la commande boot menu.

Si vous utilisez…	Exécutez cette commande à l'invite du menu de démarrage…
Gestion intégrée des clés	`recover_onboard_keymanager`
Gestion externe des clés	`recover_external_keymanager`

Vous devrez peut-être émettre le `recover_xxxxxxxx_keymanager` commande à l'invite du menu de démarrage plusieurs fois jusqu'à ce que les nœuds démarrent entièrement.

9. Démarrez les nœuds :

```
boot_ontap
```

10. Attendez que les nœuds remplacés démarrent.

Si l'un des nœuds est en mode basculement, exécutez un retour :

```
storage failover giveback
```

11. Vérifier que tous les ports se trouvent dans un broadcast domain :

    a. Afficher les domaines de diffusion :

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

    b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

    "Ajout ou suppression de ports d'un broadcast domain"

    c. Ajoutez le port physique qui hébergera les LIFs intercluster sur le Broadcast domain correspondant.

    d. Modifier les LIFs intercluster de façon à utiliser le nouveau port physique en tant que port de départ.

    e. Une fois les LIFs intercluster configurées, vérifiez le statut des clusters et redéfinissez le peering de cluster si nécessaire.

    Vous devrez peut-être reconfigurer le peering de cluster.

    "Création d'une relation entre clusters"

    f. Recréez les VLAN et les groupes d'interfaces selon les besoins.

    L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

    "Création d'un VLAN"

    "Combinaison de ports physiques pour créer des groupes d'interfaces"

12. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…
Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Vérification de la configuration de LIF

Vérifiez que les LIF sont hébergées sur le nœud/port approprié avant le rétablissement. Les étapes suivantes doivent être effectuées

Description de la tâche

Cette tâche s'effectue sur site_B, où les nœuds ont été démarrés avec des agrégats racine.

Étapes

1. Vérifiez que les LIF sont hébergées sur le nœud et les ports appropriés avant le rétablissement.

a. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

b. Remplacez la configuration des ports pour assurer un placement LIF approprié :

```
vserver config override -command "network interface modify -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node new_node_name"
```

Lors de la saisie du `network interface modify` dans la commande `vserver config override` vous ne pouvez pas utiliser la fonction de saisie semi-automatique de l'onglet. Vous pouvez créer le `network interface modify` à l'aide de la commande auto complete, puis placez-la dans le `vserver config override` commande.

a. Revenir au niveau de privilège admin :
`set -privilege admin`

2. Revert les interfaces sur leur home node :

```
network interface revert * -vserver vserver-name
```

Suivez cette étape sur tous les SVM, si nécessaire.

Installez les nouvelles licences

Avant l'opération de rétablissement, vous devez installer les licences des nouveaux contrôleurs.

Étapes

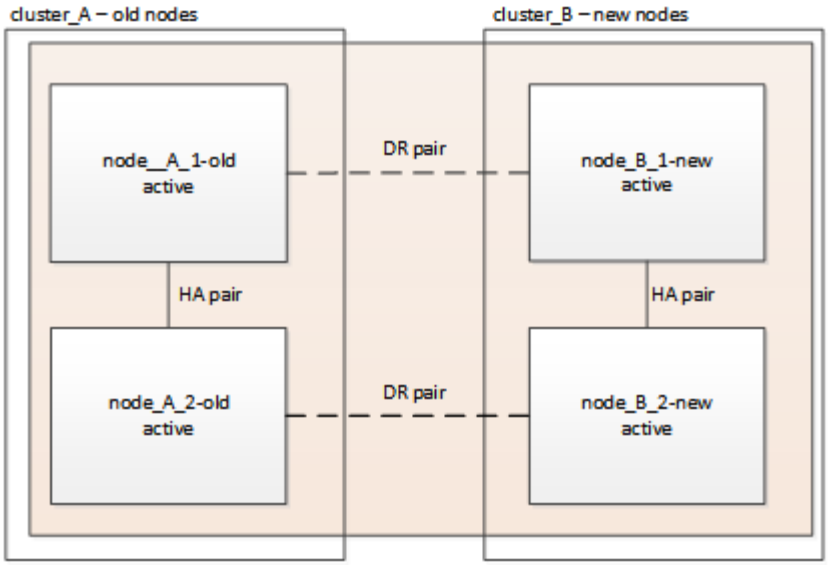
1. "Installation des licences pour le nouveau module de contrôleur"

Reprise de la configuration MetroCluster

Une fois les nouveaux contrôleurs configurés, il suffit de revenir à la configuration MetroCluster pour rétablir le fonctionnement normal.

Description de la tâche

Cette tâche vous permet d'effectuer le rétablissement et de rétablir le fonctionnement normal de la configuration MetroCluster. Les nœuds du site_A sont toujours en attente de mise à niveau.



Étapes

1. Émettez le `metrocluster node show` Commande on site_B et vérifiez la sortie.
   a. Vérifiez que les nouveaux nœuds sont correctement représentés.
   b. Vérifiez que les nouveaux nœuds sont en attente de rétablissement.
2. Rétablissement du cluster :

   ```
   metrocluster switchback
   ```

3. Vérifier la progression de l'opération de rétablissement :

   ```
   metrocluster show
   ```

   L'opération de rétablissement est toujours en cours lorsque la sortie s'affiche `waiting-for-switchback`:

   ```
   cluster_B::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_B         Configuration state configured
                             Mode                switchover
                             AUSO Failure Domain -
   Remote: cluster_A         Configuration state configured
                             Mode                waiting-for-switchback
                             AUSO Failure Domain -
   ```

   L'opération de rétablissement est terminée lorsque la sortie s'affiche `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Si un rétablissement prend beaucoup de temps, vous pouvez vérifier l'état des lignes de base en cours en utilisant le `metrocluster config-replication resync-status show` commande. Cette commande est au niveau de privilège avancé.

Vérification de l'état de santé de la configuration MetroCluster

Après la mise à niveau des modules de contrôleur, vous devez vérifier l'état de santé de la configuration MetroCluster.

Description de la tâche

Cette tâche peut être effectuée sur n'importe quel nœud de la configuration MetroCluster.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster :

   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

      `metrocluster show`

   b. Effectuer une vérification MetroCluster :

      `metrocluster check run`

   c. Afficher les résultats de la vérification MetroCluster :

      `metrocluster check show`

   Après avoir exécuté `metrocluster check run` et `metrocluster check show`, un message d'erreur similaire à ce qui suit s'affiche :

Exemple

```
Failed to validate the node and cluster components before the switchover
operation.
                  Cluster_A:: node_A_1 (non-overridable veto): DR
partner NVLog mirroring is not online. Make sure that the links between
the two sites are healthy and properly configured.
```

+ Ce comportement est attendu en raison d'une incompatibilité du contrôleur pendant le processus de mise à niveau et le message d'erreur peut être ignoré en toute sécurité.

Mise à niveau des nœuds du cluster_A

Vous devez répéter les tâches de mise à niveau sur cluster_A.

Étape

1. Répétez les étapes pour mettre à niveau les nœuds du cluster_A, en commençant par "Préparation de la mise à niveau".

   Au fur et à mesure que vous effectuez les tâches, toutes les références aux clusters et aux nœuds sont inversées. Par exemple, si vous avez l'intention de basculer du cluster_A, vous effectuez le basculement du cluster_B.

Envoi d'un message AutoSupport personnalisé après maintenance

Une fois la mise à niveau terminée, envoyer un message AutoSupport indiquant la fin de la maintenance. La création automatique de dossier peut reprendre.

Étape

1. Pour reprendre la génération automatique de dossier de support, envoyez un message AutoSupport pour indiquer que la maintenance est terminée.
   a. Exécutez la commande suivante :

      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```

   b. Répétez la commande sur le cluster partenaire.

Restauration du contrôle disjoncteur d'attache

Si le logiciel disjoncteur d'attache a déjà été configuré pour la surveillance de la configuration MetroCluster, vous pouvez restaurer la connexion ce dernier.

1. Suivez les étapes de la section "Ajout des configurations MetroCluster" Dans *MetroCluster Tiebreaker installation et configuration*.

Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 en configuration FC MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure)

Il est possible d'utiliser le basculement MetroCluster pour fournir un service sans interruption aux clients pendant la mise à niveau des modules de contrôleur du cluster partenaire. Dans le cadre de cette procédure, vous ne pouvez pas mettre à niveau d'autres composants (par exemple, des tiroirs de stockage ou des commutateurs).

Description de la tâche

- Cette procédure ne peut être utilisée que pour la mise à niveau du contrôleur.

Vous ne pouvez pas mettre à niveau d'autres composants de la configuration, par exemple des tiroirs de stockage ou des commutateurs, en même temps.

- Cette procédure permet de mettre à niveau un système AFF A700 vers un système AFF A900 avec ONTAP 9.10.1 ou version ultérieure.
- Cette procédure permet de mettre à niveau un système FAS9000 vers un système FAS9500 avec ONTAP 9.10.1P3 ou version ultérieure.
  - Les configurations à quatre et huit nœuds sont prises en charge par ONTAP 9.10.1 et les versions ultérieures.

    Le système AFF A900 n'est pris en charge que dans ONTAP 9.10.1 ou version ultérieure.

  "NetApp Hardware Universe"

- Tous les contrôleurs de la configuration doivent être mis à niveau pendant la même période de maintenance.

  Le tableau suivant présente la matrice de modèles prise en charge pour la mise à niveau du contrôleur.

Ancien modèle de plateforme	Nouveau modèle de plateforme
• AFF A700	• AFF A900
• FAS9000	• FAS9500

- Durant la procédure de mise à niveau, vous devez modifier la structure MetroCluster, notamment la FCR et les modifications physiques du câblage. Vous pouvez modifier la FCR et le câblage avant d'effectuer la mise à niveau du contrôleur.
- Cette procédure de mise à niveau ne requiert pas de modifier les connexions de stockage, FC et Ethernet entre les nœuds d'origine et les nouveaux nœuds.
- Durant la procédure de mise à niveau, vous ne devez pas ajouter ou supprimer d'autres cartes des systèmes AFF A700 ou FAS9000. Pour plus d'informations, reportez-vous à la section "NetApp Hardware Universe"

Les exemples de noms suivants sont utilisés dans les exemples et les graphiques de cette procédure :

- Site_A
  - Avant la mise à niveau :
    - Nœud_A_1-A700
    - Nœud_A_2-A700
  - Après la mise à niveau :
    - Node_A_1-A900
    - Node_A_2-A900
- Site_B
  - Avant la mise à niveau :

        - Node_B_1-A700
        - Node_B_2-A700
    - Après la mise à niveau :
        - Node_B_1-A900
        - Node_B_2-A900

Préparation à la mise à niveau

Avant d'apporter des modifications à la configuration MetroCluster existante, vous devez vérifier l'état de santé de la configuration, modifier les fichiers RCF et le câblage afin qu'ils correspondent à la nouvelle topologie de connectivité des ports requise pour la configuration AFF A900 ou FAS9000 Fabric MetroCluster, et effectuer d'autres tâches diverses.

Dégager le slot 7 sur le contrôleur AFF A700

La configuration MetroCluster sur un système AFF A900 ou FAS9500 requiert 8 ports FC-VI sur les cartes FC-VI, dans les emplacements 5 et 7. Avant de commencer la mise à niveau, si des cartes se trouvent dans l'emplacement 7 des systèmes AFF A700 ou FAS9000, vous devez les déplacer vers d'autres emplacements pour tous les nœuds du cluster.

Vérifier l'état de santé de la configuration MetroCluster

Avant de mettre à jour les fichiers RCF et le câblage de la configuration Fabric MetroCluster AFF A900 ou FAS9500, vous devez vérifier l'état et la connectivité de la configuration.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :

    a. Vérifiez si les nœuds sont multipathed :
    `node run -node node-name sysconfig -a`

    Vous devez exécuter cette commande pour chaque nœud de la configuration MetroCluster.

    b. Vérifier qu'il n'y a aucun disque défectueux dans la configuration :

    `storage disk show -broken`

    Vous devez exécuter cette commande sur chaque nœud de la configuration MetroCluster.

    c. Vérifiez si des alertes d'intégrité sont émises :

    `system health alert show`

    Vous devez exécuter cette commande sur chaque cluster.

    d. Vérifier les licences sur les clusters :

    `system license show`

    Vous devez exécuter cette commande sur chaque cluster.

    e. Vérifiez les périphériques connectés aux nœuds :

```
network device-discovery show
```

Vous devez exécuter cette commande sur chaque cluster.

f. Vérifiez que le fuseau horaire et l'heure sont correctement définis sur les deux sites :

```
cluster date show
```

Vous devez exécuter cette commande sur chaque cluster. Vous pouvez utiliser le `cluster date` commandes permettant de configurer le fuseau horaire et le fuseau horaire.

2. Vérifier la présence d'alertes d'intégrité sur les commutateurs (le cas échéant) :

```
storage switch show
```

Vous devez exécuter cette commande sur chaque cluster.

3. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.
   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

```
metrocluster show
```

   b. Vérifiez que tous les nœuds attendus s'affichent :

```
metrocluster node show
```

   c. Exécutez la commande suivante :

```
metrocluster check run
```

   d. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

4. Vérifiez le câblage MetroCluster à l'aide de l'outil Config Advisor.
   a. Téléchargez et exécutez Config Advisor.

   "Téléchargement NetApp : Config Advisor"

   b. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.

Mettre à jour les fichiers RCF de commutateur de structure

La structure MetroCluster AFF A900 ou FAS9500 exige deux adaptateurs FC-VI à quatre ports par nœud contre un seul adaptateur FC-VI à quatre ports requis par un système AFF A700. Avant de commencer la mise à niveau du contrôleur vers le contrôleur AFF A900 ou FAS9500, vous devez modifier les fichiers RCF de commutateur de structure pour prendre en charge la topologie de connexion AFF A900 ou FAS9500.

1. À partir du "Page de téléchargement du fichier RCF MetroCluster", Téléchargez le fichier RCF approprié pour un MetroCluster de structure AFF A900 ou FAS9500 et le modèle de switch utilisé avec la configuration AFF A700 ou FAS9000.
2. mettre à jour le fichier RCF sur les commutateurs de la structure A, commutateur A1 et commutateur B1

en suivant les étapes de la "Configuration des commutateurs FC".

> La mise à jour du fichier RCF pour prendre en charge la configuration AFF A900 ou FAS9500 Fabric MetroCluster n'affecte pas le port ni les connexions utilisés pour la configuration AFF A700 ou FAS9000 Fabric MetroCluster.

3. Après la mise à jour des fichiers RCF sur les commutateurs de la structure A, toutes les connexions FC-VI et de stockage doivent être mises en ligne. Vérifier les connexions FC-VI :

   `metrocluster interconnect mirror show`

   a. Vérifiez que les disques des sites locaux et distants sont répertoriés dans le `sysconfig` sortie.

4. vous devez vérifier que MetroCluster est en état de santé après la mise à jour du fichier RCF pour les commutateurs de la structure A.

   a. Vérifier les connexions du cluster en métro : `metrocluster interconnect mirror show`

   b. Exécuter la vérification MetroCluster : `metrocluster check run`

   c. Consultez les résultats de l'exécution MetroCluster une fois l'exécution terminée : `metrocluster check show`

5. Mettre à jour les commutateurs de la structure B (commutateurs 2 et 4) en répétant Étape 2 à Étape 5.

Vérifiez l'état de santé de la configuration MetroCluster après la mise à jour du fichier RCF

Vous devez vérifier l'état et la connectivité de la configuration MetroCluster avant d'effectuer la mise à niveau.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :

   a. Vérifiez si les nœuds sont multipathed :
   `node run -node node-name sysconfig -a`

   Vous devez exécuter cette commande pour chaque nœud de la configuration MetroCluster.

   b. Vérifier qu'il n'y a aucun disque défectueux dans la configuration :

   `storage disk show -broken`

   Vous devez exécuter cette commande sur chaque nœud de la configuration MetroCluster.

   c. Vérifiez si des alertes d'intégrité sont émises :

   `system health alert show`

   Vous devez exécuter cette commande sur chaque cluster.

   d. Vérifier les licences sur les clusters :

   `system license show`

   Vous devez exécuter cette commande sur chaque cluster.

   e. Vérifiez les périphériques connectés aux nœuds :

```
network device-discovery show
```

Vous devez exécuter cette commande sur chaque cluster.

f. Vérifiez que le fuseau horaire et l'heure sont correctement définis sur les deux sites :

```
cluster date show
```

Vous devez exécuter cette commande sur chaque cluster. Vous pouvez utiliser le `cluster date` commandes permettant de configurer le fuseau horaire et le fuseau horaire.

2. Vérifier la présence d'alertes d'intégrité sur les commutateurs (le cas échéant) :

```
storage switch show
```

Vous devez exécuter cette commande sur chaque cluster.

3. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.
   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

```
metrocluster show
```

   b. Vérifiez que tous les nœuds attendus s'affichent :

```
metrocluster node show
```

   c. Exécutez la commande suivante :

```
metrocluster check run
```

   d. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

4. Vérifiez le câblage MetroCluster à l'aide de l'outil Config Advisor.
   a. Téléchargez et exécutez Config Advisor.

   "Téléchargement NetApp : Config Advisor"

   b. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.

Mappez les ports des nœuds AFF A700 ou FAS9000 sur les nœuds AFF A900 ou FAS9500

Durant le processus de mise à niveau du contrôleur, il faut uniquement modifier les connexions mentionnées dans cette procédure.

Si le connecteur 7 des contrôleurs AFF A700 ou FAS9000 est associé à une carte, vous devez la déplacer vers un autre emplacement avant de lancer la procédure de mise à niveau du contrôleur. Vous devez disposer d'un emplacement 7 disponible pour l'ajout du deuxième adaptateur FC-VI requis pour le fonctionnement de Fabric MetroCluster sur les contrôleurs AFF A900 ou FAS9500.

Recueillez les informations avant la mise à niveau

Avant de procéder à la mise à niveau, vous devez recueillir des informations pour chacun des anciens nœuds et, si nécessaire, ajuster les domaines de diffusion réseau, supprimer les VLAN et les groupes d'interface et collecter des informations de chiffrement.

Description de la tâche

Cette tâche s'effectue sur la configuration FC MetroCluster existante.

Étapes

1. Collectez les ID système du nœud de configuration MetroCluster :

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Au cours de la procédure de mise à niveau, vous remplacerez ces anciens ID système par les ID système des modules de contrôleur.

   Dans cet exemple de configuration FC MetroCluster à quatre nœuds, les anciens ID système suivants sont récupérés :

   - Node_A_1-A700 : 537037649
   - Node_A_2-A700 : 537407030
   - Node_B_1-A700 : 0537407114
   - Node_B_2-A700 : 537035354

   ```
   Cluster_A::*> metrocluster node show -fields node-systemid,ha-partner-
   systemid,dr-partner-systemid,dr-auxiliary-systemid
   dr-group-id cluster    node           node-systemid ha-partner-systemid
   dr-partner-systemid dr-auxiliary-systemid
   ----------- ------------------------- ------------- -------------------
   ------------------- ---------------------
   1           Cluster_A  nodeA_1-A700   537407114     537035354
   537411005           537410611
   1           Cluster_A  nodeA_2-A700   537035354     537407114
   537410611           537411005
   1           Cluster_B  nodeB_1-A700   537410611     537411005
   537035354           537407114
   1           Cluster_B  nodeB_2-A700   537411005

   4 entries were displayed.
   ```

2. Collecte des informations relatives aux ports et aux LIF pour chaque ancien nœud.

   Vous devez collecter les valeurs de sortie des commandes suivantes pour chaque nœud :

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node-name -type physical`
   - `network port vlan show -node node-name`

- `network port ifgrp show -node node_name -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

3. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

4. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés :

   `security key-manager backup show`

5. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les informations concernant les clés et les clés de phrase secrète.

   Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

   a. Si le gestionnaire de clés intégré est configuré :

      `security key-manager onboard show-backup`

      Vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

   b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

      `security key-manager external show -instance`

   `security key-manager key query`

Supprimez la configuration existante du logiciel disjoncteur d'attache ou tout autre logiciel de surveillance

Si la configuration existante est contrôlée avec la configuration MetroCluster Tiebreaker ou d'autres applications tierces (telles que ClusterLion) capables d'effectuer un basculement, vous devez supprimer la configuration MetroCluster du logiciel disjoncteur d'attache ou d'autres logiciels avant la transition.

Étapes

1. Supprimer la configuration MetroCluster existante du logiciel disjoncteur d'attache

"Suppression des configurations MetroCluster"

2. Supprimez la configuration MetroCluster existante de toute application tierce pouvant effectuer le basculement.

   Reportez-vous à la documentation de l'application.

Envoyer un message AutoSupport personnalisé avant la maintenance

Avant d'effectuer la maintenance, vous devez envoyer un message AutoSupport pour informer le support technique de NetApp que la maintenance est en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Pour éviter la génération automatique de dossiers de demande de support, envoyez un message AutoSupport pour indiquer que la maintenance est en cours.

   a. Exécutez la commande suivante :

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` spécifie la durée de la fenêtre de maintenance, avec un maximum de 72 heures. Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Répétez la commande sur le cluster partenaire.

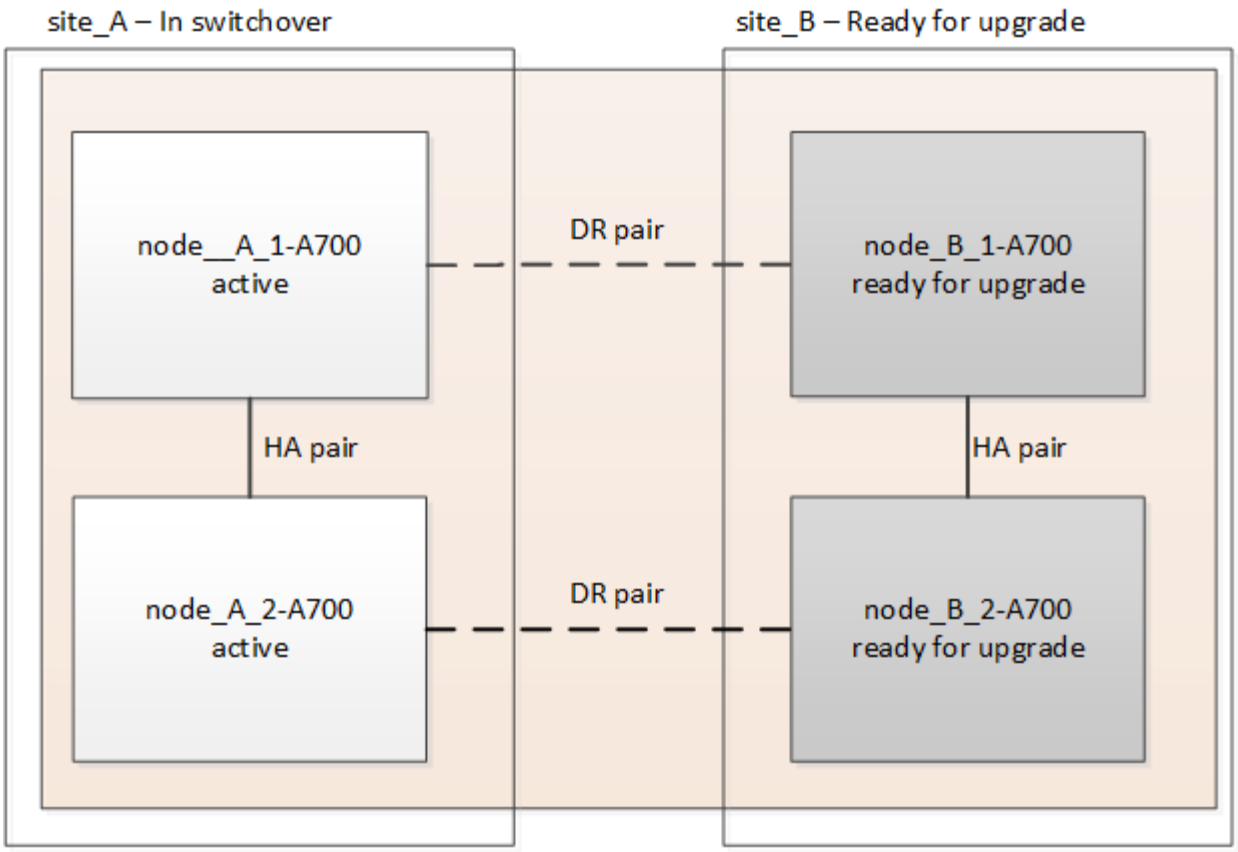
Basculer la configuration MetroCluster

Vous devez basculer la configuration vers site_A afin de pouvoir mettre à niveau les plateformes du site_B.

Description de la tâche

Cette tâche doit être effectuée sur site_A.

Une fois cette tâche effectuée, site_A est actif et transmet les données aux deux sites. Site_B est inactif et prêt à commencer le processus de mise à niveau, comme indiqué dans l'illustration suivante. (Cette illustration s'applique également à la mise à niveau d'un système FAS9000 vers un contrôleur FAS9500.)



Étapes

1. Basculer la configuration MetroCluster sur site_A afin de mettre à niveau les nœuds site_B :

   a. Exécutez la commande suivante sur site_A :

      `metrocluster switchover -controller-replacement true`

   L'opération peut prendre plusieurs minutes.

   a. Surveiller le fonctionnement du basculement :

      `metrocluster operation show`

   b. Une fois l'opération terminée, vérifiez que les nœuds sont en état de basculement :

      `metrocluster show`

   c. Vérifier l'état des nœuds MetroCluster :

      `metrocluster node show`

2. Corriger les agrégats de données.

   a. Réparation des agrégats de données :

      `metrocluster heal data-aggregates`

   b. Vérifiez que l'opération de correction est terminée en exécutant le `metrocluster operation show` commande sur le cluster sain :

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Corriger les agrégats racine.
   a. Réparation des agrégats de données :

      `metrocluster heal root-aggregates`

   b. Vérifiez que l'opération de correction est terminée en exécutant le `metrocluster operation show` commande sur le cluster sain :

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Retirez le module de contrôleur AFF A700 ou FAS9000 et le système NVS sur site_B

Vous devez supprimer les anciens contrôleurs de la configuration.

Cette tâche est effectuée sur site_B.

Avant de commencer

Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.

Étapes

1. Se connecter à la console série des anciens contrôleurs (node_B_1-700 et node_B_2-700) au site_B et vérifier qu'il affiche le `LOADER` à l'invite.
2. Rassemblez les valeurs de bootarg à partir des deux nœuds sur site_B : `printenv`
3. Mettez le châssis hors tension au niveau du site_B.

Retirez le module de contrôleur et NVS des deux nœuds du site_B.

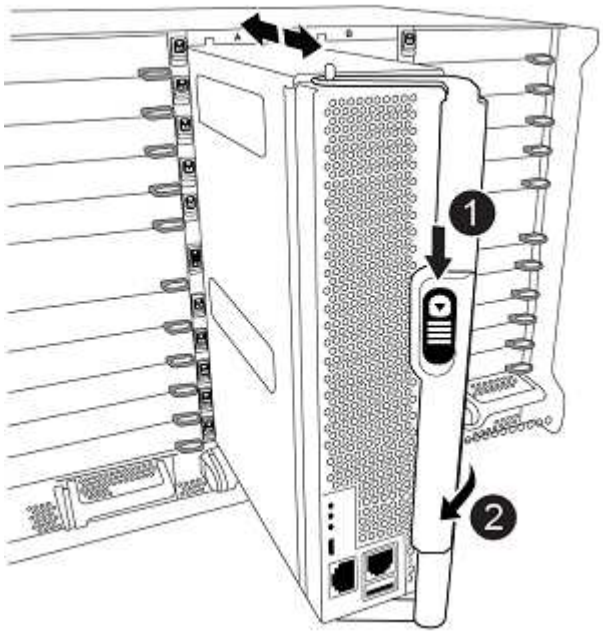
Retirez le module de contrôleur AFF A700 ou FAS9000

Suivre la procédure suivante pour retirer le module de contrôleur AFF A700 ou FAS9000.

Étapes

1. Détachez le câble de la console, le cas échéant, et le câble de gestion du module de contrôleur avant de retirer le module de contrôleur.
2. Déverrouiller et retirer le module de contrôleur du châssis.

   a. Faites glisser le bouton orange sur la poignée de came vers le bas jusqu'à ce qu'il se déverrouille.



	Bouton de déverrouillage de la poignée de came
	Poignée de came

   a. Faites pivoter la poignée de came de façon à ce qu'elle désengage complètement le module de contrôleur du châssis, puis faites glisser le module de contrôleur hors du châssis. Assurez-vous de prendre en charge la partie inférieure du module de contrôleur lorsque vous le faites glisser hors du châssis.

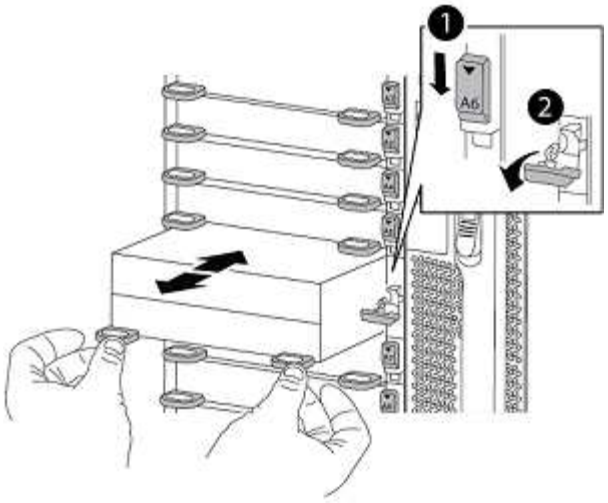
Retirez le module NVS AFF A700 ou FAS9000

Utilisez la procédure suivante pour retirer le module NVS AFF A700 ou FAS9000.

Le module NVS AFF A700 ou FAS9000 est situé dans l'emplacement 6 et double la hauteur par rapport aux autres modules du système.

1. Déverrouillez et retirez le NVS du logement 6.

   a. Appuyer sur le bouton à came numéroté et numéroté. Le bouton de came s'éloigne du châssis.
   b. Faites pivoter le loquet de came vers le bas jusqu'à ce qu'il soit en position horizontale. Le NVS se désengage du châssis et se déplace de quelques pouces.
   c. Retirez le NVS du châssis en tirant sur les languettes de traction situées sur les côtés de la face du module.



	Loquet de came d'E/S numéroté et numéroté
	Loquet d'E/S complètement déverrouillé

- Ne transférez pas les modules d'extension utilisés comme périphériques de vidage de mémoire sur le module de stockage non volatile AFF A700 dans le logement 6 vers le module NVS AFF A900. Ne transférez aucune pièce du contrôleur AFF A700 et des modules NVS vers le module de contrôleur AFF A900.
- Pour les mises à niveau du FAS9000 vers le système FAS9500, vous devez uniquement transférer les modules Flash cache sur le module NVS FAS9000 vers le module NVS FAS9500. Ne transférez aucune autre pièce du contrôleur FAS9000 et des modules NVS vers le module de contrôleur FAS9500.

Installez le AFF A900 ou FAS9500 NVS et le module de contrôleur

Vous devez installer les NVS et le module de contrôleur AFF A900 ou FAS9500 à partir du kit de mise à niveau sur les deux nœuds du site_B. Ne déplacez pas le dispositif de coredump du module NVS AFF A700 ou FAS9000 vers le module NVS AFF A900 ou FAS9500.

Avant de commencer

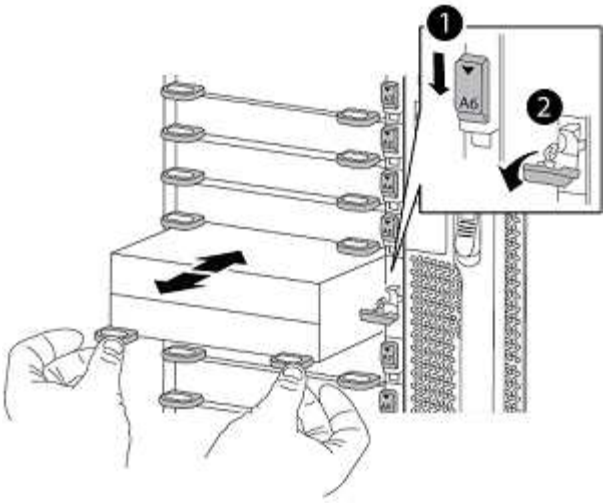
Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.

Installez les NVS AFF A900 ou FAS9500

Utilisez la procédure suivante pour installer les NVS AFF A900 ou FAS9500 dans le logement 6 des deux nœuds du site_B.

Étapes

1. Alignez le système NVS sur les bords de l'ouverture du châssis dans le logement 6.
2. Faites glisser doucement le système NVS dans le logement jusqu'à ce que le loquet de came d'E/S numéroté et numéroté commence à s'engager avec la goupille de came d'E/S, puis poussez le loquet de came d'E/S jusqu'à ce qu'il s'enclenche pour verrouiller le système NVS en place.



	Loquet de came d'E/S numéroté et numéroté
	Loquet d'E/S complètement déverrouillé

Installez le module de contrôleur AFF A900 ou FAS9500

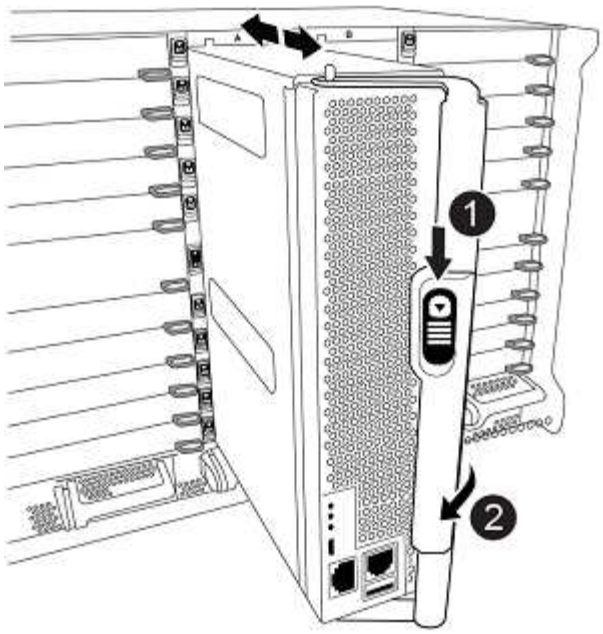
Utilisez la procédure suivante pour installer le module de contrôleur AFF A900 ou FAS9500.

Étapes

1. Alignez l'extrémité du module de contrôleur avec l'ouverture du châssis, puis poussez doucement le module de contrôleur à mi-course dans le système.
2. Poussez fermement le module de contrôleur dans le châssis jusqu'à ce qu'il rencontre le fond de panier central et qu'il soit bien en place. Le loquet de verrouillage s'élève lorsque le module de contrôleur est bien en place.

   Ne forcez pas trop lorsque vous faites glisser le module de contrôleur dans le châssis pour éviter d'endommager les connecteurs.

3. Reliez les ports de gestion et de console au module de contrôleur.



	Bouton de déverrouillage de la poignée de came
	Poignée de came

4. Installez la seconde carte X91129A dans le logement 7 de chaque nœud.
   a. Connectez les ports FC-VI du connecteur 7 aux commutateurs. Reportez-vous à la "Installation et configuration en attachement au fabric" Documentation et accédez à la configuration requise pour la connexion MetroCluster de la structure AFF A900 ou FAS9500 pour le type de commutateur de votre environnement.
5. Mettez le châssis SOUS tension et connectez-vous à la console série.
6. Après l'initialisation du BIOS, si le nœud commence à AUTOBOOT, interrompez l'AUTOBOOT en appuyant sur Control-C.
7. Après avoir interrompu l'AUTOBOOT, les nœuds s'arrêtent à l'invite DU CHARGEUR. Si vous n'interrompez pas AUTOBOOT à temps et que le nœud 1 commence le démarrage, attendez que l'invite appuyez sur Control-C pour accéder au menu de démarrage. Une fois le nœud arrêté au menu de démarrage, utilisez l'option 8 pour redémarrer le nœud et interrompre l'AUTOBOOT pendant le redémarrage.
8. Au `LOADER` à l'invite, définissez les variables d'environnement par défaut : `set-defaults`
9. Enregistrez les paramètres des variables d'environnement par défaut : `saveenv`

NetBoot les nœuds sur site_B

Après avoir remplacé le module de contrôleur AFF A900 ou FAS9500 par un système NVS, vous devez netboot les nœuds AFF A900 ou FAS9500 et installer la même version et le même niveau de patch de ONTAP qui s'exécute sur le cluster. Terme utilisé `netboot` Signifie que vous démarrez à partir d'une image ONTAP stockée sur un serveur distant. Lors de la préparation `netboot`, Vous devez ajouter une copie de l'image de démarrage ONTAP 9 sur un serveur Web auquel le système peut accéder.

Il n'est pas possible de vérifier la version de ONTAP installée sur le support de démarrage d'un module de

contrôleur AFF A900 ou FAS9500, sauf s'il est installé dans un châssis et sous tension. La version ONTAP du support de démarrage AFF A900 ou FAS9500 doit être identique à la version de ONTAP exécutée sur un système AFF A700 ou FAS9000 à mettre à niveau. Les images de démarrage primaire et de sauvegarde doivent correspondre. Vous pouvez configurer les images en exécutant un `netboot` suivi de `wipeconfig` commande dans le menu de démarrage. Si le module de contrôleur était auparavant utilisé dans un autre cluster, le `wipeconfig` commande efface toute configuration résiduelle sur le support d'amorçage.

Avant de commencer

- Vérifiez que vous pouvez accéder à un serveur HTTP avec le système.
- Vous devez télécharger les fichiers système nécessaires pour votre système et la version correcte de ONTAP à partir du "Support NetApp" le site. A propos de cette tâche vous devez `netboot` Les nouveaux contrôleurs si la version de ONTAP installée n'est pas identique à celle installée sur les contrôleurs d'origine. Après avoir installé chaque nouveau contrôleur, vous démarrez le système 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.

Étapes

1. L'accès "Support NetApp" pour télécharger les fichiers requis pour effectuer un démarrage sur le réseau système utilisé pour effectuer le démarrage sur le réseau du système.
2. Télécharger le logiciel ONTAP approprié depuis la section de téléchargement de logiciels du site de support NetApp et stocker le `<ontap_version>_image.tgz` fichier dans un répertoire accessible sur le web.
3. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles. Votre liste de répertoires devrait contenir `<ontap_version>_image.tgz`.
4. Configurer le `netboot` connexion en choisissant l'une des actions suivantes. Remarque : vous devez utiliser le port de gestion et l'adresse IP comme `netboot` connexion. 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. `<netmask>` est le masque de réseau du système de stockage. `<gateway>` est la passerelle du système de stockage. `<dns_addr>` Est l'adresse IP d'un serveur de noms sur votre réseau. Ce paramètre est facultatif. `<dns_domain>` Est le nom de domaine DNS (Domain Name Service). Ce paramètre est facultatif. REMARQUE : d'autres paramètres peuvent être nécessaires pour votre interface. Entrez help ifconfig à l'invite du micrologiciel pour plus de détails.

5. Optimisation `netboot` sur le nœud 1 : `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`Le `<path_to_the_web-accessible_directory>` vous devez indiquer où vous avez téléchargé le `<ontap_version>_image.tgz` dans Étape 2.

   N'interrompez pas l'amorçage.

6. Attendez que le nœud 1 s'exécute sur le module de contrôleur AFF A900 ou FAS9500 pour démarrer et afficher les options du menu de démarrage comme illustré ci-dessous :

```
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)?
```

7. 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 logicielles ONTAP sans interruption et non aux mises à niveau du contrôleur. 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 la mauvaise image soit installée. Ce problème s'applique à toutes les versions de ONTAP.

8. 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[]
9. 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. 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.
10. À l'invite, exécutez le `wipeconfig` pour effacer toute configuration précédente sur le support de démarrage :
    a. Lorsque vous voyez le message ci-dessous, répondez `yes`: `This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:`
    b. Le nœud redémarre pour terminer le `wipeconfig` puis s'arrête au menu de démarrage.
11. Sélectionnez option `5` pour passer en mode maintenance à partir du menu de démarrage. Réponse `yes` sur les invites jusqu'à ce que le nœud s'arrête en mode maintenance et à l'invite de commande `*>`.

Restaurez la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :
   a. Vérifiez les paramètres actuels des ports : `ucadmin show`
   b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*

Cible FC	`fcadmin config -t target adapter-name`
Initiateur FC	`fcadmin config -t initiator adapter-name`

Définissez l'état de haute disponibilité sur les nouveaux contrôleurs et châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état HA pour tous les composants doit être mcc.

2. Si l'état système affiché du contrôleur ou du châssis n'est pas correct, définissez l'état HA :

   `ha-config modify controller mcc`

   `ha-config modify chassis mcc`

3. Arrêter le nœud : `halt`Le nœud doit s'arrêter au niveau du `LOADER>` à l'invite.
4. Sur chaque nœud, vérifiez la date, l'heure et le fuseau horaire du système : `Show date`
5. Si nécessaire, définissez la date en heure UTC ou GMT (GMT) : `set date <mm/dd/yyyy>`
6. Vérifiez l'heure à l'aide de la commande suivante à l'invite de l'environnement d'amorçage : `show time`
7. Si nécessaire, définissez l'heure en UTC ou GMT : `set time <hh:mm:ss>`
8. Enregistrer les paramètres : `saveenv`
9. Collecter les variables d'environnement : `printenv`
10. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet : `boot_ontap maint`
11. Vérifiez que les modifications que vous avez effectuées sont efficaces et ucadmin affiche les ports d'initiateur FC en ligne.

Si vous avez ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`
FC	`fcadmin show`

12. Vérifiez le mode ha-config : `ha-config show`
    a. Vérifiez que vous disposez du résultat suivant :

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Définissez l'état de haute disponibilité sur les nouveaux contrôleurs et châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état HA pour tous les composants doit être mcc.

Si la configuration MetroCluster a…	L'état de la HA doit être…
Deux nœuds	mcc-2n
Quatre ou huit nœuds	mcc

2. Si l'état du système affiché du contrôleur n'est pas correct, définissez l'état HA pour le module de contrôleur et le châssis :

Si la configuration MetroCluster a…	Lancer ces commandes…

Deux nœuds	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Quatre ou huit noeuds	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Réallouer les disques racine de l'agrégat

Réaffectez les disques de l'agrégat racine au nouveau module de contrôleur, en utilisant les sysids réunis précédemment

Description de la tâche

Cette tâche est effectuée en mode Maintenance.

Les anciens ID système ont été identifiés dans "Collecte des informations avant la mise à niveau".

Les exemples de cette procédure utilisent des contrôleurs avec les ID système suivants :

Nœud	Ancien ID système	Nouvel ID système
Nœud_B_1	4068741254	1574774970

Étapes

1. Reliez toutes les autres connexions aux nouveaux modules de contrôleur (FC-VI, stockage, interconnexion de cluster, etc.).
2. Arrêtez le système et démarrez en mode maintenance à partir du `LOADER` invite :

   ```
   boot_ontap maint
   ```

3. Afficher les disques détenus par le nœud_B_1-A700 :

   ```
   disk show -a
   ```

   L'exemple de sortie montre l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (4068741254). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   ...
   ```

4. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers le nouveau contrôleur :

   ```
   disk reassign -s old-sysid -d new-sysid
   ```

   L'exemple suivant montre la réaffectation de disques :

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Vérifier que tous les disques sont réaffectés comme prévu : `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. Afficher le statut de l'agrégat : `aggr status`

```
*> aggr status
           Aggr             State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Répétez les étapes ci-dessus sur le nœud partenaire (node_B_2-A900).

Démarrer les nouveaux contrôleurs

Vous devez redémarrer les contrôleurs à partir du menu de démarrage pour mettre à jour l'image flash du contrôleur. Des étapes supplémentaires sont nécessaires si le chiffrement est configuré.

Description de la tâche

Cette tâche doit être effectuée sur tous les nouveaux contrôleurs.

Étapes

1. Arrêter le nœud : `halt`
2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Afficher le menu de démarrage : `boot_ontap menu`
4. Si le cryptage racine est utilisé, lancez la commande boot menu pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option 10 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés
Gestion externe des clés	Option 11 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés

5. Si AUTOBOOT est activé, interrompez l'AUTOBOOT en appuyant sur Control-C.
6. Dans le menu de démarrage, exécutez l'option (6).

Avec l'option 6, le nœud redémarre deux fois avant de terminer.

Répondez `y` aux invites de changement d'id système. Attendez les deuxième messages de redémarrage :

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Vérifiez que le partenaire-sysid est correct : `printenv partner-sysid`

   Si le partenaire-sysid n'est pas correct, définissez-le : `setenv partner-sysid` *`partner-sysID`*

8. Si le cryptage racine est utilisé, relancez la commande de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option 10 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés
Gestion externe des clés	Option 11 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés

   Vous devrez peut-être émettre le `recover_xxxxxxxx_keymanager` commande à l'invite du menu de démarrage plusieurs fois jusqu'à ce que les nœuds démarrent entièrement.

9. Démarrez les nœuds : `boot_ontap`
10. Attendez que les nœuds remplacés démarrent.

    Si l'un des nœuds est en mode basculement, exécutez un retour à l'aide du `storage failover giveback` commande.

11. Vérifier que tous les ports se trouvent dans un broadcast domain :

    a. Afficher les domaines de diffusion :

       `network port broadcast-domain show`

    b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

       "Ajouter ou supprimer des ports d'un broadcast domain"

    c. Ajoutez le port physique qui hébergera les LIFs intercluster sur le Broadcast domain correspondant.

    d. Modifier les LIFs intercluster de façon à utiliser le nouveau port physique en tant que port de départ.

    e. Une fois les LIFs intercluster configurées, vérifiez le statut des clusters et redéfinissez le peering de cluster si nécessaire.

Vous devrez peut-être reconfigurer le peering de cluster.

"Création d'une relation entre clusters"

f. Recréez les VLAN et les groupes d'interfaces selon les besoins.

L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

"Création d'un VLAN"

"Combinaison de ports physiques pour créer des groupes d'interfaces"

12. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…
Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Vérifier la configuration de LIF

Vérifiez que les LIF sont hébergées sur le nœud/port approprié avant le rétablissement. Les étapes suivantes doivent être effectuées

Description de la tâche

Cette tâche s'effectue sur site_B, où les nœuds ont été démarrés avec des agrégats racine.

Étapes

1. Vérifiez que les LIF sont hébergées sur le nœud et les ports appropriés avant le rétablissement.

   a. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

   b. Remplacez la configuration des ports pour assurer un placement LIF approprié :

   ```
   vserver config override -command "network interface modify" -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node new_node_name"
   ```

   Lors de la saisie du `network interface modify` dans la commande `vserver config override` vous ne pouvez pas utiliser la fonction de saisie semi-automatique de l'onglet. Vous pouvez créer le `network interface modify` à l'aide de la commande auto complete, puis placez-la dans le `vserver config override` commande.

   a. Revenir au niveau de privilège admin :

```
set -privilege admin
```

2. Revert les interfaces sur leur home node :

```
network interface revert * -vserver vserver-name
```

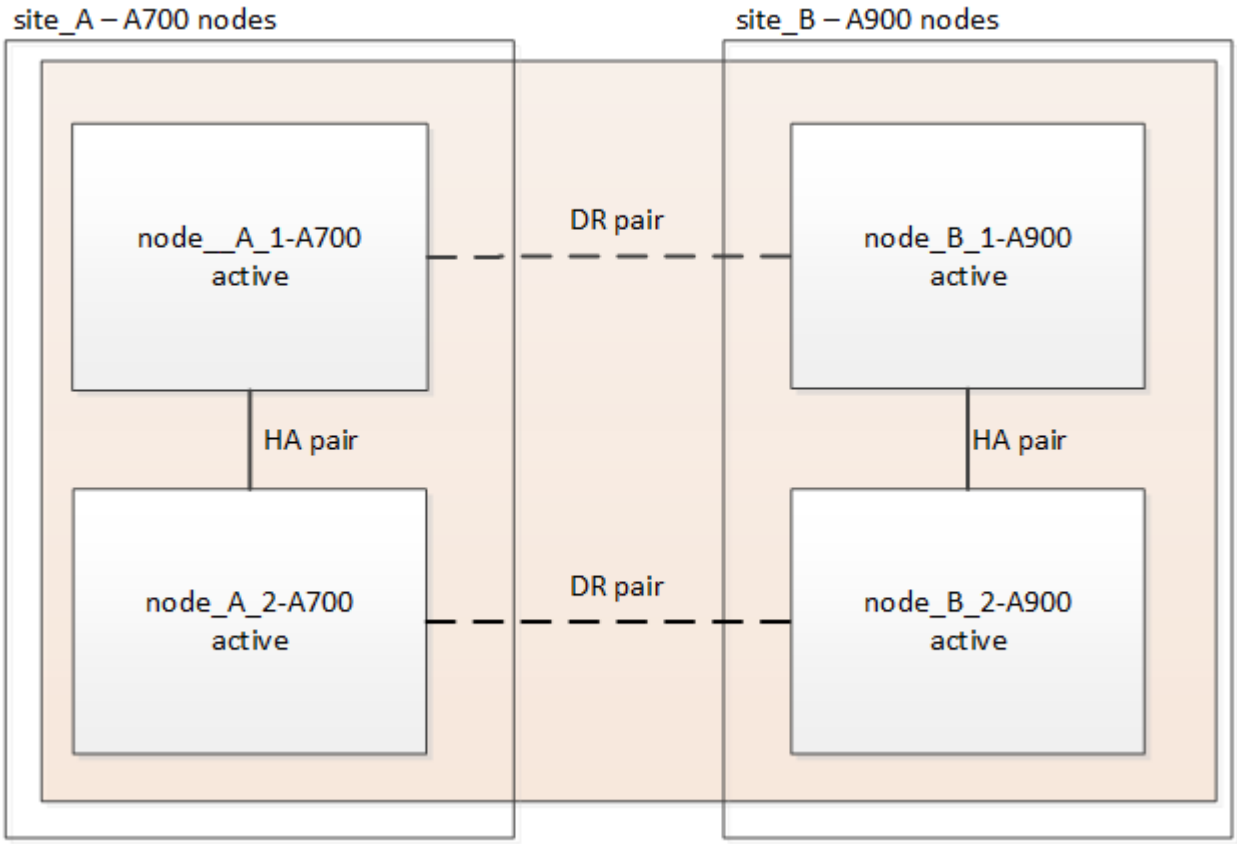
Suivez cette étape sur tous les SVM, si nécessaire.

Retournez la configuration MetroCluster

Une fois les nouveaux contrôleurs configurés, il suffit de revenir à la configuration MetroCluster pour rétablir le fonctionnement normal.

Description de la tâche

Cette tâche vous permet d'effectuer le rétablissement et de rétablir le fonctionnement normal de la configuration MetroCluster. Les nœuds du site_A sont toujours en attente de mise à niveau, comme illustré ci-dessous. (Cette illustration s'applique également à la mise à niveau d'un système FAS9000 vers un contrôleur FAS9500).



Étapes

1. Émettez le `metrocluster node show` Commande on site_B et vérifiez la sortie.
   a. Vérifiez que les nouveaux nœuds sont correctement représentés.
   b. Vérifiez que les nouveaux nœuds sont en attente de rétablissement.
2. Rétablissement du cluster :

```
metrocluster switchback
```

3. Vérifier la progression de l'opération de rétablissement :

   `metrocluster show`

   L'opération de rétablissement est toujours en cours lorsque la sortie s'affiche `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   L'opération de rétablissement est terminée lorsque la sortie s'affiche `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

   Si un rétablissement prend beaucoup de temps, vous pouvez vérifier l'état des lignes de base en cours en utilisant le `metrocluster config-replication resync-status show` commande. Cette commande est au niveau de privilège avancé.

Vérifier l'état de santé de la configuration MetroCluster

Après la mise à niveau des modules de contrôleur, vous devez vérifier l'état de santé de la configuration MetroCluster.

Description de la tâche

Cette tâche peut être effectuée sur n'importe quel nœud de la configuration MetroCluster.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster :

   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

      `metrocluster show`

b. Effectuer une vérification MetroCluster :

```
metrocluster check run
```

c. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

Après avoir exécuté le `metrocluster check run` et `metrocluster check show` commandes, une erreur similaire à l'exemple suivant peut s'afficher :

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+ Cette erreur se produit en raison d'une incompatibilité de contrôleur pendant le processus de mise à niveau. Vous pouvez ignorer l'erreur en toute sécurité et procéder à la mise à niveau des nœuds sur site_A.

Mettre à niveau les nœuds du site_A

Vous devez répéter les tâches de mise à niveau sur site_A.

Étape

1. Répétez les étapes pour mettre à niveau les nœuds du site_A, en commençant par "Préparation à la mise à niveau".

   Lorsque vous effectuez les tâches, toutes les références aux sites et aux nœuds sont inversées. Par exemple, lorsque l'exemple est donné pour basculer du site_A, vous effectuez le basculement du site_B.

Envoyez un message AutoSupport personnalisé après la maintenance

Une fois la mise à niveau terminée, envoyer un message AutoSupport indiquant la fin de la maintenance. La création automatique de dossier peut reprendre.

Étape

1. Pour reprendre la génération automatique de dossier de support, envoyez un message AutoSupport pour indiquer que la maintenance est terminée.

   a. Exécutez la commande suivante :

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   b. Répétez la commande sur le cluster partenaire.

Restaurez la surveillance du logiciel disjoncteur d'attache

Si le logiciel disjoncteur d'attache a déjà été configuré pour la surveillance de la configuration MetroCluster, vous pouvez restaurer la connexion ce dernier.

1. Suivez les étapes de la section : "Ajout des configurations MetroCluster" Dans la section *MetroCluster*

Tiebreaker installation and Configuration.

Mise à niveau des contrôleurs en une configuration FC MetroCluster à quatre nœuds via le basculement et le rétablissement avec des commandes « system contrôleur replace » (ONTAP 9.10.1 et versions ultérieures)

Vous pouvez utiliser ce basculement automatisé MetroCluster dans nos guides pour effectuer une mise à niveau du contrôleur sans interruption sur une configuration MetroCluster FC à quatre nœuds. Dans le cadre de cette procédure, d'autres composants (tels que des tiroirs de stockage ou des commutateurs) ne peuvent pas être mis à niveau.

Combinaisons de plateformes prises en charge

- Pour en savoir plus sur les combinaisons de mise à niveau de plateforme prises en charge, consultez le tableau des mises à niveau FC MetroCluster dans "Choisir la procédure de mise à niveau du contrôleur".

Reportez-vous à la section "Choisissez une méthode de mise à niveau ou de rafraîchissement" pour les procédures supplémentaires.

Description de la tâche

- Cette procédure ne peut être utilisée que pour la mise à niveau du contrôleur.

  Les autres composants de la configuration, tels que les tiroirs de stockage ou les commutateurs, ne peuvent pas être mis à niveau simultanément.

- Cette procédure s'applique aux modules de contrôleur dans une configuration FC MetroCluster à quatre nœuds.
- Ces plateformes doivent exécuter ONTAP 9.10.1 ou une version ultérieure.

  "NetApp Hardware Universe"

- Cette procédure vous permet de mettre à niveau les contrôleurs d'une configuration FC MetroCluster à quatre nœuds à l'aide du basculement et du rétablissement automatisés basé sur NSO. Pour effectuer une mise à niveau du contrôleur à l'aide du transfert d'agrégats (ARL), reportez-vous à "Utilisez les commandes « system contrôleur replace » pour mettre à niveau le matériel du contrôleur exécutant ONTAP 9.8 ou une version ultérieure". Il est recommandé d'utiliser la procédure automatisée basée sur le système NSO.
- Si vos sites MetroCluster sont physiquement situés sur deux sites différents, vous devez suivre la procédure de mise à niveau automatisée du contrôleur NSO pour mettre à niveau les contrôleurs de chaque site de manière consécutive.
- Cette procédure de mise à niveau automatisée du contrôleur NSO-5 vous permet de lancer le remplacement du contrôleur sur un site de reprise après incident MetroCluster. Vous pouvez effectuer le remplacement d'un contrôleur uniquement sur un site à la fois.
- Pour lancer un remplacement du contrôleur sur le site A, vous devez exécuter la commande de démarrage du remplacement du contrôleur depuis le site B. L'opération vous guide à remplacer les contrôleurs des deux nœuds sur le site A uniquement. Pour remplacer les contrôleurs sur le site B, vous devez exécuter la

commande de démarrage de remplacement du contrôleur depuis le site A. Un message indique le site sur lequel les contrôleurs sont remplacés.

Les exemples de noms suivants sont utilisés dans cette procédure :

- Site_A
  - Avant la mise à niveau :
    - Node_A_1-Old
    - Node_A_2-Old
  - Après la mise à niveau :
    - Node_A_1-New
    - Node_A_2-New
- Site_B
  - Avant la mise à niveau :
    - Node_B_1-Old
    - Node_B_2-Old
  - Après la mise à niveau :
    - Node_B_1-New
    - Node_B_2-New

Préparation de la mise à niveau

Pour préparer la mise à niveau du contrôleur, vous devez effectuer des contrôles préalables du système et collecter les informations de configuration.

À n'importe quel stade de la mise à niveau, vous pouvez exécuter le `system controller replace show` ou `system controller replace show-details` Commande du site A pour vérifier le statut. Si les commandes renvoient une sortie vide, attendez quelques minutes et exécutez à nouveau la commande.

Étapes

1. Lancer la procédure de remplacement automatisé du contrôleur depuis le site A pour remplacer les contrôleurs du site B :

   `system controller replace start`

   L'opération automatisée exécute les contrôles préalables. Si aucun problème n'est trouvé, l'opération s'interrompt pour que vous puissiez collecter manuellement les informations relatives à la configuration.

   > Le système source actuel et tous les systèmes cible compatibles sont affichés. Si vous avez remplacé le contrôleur source par un contrôleur possédant une version ONTAP différente ou une plateforme non compatible, l'opération d'automatisation s'arrête et signale une erreur après le démarrage des nouveaux nœuds. Pour rétablir l'état sain du cluster, il est nécessaire de suivre la procédure de restauration manuelle.

   Le `system controller replace start` la commande peut signaler l'erreur de vérification préalable suivante :

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- -------------- ------------------------------------
Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

Vérifiez si cette erreur s'est produite parce que vous avez des agrégats non mis en miroir ou en raison d'un autre problème d'agrégat. Vérifiez que tous les agrégats en miroir sont sains et ne sont pas dégradés ou ne sont pas dégradés. Si cette erreur est due uniquement aux agrégats non mis en miroir, vous pouvez annuler cette erreur en sélectionnant le `-skip-metrocluster-check true` sur le `system controller replace start` commande. Si le stockage distant est accessible, les agrégats sans miroir sont connectés après le basculement. En cas de défaillance de la liaison de stockage distante, les agrégats non mis en miroir ne parviennent pas à se mettre en ligne.

2. Collectez manuellement les informations de configuration en se connectant sur le site B et en suivant les commandes répertoriées dans le message de la console sous le `system controller replace show` ou `system controller replace show-details` commande.

Collecte des informations avant la mise à niveau

Avant de procéder à la mise à niveau, si le volume racine est chiffré, vous devez vous fournir la clé de sauvegarde ainsi que d'autres informations permettant de démarrer les nouveaux contrôleurs avec les anciens volumes root chiffrés.

Description de la tâche

Cette tâche s'effectue sur la configuration FC MetroCluster existante.

Étapes

1. Etiqueter les câbles pour les contrôleurs existants afin de faciliter l'identification des câbles lors de la configuration des nouveaux contrôleurs.
2. Afficher les commandes pour capturer la clé de sauvegarde et d'autres informations :

   `system controller replace show`

   Exécutez les commandes répertoriées sous le `show` commande provenant du cluster partenaire.

3. Collectez les ID système des nœuds de la configuration MetroCluster :

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Au cours de la procédure de mise à niveau, vous remplacerez ces anciens ID système par les ID système des nouveaux modules de contrôleur.

   Dans cet exemple de configuration FC MetroCluster à quatre nœuds, les anciens ID système suivants sont récupérés :

   - Node_A_1-Old : 4068741258
   - Node_A_2-Old : 4068741260
   - Node_B_1-Old : 4068741254

◦ Node_B_2-Old : 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256            4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254            4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258            4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260            4068741258
4 entries were displayed.
```

Dans cet exemple de configuration FC MetroCluster à deux nœuds, les anciens ID système suivants sont récupérés :

◦ Node_A_1 : 4068741258

◦ Node_B_1 : 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Collecte des informations relatives aux ports et aux LIF pour chaque ancien nœud.

   Vous devez collecter les valeurs de sortie des commandes suivantes pour chaque nœud :

   ◦ `network interface show -role cluster,node-mgmt`

   ◦ `network port show -node node-name -type physical`

   ◦ `network port vlan show -node node-name`

   ◦ `network port ifgrp show -node node_name -instance`

   ◦ `network port broadcast-domain show`

   ◦ `network port reachability show -detail`

   ◦ `network ipspace show`

- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

5. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés :

   `security key-manager backup show`

7. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les informations concernant les clés et les clés de phrase secrète.

   Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

   a. Si le gestionnaire de clés intégré est configuré :

      `security key-manager onboard show-backup`

      Vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

   b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

      `security key-manager external show -instance`

   `security key-manager key query`

8. Une fois que vous avez terminé de collecter les informations de configuration, reprenez l'opération :

   `system controller replace resume`

Suppression de la configuration existante du logiciel disjoncteur d'attache ou autre logiciel de surveillance

Si la configuration existante est contrôlée avec la configuration MetroCluster Tiebreaker ou d'autres applications tierces (telles que ClusterLion) capables d'effectuer un basculement, vous devez supprimer la configuration MetroCluster du logiciel disjoncteur d'attache ou autre logiciel avant de remplacer l'ancien contrôleur.

Étapes

1. "Supprimez la configuration MetroCluster existante" À partir du logiciel disjoncteur d'attache.
2. Supprimez la configuration MetroCluster existante de toute application tierce pouvant effectuer le

basculement.

Reportez-vous à la documentation de l'application.

Remplacement des anciens contrôleurs et démarrage des nouveaux contrôleurs

Une fois que vous avez recueilli des informations et que vous reprenez l'opération, l'automatisation procède à l'opération de basculement.

Description de la tâche

L'opération d'automatisation entraîne le basculement, `heal-aggregates`, et `heal root-aggregates` exploitation. Une fois ces opérations terminées, l'opération s'interrompt à **interrompu pour l'intervention de l'utilisateur**. Vous pouvez ainsi installer les contrôleurs, démarrer les contrôleurs partenaires et réaffecter les disques d'agrégat racine au nouveau module de contrôleur à partir de la sauvegarde flash à l'aide de `sysids` rassemblés plus tôt.

Avant de commencer

Avant de lancer le basculement, l'automatisation s'interrompt pour que vous puissiez vérifier manuellement que toutes les LIF sont « en service » sur le site B. Si nécessaire, apportez toutes les LIF « propres » à « UP » et reprenez l'opération d'automatisation à l'aide du `system controller replace resume` commande.

Préparation de la configuration réseau des anciens contrôleurs

Pour assurer la reprise du réseau correctement sur les nouveaux contrôleurs, vous devez déplacer les LIF vers un port commun, puis supprimer la configuration réseau des anciens contrôleurs.

Description de la tâche

- Cette tâche doit être effectuée sur chacun des anciens nœuds.
- Vous utiliserez les informations recueillies dans Préparation de la mise à niveau.

Étapes

1. Démarrez les anciens nœuds, puis connectez-vous aux nœuds :

   ```
   boot_ontap
   ```

2. Assignez le port de base de toutes les LIFs de données de l'ancien contrôleur à un port commun identique sur les anciens et les nouveaux modules de contrôleur.

   a. Afficher les LIFs :

      ```
      network interface show
      ```

      Toutes LES LIF de données, y compris SAN et NAS, seront admin « up » et « possède » des opérations, car celles-ci se trouvent sur le site de basculement (cluster_A).

   b. Vérifiez le résultat de cette commande pour trouver un port réseau physique commun identique sur l'ancien et le nouveau contrôleur qui n'est pas utilisé comme port du cluster.

      Par exemple, « e0d » est un port physique des anciens contrôleurs et est également présent sur les nouveaux contrôleurs. « e0d » n'est pas utilisé comme port de cluster ou autre sur les nouveaux contrôleurs.

      Pour l'utilisation des ports pour les modèles de plate-forme, reportez-vous à la section "NetApp

Hardware Universe"

c. Modifier toutes LES LIFS de données pour utiliser le port commun comme port de base :

`network interface modify -vserver svm-name -lif data-lif -home-port port-id`

Dans l'exemple suivant, il s'agit de ""e0d"".

Par exemple :

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modifier les domaines de diffusion pour supprimer les VLAN et les ports physiques qui doivent être supprimés :

`broadcast-domain remove-ports -broadcast-domain broadcast-domain-name -ports node-name:port-id`

Répétez cette étape pour tous les réseaux VLAN et les ports physiques.

4. Supprimez tous les ports VLAN utilisant des ports de cluster comme ports membres et groupes d'interfaces utilisant des ports de cluster comme ports membres.

a. Supprimer les ports VLAN :

`network port vlan delete -node node-name -vlan-name portid-vlandid`

Par exemple :

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Supprimez les ports physiques des groupes d'interface :

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Par exemple :

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Supprimer les ports VLAN et group d'interface de broadcast domain :

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modifiez les ports du groupe d'interface pour utiliser d'autres ports physiques comme membre :

`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

5. Arrêter les nœuds :

   `halt -inhibit-takeover true -node node-name`

   Cette étape doit être effectuée sur les deux nœuds.

Configuration des nouveaux contrôleurs

Vous devez installer et câbler les nouveaux contrôleurs.

Étapes

1. Planifiez le positionnement des nouveaux modules de contrôleur et tiroirs de stockage en fonction des besoins.

   L'espace rack dépend du modèle de plateforme des modules de contrôleur, des types de switchs et du nombre de tiroirs de stockage de votre configuration.

2. Mettez-vous à la terre.
3. Installez les modules de contrôleur sur le rack ou l'armoire.

   "Documentation des systèmes matériels ONTAP"

4. Si les nouveaux modules de contrôleur ne sont pas livrés avec eux-mêmes des cartes FC-VI et si les cartes FC-VI des anciens contrôleurs sont compatibles avec les nouveaux contrôleurs, remplacez les cartes FC-VI et installez-les dans les connecteurs appropriés.

   Voir la "NetApp Hardware Universe" Pour les informations sur les slots pour les cartes FC-VI.

5. Reliez les connexions d'alimentation, de console série et de gestion des contrôleurs, comme décrit dans les *MetroCluster - Guides d'installation et de configuration*.

   Ne connectez pas d'autres câbles ayant été débranchés des anciens contrôleurs à l'heure actuelle.

   "Documentation des systèmes matériels ONTAP"

6. Mettez les nouveaux nœuds sous tension et appuyez sur Ctrl-C lorsque vous êtes invité à afficher l'invite DU CHARGEUR.

Démarrage réseau des nouveaux contrôleurs

Une fois les nouveaux nœuds installés, vous devez démarrage sur le réseau pour vous assurer que la version des nouveaux nœuds exécute la même version de ONTAP que les nœuds d'origine. Le terme netboot signifie que vous êtes en cours de démarrage à partir d'une image ONTAP stockée sur un serveur distant. Lorsque vous vous préparez à netboot, vous devez placer une copie de l'image de démarrage ONTAP 9 sur un serveur web auquel le système peut accéder.

Cette tâche est effectuée sur chacun des nouveaux modules de contrôleur.

Étapes

1. Accédez au "Site de support NetApp" pour télécharger les fichiers utilisés pour effectuer le démarrage sur le réseau du système.
2. Téléchargez le logiciel ONTAP approprié depuis la section de téléchargement de logiciels du site du support NetApp et stockez le fichier ontap-version_image.tgz dans un répertoire accessible en ligne.

3. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.

Si le modèle de plateforme est…	Alors…
Systèmes de la gamme FAS/AFF8000	Extrayez le contenu d'ontap-version_image.tgzfile dans le répertoire cible : tar -zxvf ontap-version_image.tgz REMARQUE : si vous extrayez le contenu sous Windows, utilisez 7-Zip ou WinRAR pour extraire l'image netboot. Votre liste de répertoires doit contenir un dossier netboot avec un fichier de noyau:netboot/kernel
Tous les autres systèmes	Votre liste de répertoires doit contenir un dossier netboot avec un fichier du noyau : ontap-version_image.tgz vous n'avez pas besoin d'extraire le fichier ontap-version_image.tgz.

4. À l'invite DU CHARGEUR, configurez la connexion netboot pour les LIF de gestion :
   - Si l'adressage IP est DHCP, configurez la connexion automatique :

     ```
     ifconfig e0M -auto
     ```

   - Si l'adressage IP est statique, configurez la connexion manuelle :

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Effectuer la démarrage sur le réseau.
   - Si la plate-forme est un système de la série 80xx, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Si la plateforme est un autre système, utilisez la commande suivante :

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
     ```

6. Dans le menu de démarrage, sélectionnez l'option **(7) installer le nouveau logiciel en premier** pour télécharger et installer la nouvelle image logicielle sur le périphérique d'amorçage.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Si vous êtes invité à poursuivre la procédure, entrez `y`, Et lorsque
   vous êtes invité à saisir l'URL du fichier image :
   `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Assurez-vous d'entrer `n` pour ignorer la restauration de la sauvegarde lorsque vous voyez une invite similaire à la suivante :

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

8. Redémarrez en entrant `y` lorsque vous voyez une invite similaire à la suivante :

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

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   `halt`

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   `set-defaults`

3. Enregistrez l'environnement :

   `saveenv`

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   `boot_ontap menu`

5. À l'invite du menu de démarrage, effacez la configuration :

   `wipeconfig`

   Répondez `yes` à l'invite de confirmation.

   Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

   Répondez `yes` à l'invite de confirmation.

Restauration de la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :

   a. Vérifiez les paramètres actuels des ports : `ucadmin show`

   b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Cible FC	`fcadmin config -t target` *`adapter-name`*
Initiateur FC	`fcadmin config -t initiator` *`adapter-name`*

2. Quitter le mode Maintenance :

   `halt`

   Une fois que vous avez exécuté la commande, attendez que le nœud s'arrête à l'invite DU CHARGEUR.

3. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet :

   `boot_ontap maint`

4. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`
FC	`fcadmin show`

Réaffectation des disques de l'agrégat racine

Réallouer les disques de l'agrégat racine vers le nouveau module de contrôleur, à l'aide du `sysids` rassemblés plus tôt

Description de la tâche

Cette tâche est effectuée en mode Maintenance.

Les anciens ID système ont été identifiés dans "Collecte des informations avant la mise à niveau".

Les exemples de cette procédure utilisent des contrôleurs avec les ID système suivants :

Nœud	Ancien ID système	Nouvel ID système
Nœud_B_1	4068741254	1574774970

Étapes

1. Reliez toutes les autres connexions aux nouveaux modules de contrôleur (FC-VI, stockage, interconnexion de cluster, etc.).
2. Arrêtez le système et démarrez en mode maintenance à partir de l'invite DU CHARGEUR :

   ```
   boot_ontap maint
   ```

3. Afficher les disques détenus par le nœud_B_1-Old :

   ```
   disk show -a
   ```

   Le résultat de la commande affiche l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (4068741254). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   ...
   ```

4. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers le nouveau contrôleur :

   ```
   disk reassign -s old-sysid -d new-sysid
   ```

   L'exemple suivant montre la réaffectation de disques :

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Vérifier que tous les disques sont réaffectés comme prévu :

   `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                     POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------             -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Afficher le statut de l'agrégat :

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status            Options
   aggr0_node_b_1-root         online      raid_dp, aggr     root, nosnap=on,
                               mirrored
   mirror_resync_priority=high(fixed)
                               fast zeroed
                               64-bit
   ```

7. Répétez les étapes ci-dessus sur le nœud partenaire (node_B_2-New).

Démarrage des nouveaux contrôleurs

Vous devez redémarrer les contrôleurs à partir du menu de démarrage pour mettre à jour l'image flash du contrôleur. Des étapes supplémentaires sont nécessaires si le chiffrement est configuré.

Vous pouvez reconfigurer les VLAN et les groupes d'interface. Si nécessaire, modifier manuellement les ports des LIFs de cluster et des détails de broadcast domain avant de reprendre l'opération en utilisant le `system controller replace resume` commande.

Description de la tâche

Cette tâche doit être effectuée sur tous les nouveaux contrôleurs.

Étapes

1. Arrêter le nœud :

   ```
   halt
   ```

2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Afficher le menu de démarrage :

   ```
   boot_ontap menu
   ```

4. Si le cryptage racine est utilisé, sélectionnez l'option de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…

Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

5. Si AUTOBOOT est activé, interrompez l'AUTOBOOT en appuyant sur Ctrl-C.
6. Dans le menu de démarrage, exécutez l'option « 6 ».

   L'option « 6 » redémarre le nœud deux fois avant de terminer.

   Répondez « y » aux invites de changement d'ID système. Attendez les deuxième messages de redémarrage :

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Vérifiez que le partenaire-sysid est correct :

   ```
   printenv partner-sysid
   ```

   Si le partenaire-sysid n'est pas correct, définissez-le :

   ```
   setenv partner-sysid partner-sysID
   ```

8. Si le cryptage racine est utilisé, sélectionnez à nouveau l'option de menu d'amorçage pour la configuration de votre gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option « 10 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

Selon le paramètre du gestionnaire de clés, effectuez la procédure de récupération en sélectionnant l'option « 10 » ou « 11 », suivie de l'option « 6 » à la première invite du menu d'amorçage. Pour démarrer complètement les nœuds, il est possible que vous deviez répéter la procédure de restauration suite à l'option « 1 » (démarrage normal).

9. Démarrez les nœuds :

   `boot_ontap`

10. Attendez que les nœuds remplacés démarrent.

    Si l'un des nœuds est en mode basculement, exécutez un retour à l'aide du `storage failover giveback` commande.

11. Vérifier que tous les ports se trouvent dans un broadcast domain :

    a. Afficher les domaines de diffusion :

       `network port broadcast-domain show`

    b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

       "Ajout ou suppression de ports d'un broadcast domain"

    c. Ajoutez le port physique qui hébergera les LIFs intercluster sur le broadcast domain correspondant.

    d. Modifier les LIFs intercluster de façon à utiliser le nouveau port physique en tant que port de départ.

    e. Une fois les LIFs intercluster configurées, vérifiez le statut des clusters et redéfinissez le peering de cluster si nécessaire.

       Vous devrez peut-être reconfigurer le peering de cluster.

       "Création d'une relation entre clusters"

    f. Recréez les VLAN et les groupes d'interfaces selon les besoins.

       L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

       "Création d'un VLAN"

    "Combinaison de ports physiques pour créer des groupes d'interfaces"

    a. Vérifier que le cluster partenaire est accessible et que la configuration a été resynchronisée sur le cluster partenaire :

       `metrocluster switchback -simulate true`

12. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…

Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name`

13. Avant de reprendre l'opération, vérifiez que le MetroCluster est configuré correctement. Vérifier l'état du nœud :

    `metrocluster node show`

    Vérifiez que les nouveaux nœuds (site_B) sont dans **en attente de l'état de rétablissement** à partir de site_A.

14. Reprendre l'opération :

    `system controller replace resume`

Fin de la mise à niveau

L'automatisation exécute des vérifications du système, puis s'interrompt pour que vous puissiez vérifier la capacité d'accès au réseau. Une fois la vérification terminée, la phase de récupération des ressources est lancée, et l'opération d'automatisation exécute le rétablissement sur le site A et s'interrompt après les vérifications de mise à niveau. Une fois que vous avez rétabli l'opération d'automatisation, il effectue les vérifications post-mise à niveau et, si aucune erreur n'est détectée, marque la mise à niveau comme terminée.

Étapes

1. Vérifiez l'accessibilité du réseau en suivant le message de la console.
2. Une fois la vérification terminée, reprendre l'opération :

   `system controller replace resume`

3. L'opération d'automatisation effectue le rétablissement sur le site A et les vérifications post-mise à niveau. Lorsque l'opération s'interrompt, vérifier manuellement le statut LIF SAN et vérifier la configuration du réseau en suivant le message de la console.
4. Une fois la vérification terminée, reprendre l'opération :

   `system controller replace resume`

5. Vérifier l'état des vérifications post-mise à niveau :

   `system controller replace show`

   Si les vérifications post-mise à niveau n'ont pas signalé d'erreurs, la mise à niveau est terminée.

6. Une fois la mise à niveau du contrôleur terminée, connectez-vous au site B et vérifiez que les contrôleurs remplacés sont configurés correctement.

Restauration du contrôle disjoncteur d’attache

Si le logiciel disjoncteur d’attache a déjà été configuré pour la surveillance de la configuration MetroCluster, vous pouvez restaurer la connexion ce dernier.

1. Suivez les étapes de la section "Ajout des configurations MetroCluster".

Mise à niveau des contrôleurs dans une configuration MetroCluster IP à l’aide du basculement et du rétablissement (ONTAP 9.8 et versions ultérieures)

Depuis ONTAP 9.8, vous pouvez utiliser le processus de basculement MetroCluster pour fournir aux clients un service sans interruption pendant la mise à niveau des modules de contrôleur sur le cluster partenaire. Dans le cadre de cette procédure, d’autres composants (tels que des tiroirs de stockage ou des commutateurs) ne peuvent pas être mis à niveau.

Plateformes prises en charge par cette procédure

- Ces plateformes doivent exécuter ONTAP 9.8 ou une version ultérieure.
- La plateforme cible (nouvelle) doit être un modèle différent de celui de la plateforme d’origine.
- Les modèles de plateforme avec tiroirs internes ne sont pas pris en charge.
- Vous pouvez uniquement mettre à niveau des modèles de plate-forme spécifiques en suivant cette procédure dans une configuration MetroCluster IP.
  - Pour plus d’informations sur les combinaisons de mise à niveau de plate-forme prises en charge, consultez le tableau de mise à niveau IP MetroCluster dans "Choisir la procédure de mise à niveau du contrôleur".

    Reportez-vous à la section "Choisissez une méthode de mise à niveau ou de rafraîchissement" pour les procédures supplémentaires.

Description de la tâche

- Cette procédure s’applique aux modules de contrôleur dans une configuration MetroCluster IP.
- Tous les contrôleurs de la configuration doivent être mis à niveau pendant la même période de maintenance.

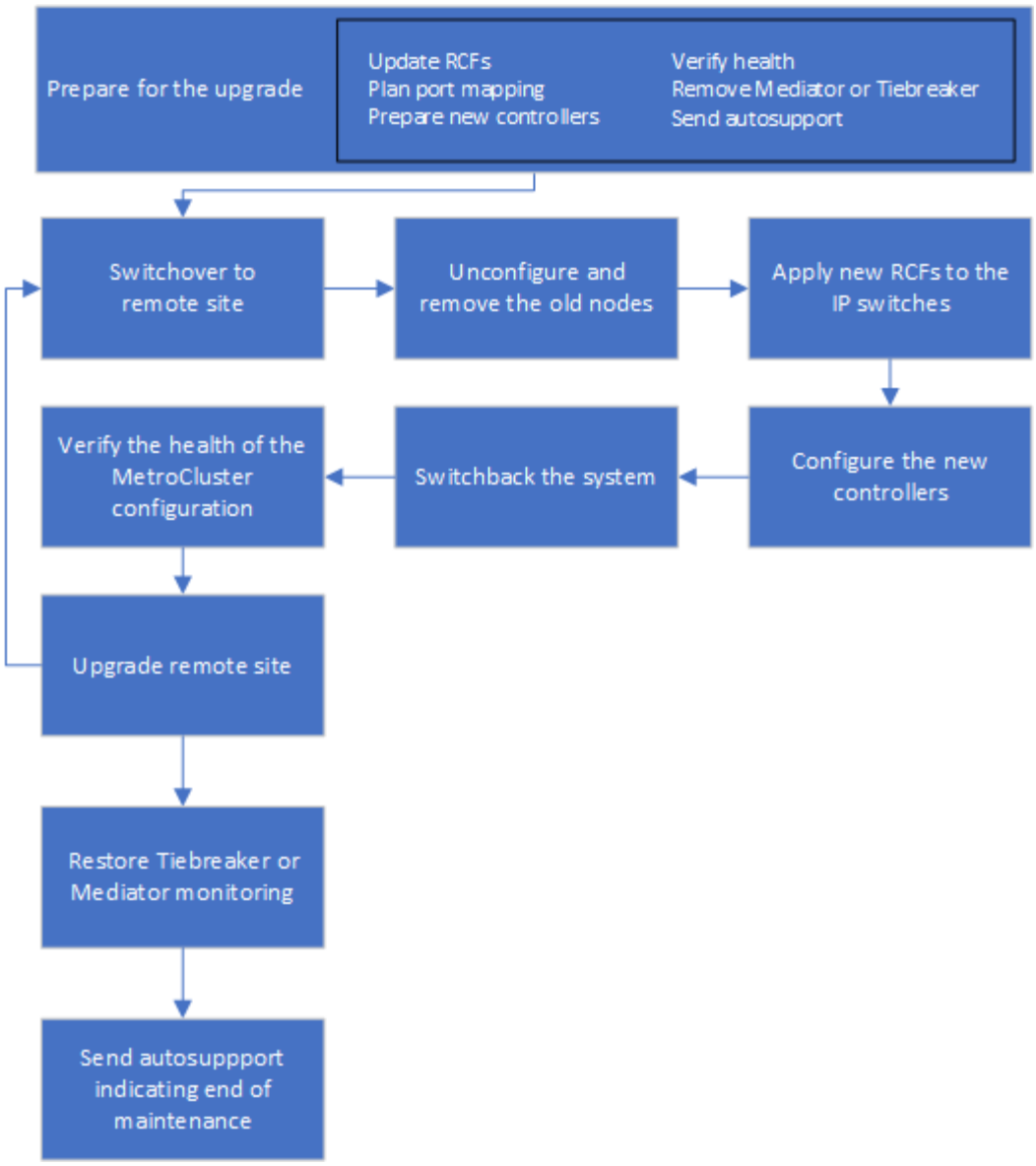
  L’exploitation de la configuration MetroCluster avec différents types de contrôleurs n’est pas prise en charge en dehors de cette activité de maintenance.
- Les commutateurs IP doivent exécuter une version de micrologiciel prise en charge.
- Si la nouvelle plate-forme comporte moins de slots que le système d’origine ou si elle comporte moins ou différents types de ports, vous devrez peut-être ajouter un adaptateur au nouveau système.

  Pour plus d’informations, reportez-vous à la section "NetApp Hardware Universe".
- Vous allez réutiliser les adresses IP, les masques réseau et les passerelles des plates-formes d’origine sur les nouvelles plates-formes.

- Les exemples de noms suivants sont utilisés dans cette procédure :
  - Site_A
    - Avant la mise à niveau :
      - Node_A_1-Old
      - Node_A_2-Old
    - Après la mise à niveau :
      - Node_A_1-New
      - Node_A_2-New
  - Site_B
    - Avant la mise à niveau :
      - Node_B_1-Old
      - Node_B_2-Old
    - Après la mise à niveau :
      - Node_B_1-New
      - Node_B_2-New

Flux de production de mise à niveau des contrôleurs dans une configuration MetroCluster IP

Vous pouvez utiliser le diagramme de workflow pour planifier les tâches de mise à niveau.



Préparation de la mise à niveau

Avant d'apporter des modifications à la configuration MetroCluster existante, vous devez vérifier l'état de santé de la configuration, préparer les nouvelles plateformes et effectuer d'autres tâches diverses.

Mise à jour des fichiers RCF de commutateur MetroCluster avant la mise à niveau des contrôleurs

Selon les anciens modèles de plateforme, ou si la configuration des commutateurs ne repose pas sur la version minimale, ou si vous souhaitez modifier les ID VLAN utilisés par les connexions MetroCluster internes, vous devez mettre à jour les fichiers RCF de commutateur avant de lancer la procédure de mise à niveau de la plateforme.

Description de la tâche

Vous devez mettre à jour le fichier RCF dans les scénarios suivants :

- Pour certains modèles de plate-forme, les commutateurs doivent utiliser un ID VLAN pris en charge pour les connexions IP MetroCluster internes. Si l'ancien ou le nouveau modèle de plate-forme sont dans le tableau suivant, **et non** utilisant un ID VLAN pris en charge, vous devez mettre à jour les fichiers RCF de commutateur.

Les connexions locales du cluster peuvent utiliser n'importe quel VLAN, elles n'ont pas besoin d'être dans la plage indiquée.

Modèle de plateforme (ancien ou nouveau)	ID de VLAN pris en charge
• AFF A400	• 10 • 20 • Toute valeur comprise entre 101 et 4096 inclus.

- La configuration du commutateur n'a pas été configurée avec la version RCF minimale prise en charge :

Changer de modèle	Version du fichier RCF requise
Cisco 3132Q-V	1.7 ou ultérieure
Cisco 3232C	1.7 ou ultérieure
Broadcom BES-53248	1.3 ou ultérieure

- Vous souhaitez modifier la configuration VLAN.

  La plage d'ID de VLAN est comprise entre 101 et 4096 inclus.

Les commutateurs du site_A seront mis à niveau lorsque les contrôleurs du site_A sont mis à niveau.

Étapes

1. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

   Suivez les étapes de la section correspondant au fournisseur de votre commutateur du "Installation et configuration de MetroCluster IP".

   - "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
   - "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

2. Téléchargez et installez les fichiers RCF.

   Suivez les étapes de la section "Installation et configuration de MetroCluster IP".

   - "Téléchargement et installation des fichiers RCF Broadcom"
   - "Téléchargement et installation des fichiers Cisco IP RCF"

Mappage des ports des anciens nœuds sur les nouveaux nœuds

Vous devez vérifier que les ports physiques du node_A_1-Old sont correctement associés aux ports physiques du node_A_1-New, qui permettront à node_A_1-New de communiquer avec d'autres nœuds du cluster et avec le réseau après la mise à niveau.

Description de la tâche

Une fois le nouveau nœud démarré au cours du processus de mise à niveau, la configuration la plus récente de l'ancien nœud qu'il remplace est retraitée. Lorsque vous démarrez node_A_1-New, ONTAP tente

d'héberger les LIFs sur les mêmes ports qui ont été utilisés sur node_A_1-Old. Par conséquent, dans le cadre de la mise à niveau, vous devez ajuster la configuration du port et de la LIF afin qu'elle soit compatible avec celle de l'ancien nœud. Durant la procédure de mise à niveau, vous effectuez les étapes des anciens et nouveaux nœuds afin d'assurer une configuration correcte du cluster, de la gestion et de la LIF de données.

Le tableau suivant présente des exemples de modifications de configuration liées aux exigences de port des nouveaux nœuds.

Ports physiques d'interconnexion de cluster		
Ancien contrôleur	Nouveau contrôleur	Action requise
e0a, e0b	e3a, e3b	Aucun port correspondant. Après la mise à niveau, vous devez recréer les ports du cluster.
e0c, e0d	e0a,e0b,e0c,e0d	e0c et e0d sont des ports correspondants. Vous n'avez pas à modifier la configuration, mais après une mise à niveau, vous pouvez répartir les LIF de cluster entre les ports disponibles.

Étapes

1. Identifiez les ports physiques disponibles sur les nouveaux contrôleurs et les LIFs peuvent être hébergées sur les ports.

   L'utilisation des ports du contrôleur dépend du module de plate-forme et des commutateurs que vous utiliserez dans la configuration IP de MetroCluster. Vous pouvez collecter l'utilisation des ports des nouvelles plates-formes à partir du "NetApp Hardware Universe".

2. Planifiez l'utilisation de vos ports et remplissez les tableaux suivants pour référence pour chacun des nouveaux nœuds.

   Vous vous référez au tableau lors de la procédure de mise à niveau.

	Node_A_1-Old			Node_A_1-New		
LIF	Ports	Les IPspaces	Les domaines de diffusion	Ports	Les IPspaces	Les domaines de diffusion
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestion de nœuds						

Gestion du cluster						
Données 1						
Données 2						
Données 3						
Données 4						
SAN						
Port intercluster						

Démarrage réseau des nouveaux contrôleurs

Une fois les nouveaux nœuds installés, vous devez démarrage sur le réseau pour vous assurer que la version des nouveaux nœuds exécute la même version de ONTAP que les nœuds d'origine. Le terme netboot signifie que vous êtes en cours de démarrage à partir d'une image ONTAP stockée sur un serveur distant. Lorsque vous vous préparez à netboot, vous devez placer une copie de l'image de démarrage ONTAP 9 sur un serveur web auquel le système peut accéder.

Étapes

1. NetBoot les nouveaux contrôleurs :

   a. Accédez au "Site de support NetApp" pour télécharger les fichiers utilisés pour effectuer le démarrage sur le réseau du système.

   b. Téléchargez le logiciel ONTAP approprié depuis la section de téléchargement des logiciels du site de support NetApp et stockez le `ontap-version_image.tgz` fichier dans un répertoire accessible sur le web.

   c. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.

Si le modèle de plateforme est…	Alors…

8000 systèmes	Extraire le contenu du *ontap-version*_image.tgz fichier dans le répertoire cible :
	
	`tar -zxvf ontap-version_image.tgz`
	
	Si vous extrayez le contenu sous Windows, utilisez 7-Zip ou WinRAR pour extraire l'image netboot. Votre liste de répertoires doit contenir un dossier netboot avec un fichier de noyau:netboot/kernel
	
	Votre liste de répertoires doit contenir un dossier netboot avec un fichier du noyau :
	
	`netboot/kernel`

Tous les autres systèmes	Votre liste de répertoires doit contenir un dossier netboot avec un fichier du noyau : `_ontap-version_image.tgz` Il n'est pas nécessaire d'extraire le `_ontap-version_image.tgz` fichier.

d. À l'invite DU CHARGEUR, configurez la connexion netboot pour les LIF de gestion :

Si l'adressage IP est…	Alors…
DHCP	Configurer la connexion automatique : `ifconfig e0M -auto`
Statique	Configurer la connexion manuelle : `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

e. Effectuer la démarrage sur le réseau.

Si le modèle de plateforme est…	Alors…
Systèmes de la gamme FAS/AFF8000	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Tous les autres systèmes	`netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

f. Dans le menu de démarrage, sélectionnez option **(7) installer le nouveau logiciel en premier** pour télécharger et installer la nouvelle image logicielle 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"`. Il s'applique aux mises à niveau logicielles sans interruption et non aux mises à niveau des contrôleurs.

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

   `http://`*`web_server_ip/path_to_web-accessible_directory/ontap-version`*`_image.tgz`

b. Entrez le nom d'utilisateur et le mot de passe, le cas échéant, ou appuyez sur entrée pour continuer.

c. Assurez-vous d'entrer `n` pour ignorer la restauration de la sauvegarde lorsque vous voyez une invite similaire à la suivante :

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

d. Redémarrez en entrant **`y`** lorsque vous voyez une invite similaire à la suivante :

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

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   `halt`

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   `set-defaults`

3. Enregistrez l'environnement :

   `saveenv`

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   `boot_ontap menu`

5. À l'invite du menu de démarrage, effacez la configuration :

`wipeconfig`

Répondez `yes` à l'invite de confirmation.

Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

   Répondez `yes` à l'invite de confirmation.

Vérifier l'état de santé du MetroCluster avant la mise à niveau du site

Vous devez vérifier l'état de santé et la connectivité de la configuration MetroCluster avant d'effectuer la mise à niveau.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :

   a. Vérifiez si les nœuds sont multipathed :
   `node run -node node-name sysconfig -a`

   Vous devez exécuter cette commande pour chaque nœud de la configuration MetroCluster.

   b. Vérifier qu'il n'y a pas de disques défectueux dans la configuration :
   `storage disk show -broken`

   Vous devez exécuter cette commande sur chaque nœud de la configuration MetroCluster.

   c. Vérifiez si des alertes d'intégrité sont émises :

   `system health alert show`

   Vous devez exécuter cette commande sur chaque cluster.

   d. Vérifier les licences sur les clusters :

   `system license show`

   Vous devez exécuter cette commande sur chaque cluster.

   e. Vérifiez les périphériques connectés aux nœuds :

   `network device-discovery show`

   Vous devez exécuter cette commande sur chaque cluster.

   f. Vérifiez que le fuseau horaire et l'heure sont correctement définis sur les deux sites :

   `cluster date show`

   Vous devez exécuter cette commande sur chaque cluster. Vous pouvez utiliser le `cluster date` commandes permettant de configurer le fuseau horaire et le fuseau horaire.

2. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.
   a. Confirmer la configuration MetroCluster et la présence du mode opérationnel `normal`:
      `metrocluster show`
   b. Confirmer que tous les nœuds attendus sont affichés :
      `metrocluster node show`
   c. Exécutez la commande suivante :

      ```
      metrocluster check run
      ```

   d. Afficher les résultats de la vérification MetroCluster :

      ```
      metrocluster check show
      ```

3. Vérifiez le câblage MetroCluster à l'aide de l'outil Config Advisor.
   a. Téléchargez et exécutez Config Advisor.

      "Téléchargement NetApp : Config Advisor"

   b. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.

Collecte des informations avant la mise à niveau

Avant la mise à niveau, vous devez collecter les informations de chacun des nœuds et, si nécessaire, ajuster les domaines de diffusion réseau, supprimer tous les VLAN et groupes d'interfaces et collecter des informations de cryptage.

Étapes

1. Notez le câblage physique de chaque nœud et étiqueteuse les câbles si nécessaire pour permettre un câblage correct des nouveaux nœuds.
2. Collecte des informations d'interconnexion, de port et de LIF pour chaque nœud

   Vous devez collecter les valeurs de sortie des commandes suivantes pour chaque nœud :

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`

- system node run -node *node-name* sysconfig -a
- vserver fcp initiator show
- storage disk show
- metrocluster configuration-settings interface show

3. Rassemblez les UUID du site_B (site dont les plates-formes sont actuellement mises à niveau) :

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

Ces valeurs doivent être configurées avec précision sur les nouveaux modules de contrôleur site_B pour garantir la réussite de la mise à niveau. Copiez les valeurs dans un fichier afin de pouvoir les copier dans les commandes appropriées ultérieurement dans le processus de mise à niveau.

L'exemple suivant montre la sortie de la commande avec les UID :

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

Il est recommandé d'enregistrer les UUID dans un tableau similaire à ce qui suit.

Cluster ou nœud	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Nœud_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Nœud_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
Nœud_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039

Nœud_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés :

   ```
   security key-manager backup show
   ```

6. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les informations concernant les clés et les clés de phrase secrète.

   Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

   a. Si le gestionnaire de clés intégré est configuré :
   `security key-manager onboard show-backup`

      Vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

   b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

      ```
      security key-manager external show -instance security key-manager key query
      ```

7. Collectez les ID système des nœuds existants :

   ```
   metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
   ```

   Le résultat suivant montre les disques réattribués.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Retrait du système de surveillance du médiateur ou du disjoncteur d'attache

Avant de mettre à niveau les plates-formes, vous devez supprimer la surveillance si la configuration MetroCluster est surveillée à l'aide de l'utilitaire Tiebreaker ou Mediator.

Étapes

1. Collectez les valeurs de sortie de la commande suivante :

   ```
   storage iscsi-initiator show
   ```

2. Supprimez la configuration MetroCluster existante du logiciel disjoncteur d'attache, du médiateur ou d'autres logiciels pouvant initier le basculement.

Si vous utilisez…	Utilisez cette procédure…
Disjoncteur d'attache	"Suppression des configurations MetroCluster" Dans le *MetroCluster Tiebreaker - Guide d'installation et de configuration*
Médiateur	Exécutez la commande suivante depuis l'invite ONTAP : `metrocluster configuration-settings mediator remove`
Applications tierces	Reportez-vous à la documentation du produit.

Envoi d'un message AutoSupport personnalisé avant la maintenance

Avant d'effectuer la maintenance, vous devez envoyer un message AutoSupport pour informer le support technique de NetApp que la maintenance est en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Connectez-vous au cluster.
2. Appelez un message AutoSupport indiquant le début de la maintenance :

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Le `maintenance-window-in-hours` le paramètre spécifie la longueur de la fenêtre de maintenance, avec un maximum de 72 heures. Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Répétez cette procédure sur le site du partenaire.

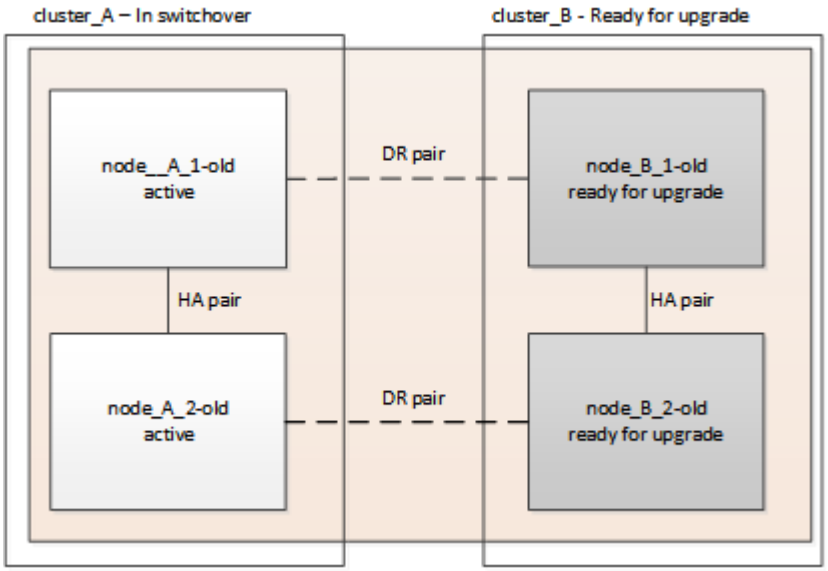
Commutation de la configuration MetroCluster

Vous devez basculer la configuration vers site_A afin de pouvoir mettre à niveau les plateformes du site_B.

Description de la tâche

Cette tâche doit être effectuée sur site_A.

Une fois cette tâche terminée, cluster_A est actif et assure le service des données des deux sites. Cluster_B est inactif et prêt à démarrer le processus de mise à niveau.



Étapes

1. Basculer la configuration MetroCluster sur site_A afin de mettre à niveau les nœuds site_B :

   a. Exécutez la commande suivante sur cluster_A :

      ```
      metrocluster switchover -controller-replacement true
      ```

      L'opération peut prendre plusieurs minutes.

   b. Surveiller le fonctionnement du basculement :

      ```
      metrocluster operation show
      ```

   c. Une fois l'opération terminée, vérifiez que les nœuds sont en état de basculement :

      ```
      metrocluster show
      ```

   d. Vérifier l'état des nœuds MetroCluster :

      ```
      metrocluster node show
      ```

   La fonctionnalité de correction automatique des agrégats après le basculement négocié est désactivée lors de la mise à niveau du contrôleur.

Suppression des configurations d'interface et désinstallation des anciens contrôleurs

Vous devez déplacer les LIF de données vers un port commun, supprimer les VLAN et les groupes d'interfaces des anciens contrôleurs, puis désinstaller physiquement les contrôleurs.

Description de la tâche

- Ces étapes sont réalisées sur les anciens contrôleurs (node_B_1-Old, node_B_2-Old).
- Consultez les informations que vous avez rassemblées dans "Mappage des ports des anciens nœuds sur les nouveaux nœuds".

Étapes

1. Démarrez les anciens nœuds et connectez-vous aux nœuds :

   ```
   boot_ontap
   ```

2. Assignez le port de base de toutes les LIFs de données de l'ancien contrôleur à un port commun identique sur les anciens et les nouveaux modules de contrôleur.

   a. Afficher les LIFs :

      ```
      network interface show
      ```

      Toutes LES LIF de données, y compris SAN et NAS, seront administrative et hors service, car celles-ci fonctionnent sur le site basculement (cluster_A).

   b. Vérifiez le résultat de cette commande pour trouver un port réseau physique commun identique sur l'ancien et le nouveau contrôleur qui n'est pas utilisé comme port du cluster.

      Ainsi, le port e0d est un port physique des anciens contrôleurs et il est également présent sur les

nouveaux contrôleurs. e0d n'est pas utilisé comme port de cluster ou autre sur les nouveaux contrôleurs.

Pour l'utilisation des ports pour les modèles de plate-forme, reportez-vous à la section "NetApp Hardware Universe"

c. Modifier toutes LES LIFS de données de manière à utiliser le port commun comme port de base :
`network interface modify -vserver svm-name -lif data-lif -home-port port-id`

Dans l'exemple suivant, il s'agit de « e0d ».

Par exemple :

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Retirez tous les ports VLAN utilisant les ports de cluster comme ports membres et ifgrps utilisant les ports de cluster comme ports membres.

a. Supprimez les ports VLAN :
`network port vlan delete -node node-name -vlan-name portid-vlandid`

Par exemple :

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Supprimez les ports physiques des groupes d'interface :

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Par exemple :

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Supprimer les ports VLAN et group d'interface de broadcast domain :

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modifiez les ports du groupe d'interface pour utiliser d'autres ports physiques comme membre :

`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

4. Arrêtez les nœuds à l'invite DU CHARGEUR :

```
halt -inhibit-takeover true
```

5. Se connecter à la console série des anciens contrôleurs (node_B_1-Old et node_B_2-Old) au site_B et vérifier qu'il affiche l'invite DU CHARGEUR.

6. Rassemblez les valeurs de bootarg :

   ```
   printenv
   ```

7. Déconnectez les connexions de stockage et de réseau du nœud_B_1-Old et du nœud_B_2-Old et étiquetez les câbles pour qu'ils puissent être reconnectés aux nouveaux nœuds.
8. Déconnectez les câbles d'alimentation du nœud_B_1-Old et du nœud_B_2-Old.
9. Retirez le rack des contrôleurs node_B_1-Old et node_B_2-Old.

Mise à jour des RCFs de commutateur pour les nouvelles plates-formes

Vous devez mettre à jour les commutateurs vers une configuration prenant en charge les nouveaux modèles de plate-forme.

Description de la tâche

Vous pouvez effectuer cette tâche sur le site contenant les contrôleurs en cours de mise à niveau. Dans les exemples présentés dans cette procédure, nous mettons d'abord à niveau site_B.

Les commutateurs du site_A seront mis à niveau lorsque les contrôleurs du site_A sont mis à niveau.

Étapes

1. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

   Suivez les étapes de la procédure pour votre fournisseur de commutateur :

   "Installation et configuration de MetroCluster IP"

   - "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
   - "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

2. Téléchargez et installez les fichiers RCF.

   Suivez les étapes de la section correspondant au fournisseur de votre commutateur du "Installation et configuration de MetroCluster IP".

   - "Téléchargement et installation des fichiers RCF Broadcom"
   - "Téléchargement et installation des fichiers Cisco IP RCF"

Configuration des nouveaux contrôleurs

Vous devez installer et installer les contrôleurs, effectuer la configuration requise en mode maintenance, puis démarrer les contrôleurs, et vérifier la configuration LIF sur les contrôleurs.

Configuration des nouveaux contrôleurs

Vous devez installer et câbler les nouveaux contrôleurs.

Étapes

1. Planifiez le positionnement des nouveaux modules de contrôleur et tiroirs de stockage en fonction des besoins.

   L'espace rack dépend du modèle de plateforme des modules de contrôleur, des types de switchs et du

nombre de tiroirs de stockage de votre configuration.

2. Mettez-vous à la terre.
3. Installez les modules de contrôleur sur le rack ou l'armoire.

   "Documentation des systèmes matériels ONTAP"

4. Reliez les contrôleurs aux commutateurs IP, comme décrit dans la "Installation et configuration de MetroCluster IP".
   - "Câblage des commutateurs IP"
5. Mettez les nouveaux nœuds sous tension et démarrez-les en mode de maintenance.

Restauration de la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :

   a. Vérifiez les paramètres actuels des ports :

      `ucadmin show`

   b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Cible FC	`fcadmin config -t target` *`adapter-name`*
Initiateur FC	`fcadmin config -t initiator` *`adapter-name`*

2. Quitter le mode Maintenance :

   `halt`

   Une fois que vous avez exécuté la commande, attendez que le nœud s'arrête à l'invite DU CHARGEUR.

3. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet :

   `boot_ontap maint`

4. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`
FC	`fcadmin show`

Configuration de l'état haute disponibilité sur les nouveaux contrôleurs et le châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état HA pour tous les composants devrait être "mccip".

2. Si l'état système affiché du contrôleur ou du châssis n'est pas correct, définissez l'état HA :

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

Définition des variables bootarg IP MetroCluster

Certaines valeurs d'amorçage MetroCluster IP doivent être configurées sur les nouveaux modules de contrôleur. Les valeurs doivent correspondre à celles configurées sur les anciens modules de contrôleur.

Description de la tâche

Dans cette tâche, vous utiliserez les UUID et les ID système identifiés précédemment dans la procédure de mise à niveau de "Collecte des informations avant la mise à niveau".

Étapes

1. Si les nœuds mis à niveau sont des modèles AFF A400, FAS8300 ou FAS8700, définissez les bootargs suivants à l'invite DU CHARGEUR :

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   Si les interfaces utilisent les VLAN par défaut, le vlan-ID n'est pas nécessaire.

   Les commandes suivantes définissent les valeurs pour node_B_1-New en utilisant VLAN 120 pour le premier réseau et VLAN 130 pour le second réseau :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

Les commandes suivantes définissent les valeurs pour node_B_2-New en utilisant VLAN 120 pour le premier réseau et VLAN 130 pour le second réseau :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

L'exemple suivant montre les commandes du node_B_1-New lorsque le VLAN par défaut est utilisé :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

L'exemple suivant montre les commandes du node_B_2-New lorsque le VLAN par défaut est utilisé :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. Si les nœuds mis à niveau ne sont pas des systèmes répertoriés à l'étape précédente, à l'invite DU CHARGEUR pour chacun des noeuds survivants, définissez les bootargs suivants avec local_IP/mask :

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   Les commandes suivantes définissent les valeurs du noeud_B_1-New :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

Les commandes suivantes définissent les valeurs du noeud_B_2-New :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

3. Dans l'invite DU CHARGEUR des nouveaux nœuds, définissez les UID :

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID
```

   a. Définissez les UUID sur noeud_B_1-New.

      L'exemple suivant montre les commandes de paramétrage des UID sur node_B_1-New :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. Définissez les UUID sur node_B_2-New :

      L'exemple suivant montre les commandes de paramétrage des UID sur node_B_2-New :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

4. Si les systèmes d'origine ont été configurés pour ADP, à l'invite DU CHARGEUR des nœuds de remplacement, activez ADP :

```
setenv bootarg.mcc.adp_enabled true
```

5. Définissez les variables suivantes :

```
setenv bootarg.mcc.local_config_id original-sys-id

setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> Le `setenv bootarg.mcc.local_config_id` La variable doit être définie sur l'ID système du module de contrôleur **Original**, noeud_B_1-Old.

a. Définissez les variables sur noeud_B_1-New.

L'exemple suivant montre les commandes de paramétrage des valeurs sur node_B_1-New :

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Définissez les variables sur noeud_B_2-New.

L'exemple suivant montre les commandes de paramétrage des valeurs sur node_B_2-New :

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Si vous utilisez le chiffrement avec un gestionnaire de clés externe, définissez les paramètres d'amorçage requis :

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Réaffectation des disques de l'agrégat racine

Réaffectez les disques de l'agrégat racine au nouveau module de contrôleur, en utilisant les sysids réunis précédemment.

Description de la tâche

Ces étapes sont réalisées en mode Maintenance.

> Les disques de l'agrégat racine sont les seuls disques qui doivent être réaffectés pendant le processus de mise à niveau du contrôleur. La propriété des disques des agrégats de données est gérée dans le cadre de l'opération de basculement/rétablissement.

Étapes

1. Démarrez le système en mode maintenance :

   ```
   boot_ontap maint
   ```

2. Afficher les disques du node_B_1-New à partir de l'invite du mode maintenance :

   ```
   disk show -a
   ```

   Le résultat de la commande affiche l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (537403322). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

   ```
   *> disk show -a
   Local System ID: 1574774970
   DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
   DR HOME
   ------------          ---------             -----  -------------
   -------------         -------------
   prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
   node_B_1-old(537403322)  node_B_1-old(537403322)
   .
   .
   .
   ```

3. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers les nouveaux contrôleurs.

Si vous utilisez ADP…	Utilisez ensuite cette commande…
Oui.	`disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid`
Non	`disk reassign -s old-sysid -d new-sysid`

4. Réallouer les disques root de l'agrégat sur les tiroirs disques vers les nouveaux contrôleurs :

```
disk reassign -s old-sysid -d new-sysid
```

L'exemple suivant montre la réaffectation de disques dans une configuration non ADP :

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Vérifier que les disques de l'agrégat racine sont correctement réaffectés Old-remove :

```
disk show

storage aggr status
```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zoned
                                         64-bit
```

Démarrage des nouveaux contrôleurs

Vous devez démarrer les nouveaux contrôleurs, en vous assurant que les variables bootarg sont correctes et, si nécessaire, effectuez les étapes de récupération du cryptage.

Étapes

1. Arrêter les nouveaux nœuds :

   ```
   halt
   ```

2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Vérifiez si le Partner-sysid est le courant :

   ```
   printenv partner-sysid
   ```

   Si le partenaire-sysid n'est pas correct, définissez-le :

   ```
   setenv partner-sysid partner-sysID
   ```

4. Afficher le menu de démarrage ONTAP :

   ```
   boot_ontap menu
   ```

5. Si le cryptage racine est utilisé, sélectionnez l'option de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option `10` Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option `11` Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

6. Dans le menu de démarrage, sélectionnez "`(6) mettre à jour la mémoire flash à partir de la configuration de sauvegarde".

   Avec l'option 6, le nœud redémarre deux fois avant de terminer.

   Répondez « y » aux invites de changement d'ID système. Attendez les deuxième messages de redémarrage :

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Sur LE CHARGEUR, vérifiez deux fois les valeurs d'amorçage et mettez à jour les valeurs si nécessaire.

   Suivez les étapes de la section "Définition des variables bootarg IP MetroCluster".

8. Vérifiez que le partenaire-sysid est correct :

   ```
   printenv partner-sysid
   ```

Si le partenaire-sysid n'est pas correct, définissez-le :

`setenv partner-sysid *partner-sysID*`

9. Si le cryptage racine est utilisé, sélectionnez à nouveau l'option de menu d'amorçage pour la configuration de votre gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option `10` Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.
Gestion externe des clés	Option « 11 » Suivez les invites pour fournir les entrées requises pour récupérer et restaurer la configuration du gestionnaire de clés.

Selon le paramètre du gestionnaire de clés, effectuez la procédure de récupération en sélectionnant l'option « 10 » ou « 11 », suivie de l'option `6` à la première invite du menu de démarrage. Pour démarrer complètement les nœuds, il est possible que vous deviez répéter la procédure de restauration suite à l'option « 1 » (démarrage normal).

10. Attendez que les nœuds remplacés démarrent.

Si l'un des nœuds est en mode basculement, exécutez un retour à l'aide du `storage failover giveback` commande.

11. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…
Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name`

12. Vérifier que tous les ports se trouvent dans un broadcast domain :

a. Afficher les domaines de diffusion :

`network port broadcast-domain show`

b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

"Ajout ou suppression de ports d'un broadcast domain"

c. Recréez les VLAN et les groupes d'interfaces selon les besoins.

L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

"Création d'un VLAN"

"Combinaison de ports physiques pour créer des groupes d'interfaces"

Vérification et restauration de la configuration LIF

Vérifiez que les LIFs sont hébergées sur des nœuds et des ports appropriés, tels qu'ils sont mappés au début de la procédure de mise à niveau.

À propos de ce tsak

- Cette tâche est effectuée sur site_B.
- Voir le plan de mappage des ports que vous avez créé dans "Mappage des ports des anciens nœuds sur les nouveaux nœuds".

Étapes

1. Vérifiez que les LIF sont hébergées sur le nœud et les ports appropriés avant le rétablissement.

   a. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

   b. Remplacez la configuration des ports pour assurer un placement LIF approprié :

   ```
   vserver config override -command "network interface modify -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node new_node_name"
   ```

   Lors de la saisie de la commande network interface modify dans le `vserver config override` vous ne pouvez pas utiliser la fonction de saisie semi-automatique de l'onglet. Vous pouvez créer le réseau `interface modify` à l'aide de la commande auto complete, puis placez-la dans le `vserver config override` commande.

   a. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

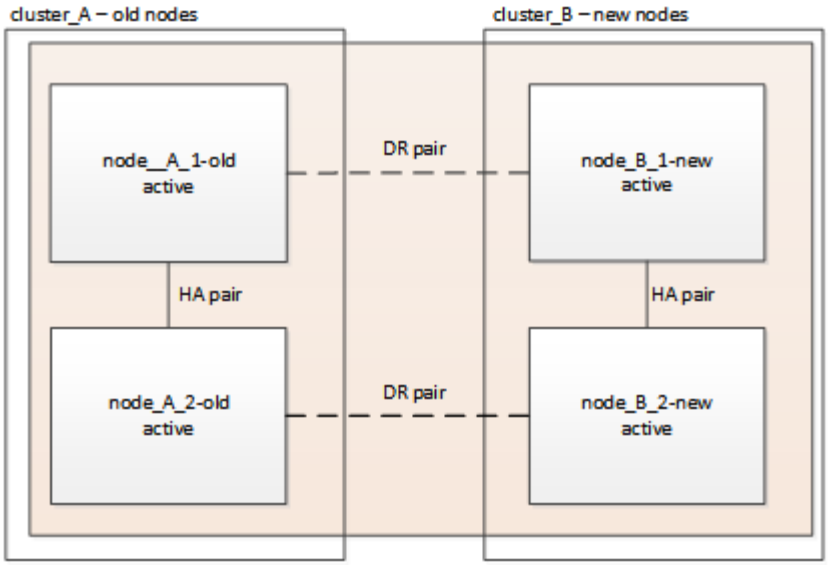
2. Revert les interfaces sur leur home node :

   ```
   network interface revert * -vserver vserver-name
   ```

   Suivez cette étape sur tous les SVM, si nécessaire.

Reprise de la configuration MetroCluster

Cette tâche vous permet d'effectuer le rétablissement, et la configuration MetroCluster revient à un fonctionnement normal. Les nœuds du site_A sont toujours en attente de mise à niveau.



Étapes

1. Émettez le `metrocluster node show` Commande on site_B et vérifiez la sortie.
   a. Vérifiez que les nouveaux nœuds sont correctement représentés.
   b. Vérifiez que les nouveaux nœuds sont en attente de rétablissement.
2. Exécutez ce rétablissement et ce rétablissement en exécutant les commandes requises depuis n'importe quel nœud du cluster actif (cluster non mis à niveau).
   a. Réparation des agrégats de données :
   `metrocluster heal aggregates`
   b. Corriger les agrégats racine :

   `metrocluster heal root`

   c. Rétablissement du cluster :

   `metrocluster switchback`

3. Vérifier la progression de l'opération de rétablissement :

   `metrocluster show`

   L'opération de rétablissement est toujours en cours lorsque la sortie s'affiche `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'opération de rétablissement est terminée lorsque la sortie affiche normal :

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Si un rétablissement prend beaucoup de temps, vous pouvez vérifier l'état des lignes de base en cours en utilisant le `metrocluster config-replication resync-status show` commande. Cette commande est au niveau de privilège avancé.

Vérification de l'état de santé de la configuration MetroCluster

Après la mise à niveau des modules de contrôleur, vous devez vérifier l'état de santé de la configuration MetroCluster.

Description de la tâche

Cette tâche peut être effectuée sur n'importe quel nœud de la configuration MetroCluster.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster :
   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :
      `metrocluster show`
   b. Effectuer une vérification MetroCluster :
      `metrocluster check run`
   c. Afficher les résultats de la vérification MetroCluster :

      `metrocluster check show`

2. Vérifiez la connectivité et le statut de MetroCluster.

a. Vérifiez les connexions IP du MetroCluster :

```
storage iscsi-initiator show
```

b. Vérifiez que les nœuds fonctionnent :

```
metrocluster node show
```

c. Vérifier que les interfaces IP MetroCluster sont bien les suivantes :

```
metrocluster configuration-settings interface show
```

d. Vérifier que le basculement local est activé :

```
storage failover show
```

Mise à niveau des nœuds du cluster_A

Vous devez répéter les tâches de mise à niveau sur cluster_A.

Étapes

1. Répétez les étapes pour mettre à niveau les nœuds du cluster_A, en commençant par "Préparation de la mise à niveau".

   Au fur et à mesure que vous effectuez les tâches, toutes les références aux clusters et aux nœuds sont inversées. Par exemple, si vous avez l'intention de basculer du cluster_A, vous effectuez le basculement du cluster_B.

Restauration de la surveillance du disjoncteur d'attache ou du médiateur

Après avoir effectué la mise à niveau de la configuration MetroCluster, vous pouvez reprendre la surveillance avec l'utilitaire Tiebreaker ou Mediator.

Étapes

1. Restaurer la surveillance si nécessaire, en suivant la procédure de configuration.

Si vous utilisez…	Suivre cette procédure
Disjoncteur d'attache	"Ajout des configurations MetroCluster".
Médiateur	Lien :../install-ip/concept_mediator_requirements.html [Configuration du service médiateur ONTAP à partir d'une configuration IP MetroCluster].
Applications tierces	Reportez-vous à la documentation du produit.

Envoi d'un message AutoSupport personnalisé après maintenance

Une fois la mise à niveau terminée, envoyer un message AutoSupport indiquant la fin de la maintenance. La

création automatique de dossier peut reprendre.

Étapes

1. Pour reprendre la génération automatique de dossier de support, envoyez un message AutoSupport pour indiquer que la maintenance est terminée.

   a. Lancer la commande suivante :
   `system node autosupport invoke -node * -type all -message MAINT=end`

   b. Répétez la commande sur le cluster partenaire.

Mise à niveau des contrôleurs AFF A700/FAS9000 vers AFF A900/FAS9500 dans une configuration IP MetroCluster avec basculement et rétablissement (ONTAP 9.10.1 ou version ultérieure)

Il est possible d'utiliser le basculement MetroCluster pour fournir un service sans interruption aux clients pendant la mise à niveau des modules de contrôleur du cluster partenaire. Dans le cadre de cette procédure, d'autres composants (tels que des tiroirs de stockage ou des commutateurs) ne peuvent pas être mis à niveau.

Description de la tâche

- Pour mettre à niveau les modules de contrôleur AFF A700 vers AFF A900, les contrôleurs doivent exécuter ONTAP 9.10.1 ou une version ultérieure.
- Pour mettre à niveau les modules de contrôleur FAS9000 vers le système FAS9500, les contrôleurs doivent exécuter ONTAP 9.10.1P3 ou version ultérieure.
- Tous les contrôleurs de la configuration doivent être mis à niveau pendant la même période de maintenance.

  L'exploitation de la configuration MetroCluster avec un système AFF A700 et un système AFF A900, ou un système FAS9000 et un contrôleur FAS9500 n'est pas prise en charge en dehors de cette activité de maintenance.

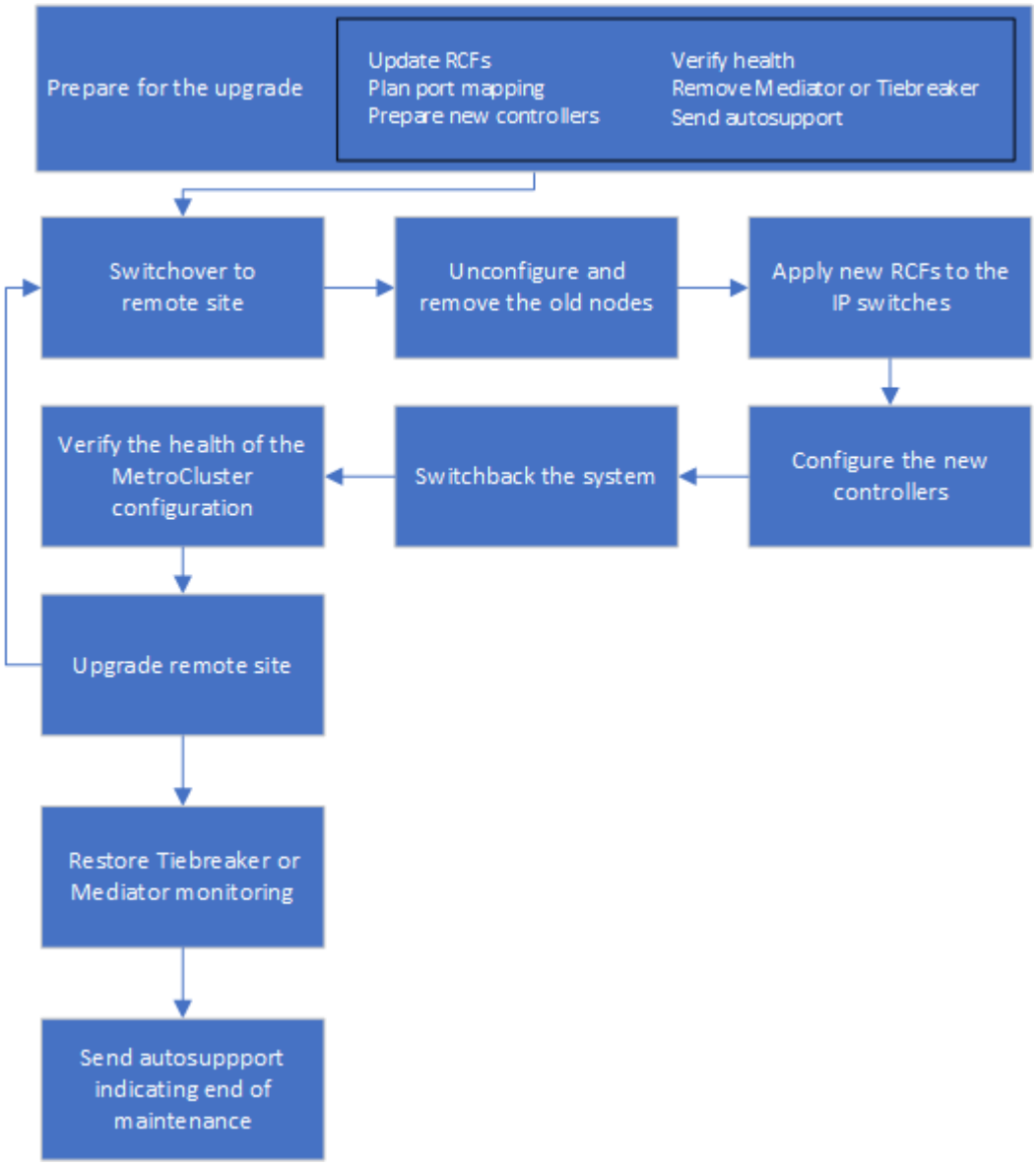
- Les commutateurs IP doivent exécuter une version de micrologiciel prise en charge.
- Vous allez réutiliser les adresses IP, les masques réseau et les passerelles des plates-formes d'origine sur les nouvelles plates-formes.
- Les noms d'exemple suivants sont utilisés dans cette procédure, dans les exemples et les graphiques :
  - Site_A
    - Avant la mise à niveau :
      - Nœud_A_1-A700
      - Nœud_A_2-A700
    - Après la mise à niveau :
      - Node_A_1-A900
      - Node_A_2-A900
  - Site_B
    - Avant la mise à niveau :

- Node_B_1-A700
- Node_B_2-A700

- Après la mise à niveau :
  - Node_B_1-A900
  - Node_B_2-A900

Flux de production de mise à niveau des contrôleurs dans une configuration MetroCluster IP

Vous pouvez utiliser le diagramme de workflow pour planifier les tâches de mise à niveau.



Préparation à la mise à niveau

Avant d'apporter des modifications à la configuration MetroCluster existante, vous devez vérifier l'état de santé de la configuration, préparer les nouvelles plateformes et effectuer d'autres tâches diverses.

Désactivez le connecteur 7 sur le contrôleur AFF A700 ou FAS9000

La configuration MetroCluster d'un AFF A900 ou FAS9500 utilise l'un de chacun des ports des cartes de reprise sur incident situées dans les emplacements 5 et 7. Avant de commencer la mise à niveau, si des cartes se trouvent dans l'emplacement 7 des systèmes AFF A700 ou FAS9000, vous devez les déplacer vers d'autres emplacements pour tous les nœuds du cluster.

Mettre à jour les fichiers RCF des commutateurs MetroCluster avant de mettre à niveau les contrôleurs

Vous devez mettre à jour les fichiers RCF sur les commutateurs MetroCluster lors de cette mise à niveau. Le tableau suivant fournit les plages de VLAN prises en charge pour les configurations IP MetroCluster AFF A900/FAS9500.

Modèle de plateforme	ID de VLAN pris en charge
• AFF A900 OU FAS9500	• 10 • 20 • Toute valeur comprise entre 101 et 4096 inclus.

- Si le commutateur n'est pas configuré avec la version minimale du fichier RCF pris en charge, vous devez mettre à jour le fichier RCF. Pour connaître la version de fichier RCF appropriée pour votre modèle de commutateur, reportez-vous à "Outil RcfFileGenerator". Les étapes suivantes sont destinées à l'application du fichier RCF.

Étapes

1. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

   Suivez les étapes de la section correspondant au fournisseur de votre commutateur du "Installation et configuration IP de MetroCluster" le contenu.

   - "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
   - "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

2. Téléchargez et installez les fichiers RCF.

   Suivez les étapes de la section "Installation et configuration IP de MetroCluster" le contenu.

   - "Téléchargement et installation des fichiers RCF Broadcom"
   - "Téléchargement et installation des fichiers Cisco IP RCF"

Mappage des ports des anciens nœuds sur les nouveaux nœuds

Lors de la mise à niveau d'un système AFF A700 vers un système AFF A900, ou FAS9000 vers un système FAS9500, vous ne devez pas modifier les ports du réseau de données, les ports d'adaptateur SAN FCP et les ports de stockage SAS et NVMe. Les LIF de données restent au même endroit pendant et après la mise à niveau. Vous n'avez donc pas besoin de mapper les ports réseau des anciens nœuds sur les nouveaux nœuds.

Vérifier l'état de santé des MetroCluster avant la mise à niveau du site

Vous devez vérifier l'état de santé et la connectivité de la configuration MetroCluster avant d'effectuer la mise à niveau.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :

   a. Vérifiez si les nœuds sont multipathed :
   `node run -node node-name sysconfig -a`

      Vous devez exécuter cette commande pour chaque nœud de la configuration MetroCluster.

   b. Vérifier qu'il n'y a pas de disques défectueux dans la configuration :
   `storage disk show -broken`

      Vous devez exécuter cette commande sur chaque nœud de la configuration MetroCluster.

   c. Vérifiez si des alertes d'intégrité sont émises :

      `system health alert show`

      Vous devez exécuter cette commande sur chaque cluster.

   d. Vérifier les licences sur les clusters :

      `system license show`

      Vous devez exécuter cette commande sur chaque cluster.

   e. Vérifiez les périphériques connectés aux nœuds :

      `network device-discovery show`

      Vous devez exécuter cette commande sur chaque cluster.

   f. Vérifiez que le fuseau horaire et l'heure sont correctement définis sur les deux sites :

      `cluster date show`

   Vous devez exécuter cette commande sur chaque cluster. Vous pouvez utiliser le `cluster date` commande pour configurer le fuseau horaire et le fuseau horaire.

2. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.

   a. Confirmer la configuration MetroCluster et la présence du mode opérationnel `normal`:
   `metrocluster show`

   b. Confirmer que tous les nœuds attendus sont affichés :
   `metrocluster node show`

   c. Exécutez la commande suivante :

      `metrocluster check run`

   d. Afficher les résultats de la vérification MetroCluster :

      `metrocluster check show`

3. Vérifiez le câblage MetroCluster à l'aide de l'outil Config Advisor.

a. Téléchargez et exécutez Config Advisor.

   "Téléchargement NetApp : Config Advisor"

b. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.

Recueillez les informations avant la mise à niveau

Avant la mise à niveau, vous devez collecter les informations de chacun des nœuds et, si nécessaire, ajuster les domaines de diffusion réseau, supprimer tous les VLAN et groupes d'interfaces et collecter des informations de cryptage.

Étapes

1. Notez le câblage physique de chaque nœud et étiqueteuse les câbles si nécessaire pour permettre un câblage correct des nouveaux nœuds.
2. Collectez les valeurs de sortie des commandes suivantes pour chaque nœud :
   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`
   - `vserver fcp initiator show`
   - `storage disk show`
   - `metrocluster configuration-settings interface show`
3. Rassemblez les UUID du site_B (site dont les plates-formes sont actuellement mises à niveau) :
   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Ces valeurs doivent être configurées avec précision sur les nouveaux modules de contrôleur site_B pour garantir la réussite de la mise à niveau. Copiez les valeurs dans un fichier afin de pouvoir les copier dans les commandes appropriées ultérieurement dans le processus de mise à niveau. + l'exemple suivant montre la sortie de la commande avec les UID :

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
   (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

Il est recommandé d'enregistrer les UUID dans un tableau similaire à ce qui suit.

Cluster ou nœud	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1-A700	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2-A700	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
Nœud_A_1-A700	f03cb63c-9a7e-11e7-b68b-00a098908039
Nœud_A_2-A700	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Si les nœuds MetroCluster se trouvent dans une configuration SAN, collectez les informations pertinentes.

   Vous devez collecter le résultat des commandes suivantes :

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Si le volume racine est chiffré, collectez et enregistrez la phrase secrète utilisée pour le gestionnaire de clés : `security key-manager backup show`
6. Si les nœuds MetroCluster utilisent le chiffrement pour des volumes ou des agrégats, copiez les

informations concernant les clés et les clés de phrase secrète. Pour plus d'informations, reportez-vous à la section "Sauvegarde manuelle des informations de gestion intégrée des clés".

a. Si le gestionnaire de clés intégré est configuré : `security key-manager onboard show-backup`+ vous aurez besoin de la phrase de passe plus tard dans la procédure de mise à niveau.

b. Si le protocole KMIP (Enterprise Key Management) est configuré, exécutez les commandes suivantes :

```
security key-manager external show -instance
security key-manager key query
```

7. Collectez les ID système des nœuds existants : `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

Le résultat suivant montre les disques réattribués.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322           537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323           537403324
1           cluster_B node_B_2-A700   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Retirer le système de surveillance du médiateur ou du disjoncteur d'attache

Avant de mettre à niveau les plates-formes, vous devez supprimer la surveillance si la configuration MetroCluster est surveillée à l'aide de l'utilitaire Tiebreaker ou Mediator.

Étapes

1. Collectez les valeurs de sortie de la commande suivante :

```
storage iscsi-initiator show
```

2. Supprimez la configuration MetroCluster existante du logiciel disjoncteur d'attache, du médiateur ou d'autres logiciels pouvant initier le basculement.

Si vous utilisez…	Utilisez cette procédure…

Disjoncteur d'attache	"Suppression des configurations MetroCluster" Dans le contenu *MetroCluster Tiebreaker installation et configuration*
Médiateur	Exécutez la commande suivante depuis l'invite ONTAP : `metrocluster configuration-settings mediator remove`
Applications tierces	Reportez-vous à la documentation du produit.

Envoyer un message AutoSupport personnalisé avant la maintenance

Avant d'effectuer la maintenance, vous devez envoyer un message AutoSupport pour informer le support technique que la maintenance est en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Connectez-vous au cluster.
2. Appelez un message AutoSupport indiquant le début de la maintenance :

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   Le `maintenance-window-in-hours` le paramètre spécifie la longueur de la fenêtre de maintenance, avec un maximum de 72 heures. Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Répétez cette procédure sur le site du partenaire.

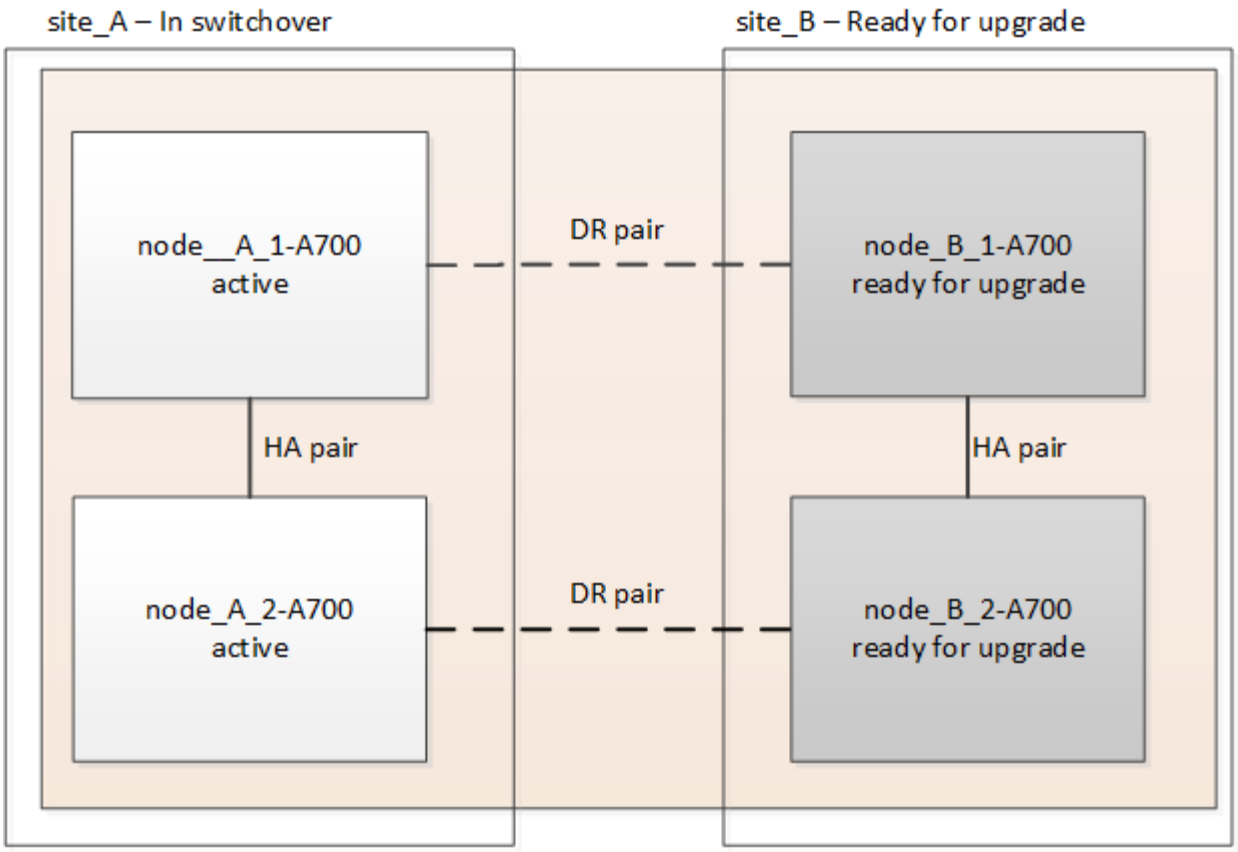
Basculer la configuration MetroCluster

Vous devez basculer la configuration vers site_A afin de pouvoir mettre à niveau les plateformes du site_B.

Description de la tâche

Cette tâche doit être effectuée sur site_A.

Une fois cette tâche effectuée, site_A est actif et transmet les données aux deux sites. Site_B est inactif et prêt à commencer le processus de mise à niveau.



Étapes

1. Basculer la configuration MetroCluster sur site_A afin de mettre à niveau les nœuds site_B :

   a. Exécutez la commande suivante sur site_A :

      `metrocluster switchover -controller-replacement true`

      L'opération peut prendre plusieurs minutes.

   b. Surveiller le fonctionnement du basculement :

      `metrocluster operation show`

   c. Une fois l'opération terminée, vérifiez que les nœuds sont en état de basculement :

      `metrocluster show`

   d. Vérifier l'état des nœuds MetroCluster :

      `metrocluster node show`

   La fonctionnalité de correction automatique des agrégats après le basculement négocié est désactivée lors de la mise à niveau du contrôleur. Les nœuds du site_B sont arrêtés et arrêtés au niveau du `LOADER` à l'invite.

Retirez le module de contrôleur de la plateforme AFF A700 ou FAS9000 et le NVS

Description de la tâche

Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.

Étapes

1. Rassemblez les valeurs de bootarg à partir des deux nœuds sur site_B : `printenv`
2. Mettez le châssis hors tension au niveau du site_B.

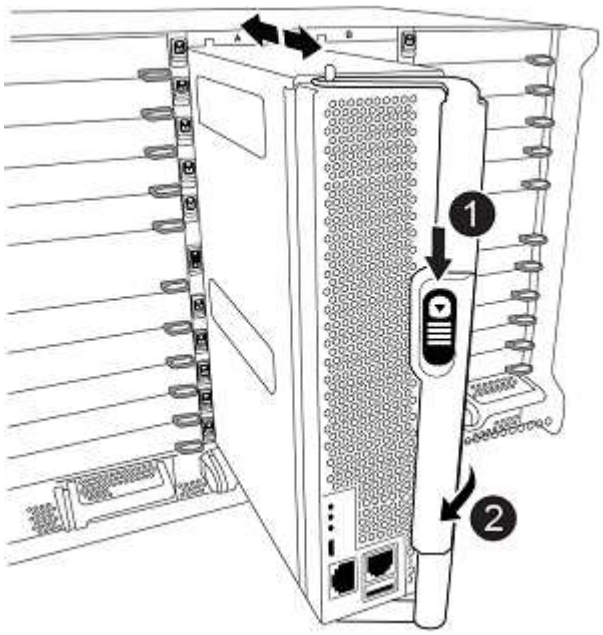
Retirez le module de contrôleur AFF A700 ou FAS9000

Suivre la procédure suivante pour retirer le module de contrôleur AFF A700 ou FAS9000

Étapes

1. Détachez le câble de la console, le cas échéant, et le câble de gestion du module de contrôleur avant de retirer le module de contrôleur.
2. Déverrouiller et retirer le module de contrôleur du châssis.

   a. Faites glisser le bouton orange sur la poignée de came vers le bas jusqu'à ce qu'il se déverrouille.



	Bouton de déverrouillage de la poignée de came
	Poignée de came

   a. Faites pivoter la poignée de came de façon à ce qu'elle désengage complètement le module de contrôleur du châssis, puis faites glisser le module de contrôleur hors du châssis. Assurez-vous de prendre en charge la partie inférieure du module de contrôleur lorsque vous le faites glisser hors du châssis.

Retirez le module NVS AFF A700 ou FAS9000

Utilisez la procédure suivante pour retirer le module NVS AFF A700 ou FAS9000.

Remarque : le module NVS est dans le logement 6 et représente une hauteur double par rapport aux autres modules du système.

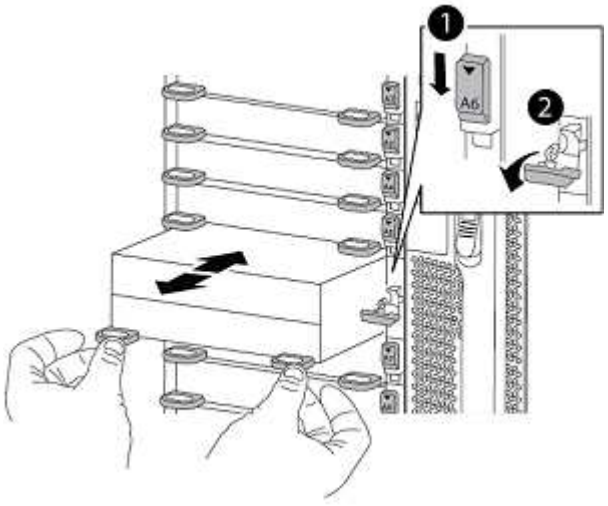
Étapes

1. Déverrouillez et retirez le NVS du logement 6.

   a. Appuyer sur le bouton « came » numéroté et numéroté. Le bouton de came s'éloigne du châssis.

   b. Faites pivoter le loquet de came vers le bas jusqu'à ce qu'il soit en position horizontale. Le NVS se désengage du châssis et se déplace de quelques pouces.

   c. Retirez le NVS du châssis en tirant sur les languettes de traction situées sur les côtés de la face du module.



	Loquet de came d'E/S numéroté et numéroté
	Loquet d'E/S complètement déverrouillé

2. Si vous utilisez des modules d'extension utilisés comme périphériques coredump sur les systèmes AFF A700 ou FAS9000 NVS, ne les transférez pas vers les systèmes AFF A900 ou FAS9500 NVS. Ne transférez aucune pièce du module de contrôleur AFF A700 ou FAS9000, et NVS, vers le module AFF A900 ou FAS9500.

Installez les AFF A900 ou FAS9500 NVS et les modules de contrôleur

Vous devez installer les NVS et le module de contrôleur AFF A900 ou FAS9500 que vous avez reçus dans le kit de mise à niveau sur les deux nœuds du site_B. Ne déplacez pas le dispositif de coredump du module NVS AFF A700 ou FAS9000 vers le module NVS AFF A900 ou FAS9500.

Description de la tâche

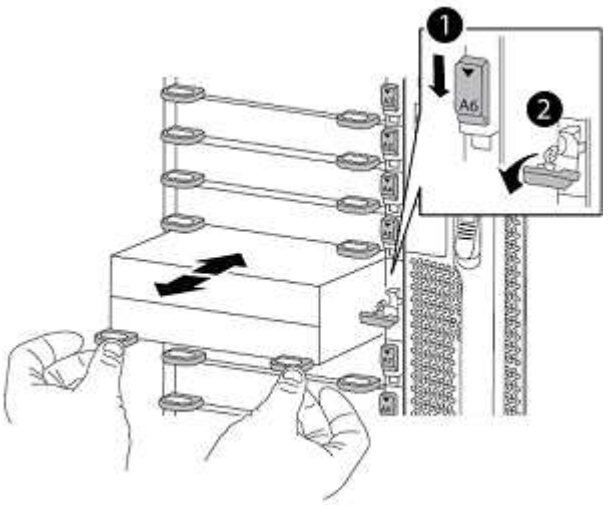
Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.

Installez les NVS AFF A900 ou FAS9500

Utilisez la procédure suivante pour installer les NVS AFF A900 ou FAS9500 dans le logement 6 des deux nœuds du site_B.

Étapes

1. Alignez le système NVS sur les bords de l'ouverture du châssis dans le logement 6.
2. Faites glisser doucement le système NVS dans le logement jusqu'à ce que le loquet de came d'E/S numéroté et numéroté commence à s'engager avec la goupille de came d'E/S, puis poussez le loquet de came d'E/S jusqu'à ce qu'il s'enclenche pour verrouiller le système NVS en place.



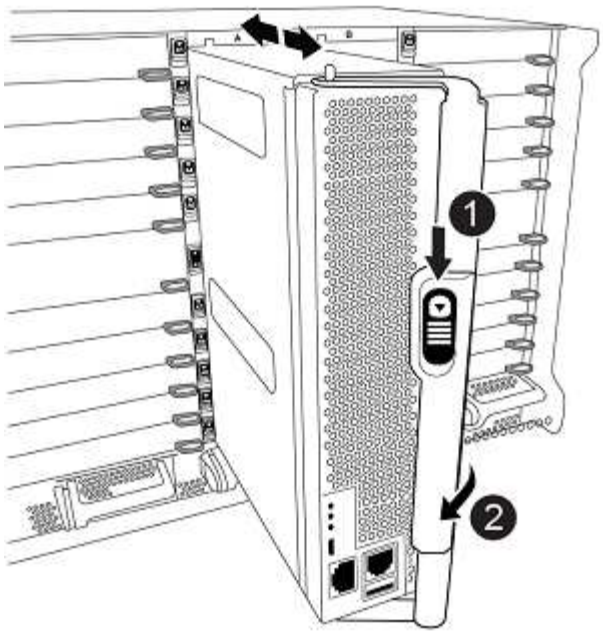
	Loquet de came d'E/S numéroté et numéroté
	Loquet d'E/S complètement déverrouillé

Installez le module de contrôleur AFF A900 ou FAS9500.

Utilisez la procédure suivante pour installer le module de contrôleur AFF A900 ou FAS9500.

Étapes

1. Alignez l'extrémité du module de contrôleur avec l'ouverture du châssis, puis poussez doucement le module de contrôleur à mi-course dans le système.
2. Poussez fermement le module de contrôleur dans le châssis jusqu'à ce qu'il rencontre le fond de panier central et qu'il soit bien en place. Le loquet de verrouillage s'élève lorsque le module de contrôleur est bien en place. Attention : pour éviter d'endommager les connecteurs, ne pas exercer de force excessive lors du déplacement du module de contrôleur dans le châssis.
3. Reliez les ports de gestion et de console au module de contrôleur.



	Bouton de déverrouillage de la poignée de came
	Poignée de came

4. Installez la deuxième carte X91146A dans l'emplacement 7 de chaque nœud.
   a. Déplacer la connexion e5b vers e7b.
   b. Placer la connexion e5a sur e5b.

> Le slot 7 sur tous les nœuds du cluster doit être vide comme indiqué dans Mappage des ports des anciens nœuds sur les nouveaux nœuds section.

5. Mettez le châssis SOUS tension et connectez-vous à la console série.
6. Après l'initialisation du BIOS, si le nœud démarre AUTOBOOT, interrompez le AUTOBOOT en appuyant sur Control-C.
7. Une fois l'AUTOBOOT interrompue, les nœuds s'arrêtent dans l'invite DU CHARGEUR. Si vous n'interrompez pas AUTOBOOT à l'heure et que le nœud 1 commence le démarrage, attendez que l'invite appuie sur Ctrl-C pour accéder au menu de démarrage. Une fois le nœud arrêté dans le menu de démarrage, utilisez l'option 8 pour redémarrer le nœud et interrompre l'AUTOBOOT pendant le redémarrage.
8. À l'invite DU CHARGEUR, définissez les variables d'environnement par défaut : valeurs par défaut
9. Enregistrez les paramètres des variables d'environnement par défaut : `saveenv`

Nœuds NetBoot sur site_B

Après avoir remplacé le module de contrôleur AFF A900 ou FAS9500 par un système NVS, vous devez netboot les nœuds AFF A900 ou FAS9500 et installer la même version et le même niveau de patch de ONTAP qui s'exécute sur le cluster. Le terme netboot signifie que vous êtes en cours de démarrage à partir d'une image ONTAP stockée sur un serveur distant. Pour vous préparer à netboot, vous devez ajouter une copie de l'image de démarrage ONTAP 9 sur un serveur web auquel le système peut accéder. Il n'est pas possible de

vérifier la version de ONTAP installée sur le support de démarrage d'un module de contrôleur AFF A900 ou FAS9500, sauf s'il est installé dans un châssis et sous tension. La version ONTAP du support de démarrage AFF A900 ou FAS9500 doit être identique à la version ONTAP exécutée sur un système AFF A700 ou FAS9000 mis à niveau, et les images de démarrage primaire et de sauvegarde doivent correspondre. Vous pouvez configurer les images en effectuant un démarrage suivi de l' `wipeconfig` commande dans le menu de démarrage. Si le module de contrôleur était auparavant utilisé dans un autre cluster, le `wipeconfig` commande efface toute configuration résiduelle sur le support d'amorçage.

Avant de commencer

- Vérifiez que vous pouvez accéder à un serveur HTTP avec le système.
- Vous devez télécharger les fichiers système nécessaires pour votre système et la version correcte de ONTAP sur le site de support NetApp.

Description de la tâche

Vous devez netboot les nouveaux contrôleurs, si la version de ONTAP installée n'est pas identique à la version installée sur les contrôleurs d'origine. Après avoir installé chaque nouveau contrôleur, vous démarrez le système 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.

Étapes

1. Accédez au "Site de support NetApp" pour télécharger les fichiers utilisés pour effectuer le démarrage sur le réseau du système.
2. Télécharger le logiciel ONTAP approprié depuis la section de téléchargement de logiciels du site de support NetApp et stocker le `ontap-version_image.tgz` fichier dans un répertoire accessible sur le web.
3. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.
4. La liste de vos répertoires doit contenir ontap_version_image.tgz.
5. 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 DCHP (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. `<netmask>` est le masque de réseau du système de stockage. `<gateway>` est la passerelle du système de stockage. `<dns_addr>` Est l'adresse IP d'un serveur de noms sur votre réseau. Ce paramètre est facultatif. `<dns_domain>` Est le nom de domaine DNS (Domain Name Service). Ce paramètre est facultatif. REMARQUE : d'autres paramètres peuvent être nécessaires pour votre interface. Entrez `help ifconfig` à l'invite du micrologiciel pour plus de détails.

6. Démarrage sur le nœud_B_1 : `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Le `<path_to_the_web-accessible_directory>` vous devez indiquer où vous avez téléchargé le `<ontap_version>\_image.tgz` dans Étape 2.

   N'interrompez pas l'amorçage.

7. Attendez que le nœud_B_1 s'exécute maintenant sur le module de contrôleur AFF A900 ou FAS9500 pour démarrer et afficher les options du menu de démarrage comme indiqué ci-dessous :

```
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)?
```

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. REMARQUE : ignorez le message suivant : `This procedure is not supported for Non-`

`Disruptive Upgrade on an HA pair`. Cette remarque s'applique aux mises à niveau logicielles ONTAP sans interruption et non aux mises à niveau du contrôleur.

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.

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. Entrez `y to reboot when you see the following prompt: `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. À l'invite, exécutez le `wipeconfig` pour effacer toute configuration précédente sur le support de démarrage :
    a. Lorsque vous voyez le message suivant, répondez `yes`: `This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:`
    b. Le nœud redémarre pour terminer le `wipeconfig` puis s'arrête au menu de démarrage.
12. Sélectionnez option `5` pour passer en mode maintenance à partir du menu de démarrage. Réponse `yes` sur les invites jusqu'à ce que le nœud s'arrête en mode maintenance et à l'invite de commande *.
13. Répétez cette procédure pour netboot node_B_2.

Restaurez la configuration HBA

En fonction de la présence et de la configuration des cartes HBA dans le module de contrôleur, vous devez les configurer correctement pour l'utilisation de votre site.

Étapes

1. En mode Maintenance, configurez les paramètres de tous les HBA du système :
    a. Vérifiez les paramètres actuels des ports :

    ```
    ucadmin show
    ```

    b. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité…	Utilisez cette commande…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*

Cible FC	`fcadmin config -t target adapter-name`
Initiateur FC	`fcadmin config -t initiator adapter-name`

2. Quitter le mode Maintenance :

   `halt`

   Une fois que vous avez exécuté la commande, attendez que le nœud s'arrête à l'invite DU CHARGEUR.

3. Redémarrez le nœud en mode maintenance pour que les modifications de configuration prennent effet :

   `boot_ontap maint`

4. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA…	Utilisez cette commande…
CNA	`ucadmin show`
FC	`fcadmin show`

Définissez l'état de haute disponibilité sur les nouveaux contrôleurs et châssis

Vous devez vérifier l'état haute disponibilité des contrôleurs et du châssis, et mettre à jour si nécessaire l'état en fonction de la configuration du système.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état de haute disponibilité de tous les composants doit être `mccip`.

2. Si l'état système affiché du contrôleur ou du châssis n'est pas correct, définissez l'état HA :

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

3. Arrêter le nœud : `halt`

   Le nœud doit s'arrêter au niveau du `LOADER>` à l'invite.

4. Sur chaque nœud, vérifiez la date, l'heure et le fuseau horaire du système : `show date`
5. Si nécessaire, définissez la date en UTC ou GMT : `set date <mm/dd/yyyy>`
6. Vérifiez l'heure à l'aide de la commande suivante à l'invite de l'environnement d'amorçage : `show time`

7. Si nécessaire, définissez l'heure en UTC ou GMT : `set time <hh:mm:ss>`
8. Enregistrer les paramètres : `saveenv`
9. Collecter les variables d'environnement : `printenv`

Mettre à jour les fichiers RCF de commutateur afin de s'adapter aux nouvelles plateformes

Vous devez mettre à jour les commutateurs vers une configuration prenant en charge les nouveaux modèles de plate-forme.

Description de la tâche

Vous pouvez effectuer cette tâche sur le site contenant les contrôleurs en cours de mise à niveau. Dans les exemples présentés dans cette procédure, nous mettons d'abord à niveau site_B.

Les commutateurs du site_A seront mis à niveau lorsque les contrôleurs du site_A sont mis à niveau.

Étapes

1. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

   Suivez les étapes de la section correspondant à votre fournisseur de commutateur dans la section *MetroCluster IP installation and Configuration*.

   "Installation et configuration de MetroCluster IP"

   - "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
   - "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

2. Téléchargez et installez les fichiers RCF.

   Suivez les étapes de la section correspondant au fournisseur de votre commutateur du "Installation et configuration de MetroCluster IP".

   - "Téléchargement et installation des fichiers RCF Broadcom"
   - "Téléchargement et installation des fichiers Cisco IP RCF"

Configuration des nouveaux contrôleurs

Les nouveaux contrôleurs doivent être prêts et câblés à ce stade.

Définissez les variables bootarg IP MetroCluster

Certaines valeurs d'amorçage MetroCluster IP doivent être configurées sur les nouveaux modules de contrôleur. Les valeurs doivent correspondre à celles configurées sur les anciens modules de contrôleur.

Description de la tâche

Dans cette tâche, vous utiliserez les UUID et les ID système identifiés précédemment dans la procédure de mise à niveau de "Collecte des informations avant la mise à niveau".

Étapes

1. Au `LOADER>` À l'invite, définissez les bootargs suivants sur les nouveaux nœuds à site_B :

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```

L'exemple suivant définit les valeurs pour node_B_1-A900 à l'aide du VLAN 120 pour le premier réseau et du VLAN 130 pour le second réseau :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

L'exemple suivant définit les valeurs pour node_B_2-A900 à l'aide du VLAN 120 pour le premier réseau et du VLAN 130 pour le second réseau :

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

2. Dans les nouveaux nœuds » `LOADER` À l'invite, définissez les UUID :

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID
```

   a. Définissez les UUID sur le noeud_B_1-A900.

      L'exemple suivant montre les commandes de paramétrage des UID sur node_B_1-A900 :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Définissez les UUID sur le noeud_B_2-A900 :

L'exemple suivant montre les commandes de paramétrage des UID sur node_B_2-A900 :

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Si les systèmes d'origine ont été configurés pour ADP, à l'invite DU CHARGEUR des nœuds de remplacement, activez ADP :

```
setenv bootarg.mcc.adp_enabled true
```

4. Définissez les variables suivantes :

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

Le `setenv bootarg.mcc.local_config_id` La variable doit être définie sur sys-ID du module de contrôleur **Original**, node_B_1-A700.

a. Définissez les variables sur Node_B_1-A900.

L'exemple suivant montre les commandes de paramétrage des valeurs sur node_B_1-A900 :

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Définissez les variables sur Node_B_2-A900.

L'exemple suivant montre les commandes de paramétrage des valeurs sur node_B_2-A900 :

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Si vous utilisez le chiffrement avec un gestionnaire de clés externe, définissez les paramètres d'amorçage requis :

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Réallouer les disques racine de l'agrégat

Réaffectez les disques de l'agrégat racine au nouveau module de contrôleur, en utilisant les sysids réunis précédemment.

Description de la tâche

Ces étapes sont réalisées en mode Maintenance.

Étapes

1. Démarrez le système en mode maintenance :

   ```
   boot_ontap maint
   ```

2. Afficher les disques du nœud_B_1-A900 à partir de l'invite du mode maintenance :

   ```
   disk show -a
   ```

   Le résultat de la commande affiche l'ID système du nouveau module de contrôleur (1574774970). Cependant, les disques de l'agrégat racine appartiennent toujours à l'ancien ID système (537403322). Dans cet exemple, les disques qui appartiennent aux autres nœuds de la configuration MetroCluster ne s'affichent pas.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------              -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. Réallouer les disques racine de l'agrégat sur les tiroirs disques vers les nouveaux contrôleurs.

Si vous utilisez ADP…	Utilisez ensuite cette commande…
Oui.	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
Non	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Réallouer les disques root de l'agrégat sur les tiroirs disques vers les nouveaux contrôleurs :

   `disk reassign -s old-sysid -d new-sysid`

   L'exemple suivant montre la réaffectation de disques dans une configuration non ADP :

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Vérifier que les disques de l'agrégat racine sont correctement réaffectés Old-remove :

```
disk show

storage aggr status
```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Démarrer les nouveaux contrôleurs

Vous devez démarrer les nouveaux contrôleurs, en vous assurant que les variables bootarg sont correctes et, si nécessaire, effectuez les étapes de récupération du cryptage.

Étapes

1. Arrêter les nouveaux nœuds :

   ```
   halt
   ```

2. Si le gestionnaire de clés externe est configuré, définissez les paramètres bootargs associés :

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Vérifiez si le Partner-sysid est le courant :

   ```
   printenv partner-sysid
   ```

   Si le partenaire-sysid n'est pas correct, définissez-le :

   ```
   setenv partner-sysid partner-sysID
   ```

4. Afficher le menu de démarrage ONTAP :

   ```
   boot_ontap menu
   ```

5. Si le cryptage racine est utilisé, sélectionnez l'option de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option 10 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés
Gestion externe des clés	Option 11 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés

6. Dans le menu de démarrage, sélectionnez `(6) Update flash from backup config`.

   Avec l'option 6, le nœud redémarre deux fois avant de terminer.

   Répondez `y` aux invites de changement d'id système. Attendez les deuxième messages de redémarrage :

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Interrompez l'AUTOBOOT pour arrêter les contrôleurs du CHARGEUR.

   Sur chaque nœud, vérifiez les bootargs définis dans "Définition des variables bootarg IP MetroCluster" et corriger toute valeur incorrecte. Ne passez à l'étape suivante qu'après avoir vérifié les valeurs de bootarg.

8. Vérifiez que le partenaire-sysid est correct :

   ```
   printenv partner-sysid
   ```

   Si le partenaire-sysid n'est pas correct, définissez-le :

   ```
   setenv partner-sysid partner-sysID
   ```

9. Si le cryptage racine est utilisé, sélectionnez l'option de menu de démarrage pour votre configuration de gestion des clés.

Si vous utilisez…	Sélectionnez cette option de menu de démarrage…
Gestion intégrée des clés	Option 10 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés
Gestion externe des clés	Option 11 et suivez les invites pour fournir les entrées requises pour récupérer ou restaurer la configuration du gestionnaire de clés

   Vous devez effectuer la procédure de récupération en sélectionnant l'option 10 ou l'option 11 selon le paramètre du gestionnaire de clés et l'option 6 à l'invite du menu de démarrage. Pour démarrer complètement les nœuds, il peut être nécessaire d'effectuer la procédure de restauration suite à l'option 1 (démarrage normal).

10. Attendez que les nouveaux nœuds, Node_B_1-A900 et node_B_2-A900, démarrent.

    Si l'un des nœuds est en mode basculement, exécutez un retour à l'aide du `storage failover giveback` commande.

11. Si le chiffrement est utilisé, restaurez les clés à l'aide de la commande correcte pour la configuration de la gestion des clés.

Si vous utilisez…	Utilisez cette commande…
Gestion intégrée des clés	`security key-manager onboard sync` Pour plus d'informations, voir "Restauration des clés de chiffrement intégrées de gestion des clés".
Gestion externe des clés	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Vérifier que tous les ports se trouvent dans un broadcast domain :

    a. Afficher les domaines de diffusion :

       `network port broadcast-domain show`

    b. Ajoutez n'importe quel port à un broadcast domain si nécessaire.

       "Ajout ou suppression de ports d'un broadcast domain"

    c. Recréez les VLAN et les groupes d'interfaces selon les besoins.

       L'appartenance au VLAN et aux groupes d'interfaces peut être différente de celle de l'ancien nœud.

       "Création d'un VLAN"

"Combinaison de ports physiques pour créer des groupes d'interfaces"

Vérification et restauration de la configuration LIF

Vérifiez que les LIFs sont hébergées sur des nœuds et des ports appropriés, tels qu'ils sont mappés au début de la procédure de mise à niveau.

Description de la tâche

- Cette tâche est effectuée sur site_B.
- Voir le plan de mappage des ports que vous avez créé dans "Mappage des ports des anciens nœuds sur les nouveaux nœuds".

Étapes

1. Vérifiez que les LIF sont hébergées sur le nœud et les ports appropriés avant le rétablissement.

   a. Changement au niveau de privilège avancé :

      `set -privilege advanced`

   b. Remplacez la configuration des ports pour assurer un placement LIF approprié :

      `vserver config override -command "network interface modify -vserver` *`vserver_name`* `-home-port` *`active_port_after_upgrade`* `-lif` *`lif_name`* `-home-node` *`new_node_name`*`"`

   Lors de la saisie de la commande network interface modify dans le `vserver config override` vous ne pouvez pas utiliser la fonction de saisie semi-automatique de l'onglet. Vous pouvez créer le réseau `interface modify` à l'aide de la commande auto complete, puis placez-la dans le `vserver config override` commande.

   a. Retour au niveau de privilège admin :

      `set -privilege admin`

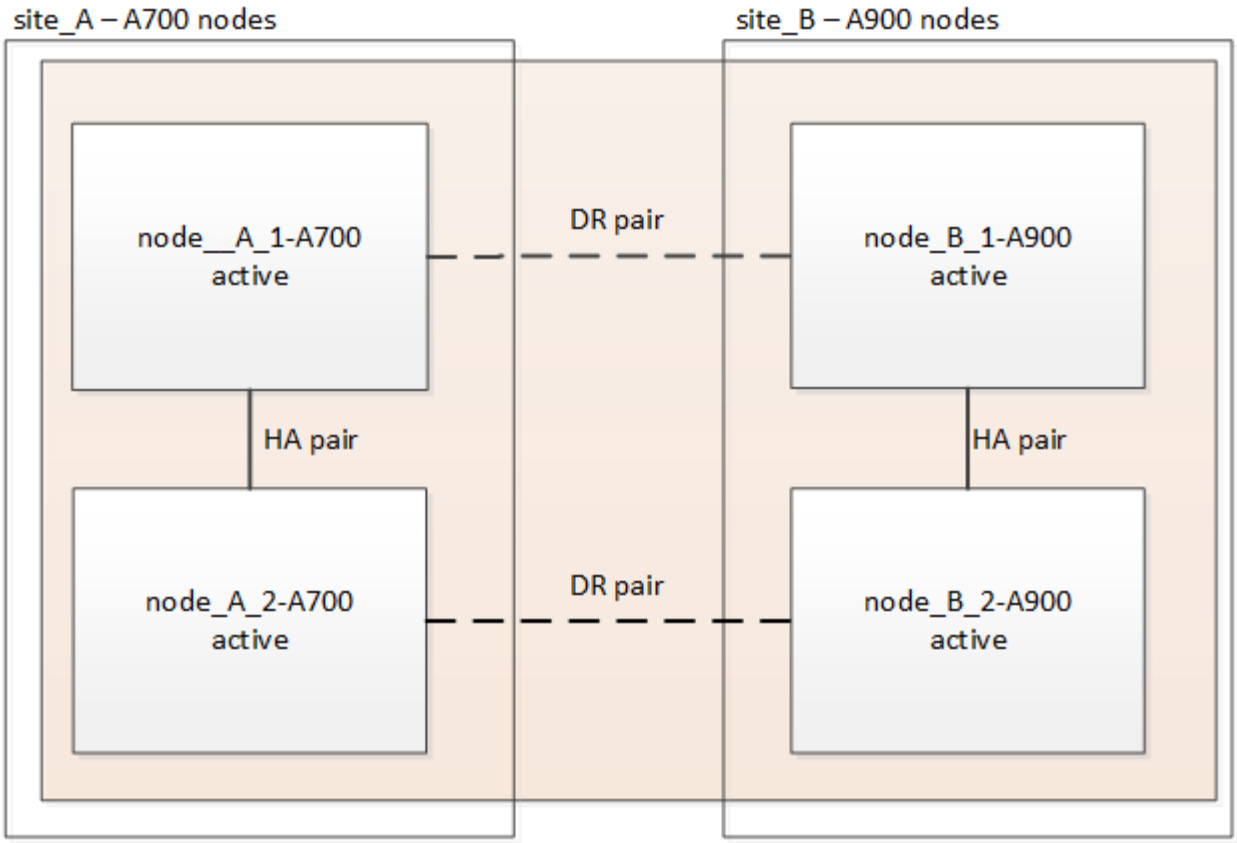
2. Revert les interfaces sur leur home node :

   `network interface revert * -vserver` *`vserver-name`*

   Suivez cette étape sur tous les SVM, si nécessaire.

Retournez la configuration MetroCluster

Cette tâche vous permet d'effectuer le rétablissement, et la configuration MetroCluster revient à un fonctionnement normal. Les nœuds du site_A sont toujours en attente de mise à niveau.



Étapes

1. Émettez le `metrocluster node show` Commande du site_B et vérifiez la sortie.
   a. Vérifiez que les nouveaux nœuds sont correctement représentés.
   b. Vérifiez que les nouveaux nœuds sont en attente de rétablissement.
2. Exécutez ce rétablissement et ce rétablissement en exécutant les commandes requises depuis n'importe quel nœud du cluster actif (cluster non mis à niveau).
   a. Réparation des agrégats de données :
   `metrocluster heal aggregates`
   b. Corriger les agrégats racine :

   ```
   metrocluster heal root
   ```

   c. Rétablissement du cluster :

   ```
   metrocluster switchback
   ```

3. Vérifier la progression de l'opération de rétablissement :

   ```
   metrocluster show
   ```

   L'opération de rétablissement est toujours en cours lorsque la sortie s'affiche `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'opération de rétablissement est terminée lorsque la sortie affiche normal :

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Si un rétablissement prend beaucoup de temps, vous pouvez vérifier l'état des lignes de base en cours en utilisant le `metrocluster config-replication resync-status show` commande. Cette commande est au niveau de privilège avancé.

Vérifier l'état de santé de la configuration MetroCluster

Après la mise à niveau des modules de contrôleur, vous devez vérifier l'état de santé de la configuration MetroCluster.

Description de la tâche

Cette tâche peut être effectuée sur n'importe quel nœud de la configuration MetroCluster.

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster :
   a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :
      `metrocluster show`
   b. Effectuer une vérification MetroCluster :
      `metrocluster check run`
   c. Afficher les résultats de la vérification MetroCluster :

      `metrocluster check show`

2. Vérifiez la connectivité et le statut de MetroCluster.

a. Vérifiez les connexions IP du MetroCluster :

```
storage iscsi-initiator show
```

b. Vérifiez que les nœuds fonctionnent :

```
metrocluster node show
```

c. Vérifier que les interfaces IP MetroCluster sont bien les suivantes :

```
metrocluster configuration-settings interface show
```

d. Vérifier que le basculement local est activé :

```
storage failover show
```

Mettre à niveau les nœuds du site_A

Vous devez répéter les tâches de mise à niveau sur site_A.

Étapes

1. Répétez les étapes pour mettre à niveau les nœuds du site_A, en commençant par "Préparation à la mise à niveau".

   Lorsque vous effectuez les tâches, toutes les références aux sites et aux nœuds sont inversées. Par exemple, si l'exemple est donné pour effectuer un basculement à partir de site_A, vous effectuez un basculement à partir de site_B.

Restaurer la surveillance du disjoncteur d'attache ou du médiateur

Après avoir effectué la mise à niveau de la configuration MetroCluster, vous pouvez reprendre la surveillance avec l'utilitaire Tiebreaker ou Mediator.

Étapes

1. Restaurer la surveillance si nécessaire, en suivant la procédure de configuration.

Si vous utilisez…	Suivre cette procédure
Disjoncteur d'attache	"Ajout des configurations MetroCluster" Dans la section *MetroCluster Tiebreaker installation and Configuration*.
Médiateur	"Configuration du service médiateur ONTAP à partir d'une configuration IP MetroCluster" Dans la section *MetroCluster IP installation and Configuration*.
Applications tierces	Reportez-vous à la documentation du produit.

Envoyez un message AutoSupport personnalisé après la maintenance

Une fois la mise à niveau terminée, envoyer un message AutoSupport indiquant la fin de la maintenance. La création automatique de dossier peut reprendre.

Étapes

1. Pour reprendre la génération automatique de dossier de support, envoyez un message AutoSupport pour indiquer que la maintenance est terminée.
   a. Lancer la commande suivante :
   `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Répétez la commande sur le cluster partenaire.

Mise à jour d'une configuration FC MetroCluster à quatre nœuds

Vous pouvez mettre à niveau les contrôleurs et le stockage dans une configuration MetroCluster à quatre nœuds en étendant la configuration pour devenir une configuration à huit nœuds et en supprimant l'ancien groupe de reprise après incident.

Description de la tâche

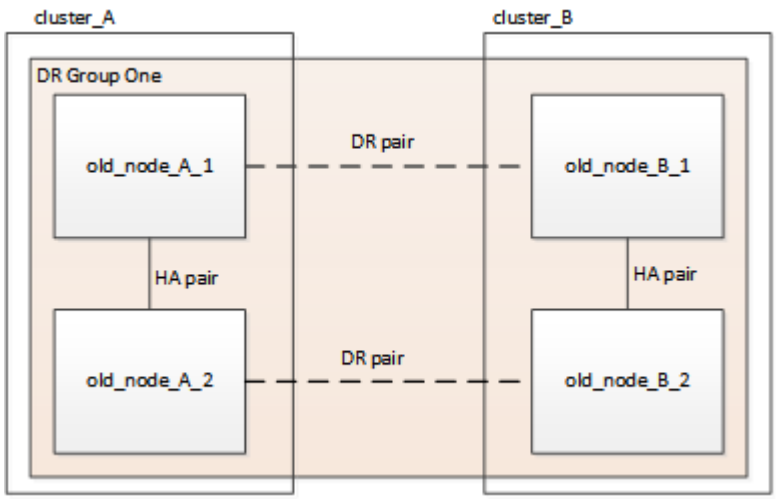
Les références aux « anciens nœuds » désignent les nœuds que vous souhaitez remplacer.

- Vous pouvez uniquement actualiser des modèles de plateforme spécifiques en suivant cette procédure dans une configuration MetroCluster FC.
  - Pour en savoir plus sur les combinaisons de mise à niveau de plateforme prises en charge, consultez le tableau de mise à jour FC MetroCluster dans "Choix d'une méthode de renouvellement du système".

Étapes

1. Collecte des informations des anciens nœuds.

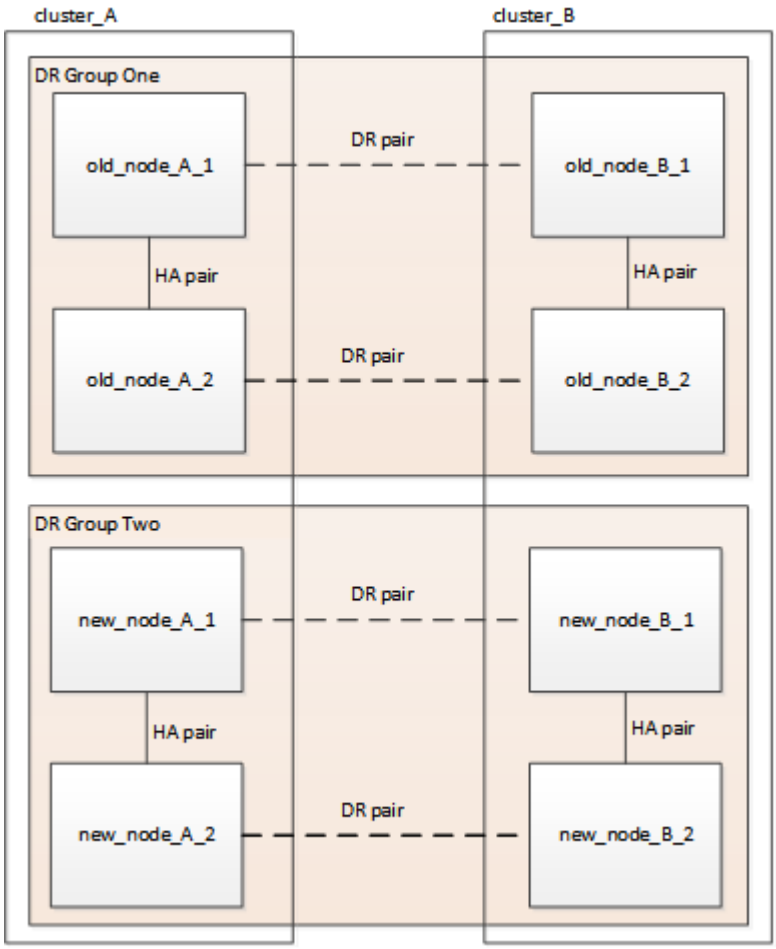
   À ce stade, la configuration à quatre nœuds apparaît comme illustré sur l'image suivante :



2. Suivez toutes les étapes de la procédure d'extension à quatre nœuds pour votre type de MetroCluster.

   "Extension d'une configuration FC MetroCluster à quatre nœuds à une configuration à huit nœuds"

Lorsque la procédure d'extension est terminée, la configuration s'affiche comme illustré dans l'image suivante :



3. Déplacez les volumes CRS.

   Suivez les étapes de la section "Déplacer un volume de métadonnées dans les configurations MetroCluster".

4. Déplacez les données des anciens nœuds vers les nouveaux nœuds en procédant comme suit :
   a. Effectuez toutes les étapes de la section "Créez un agrégat et déplacez des volumes vers les nouveaux nœuds".

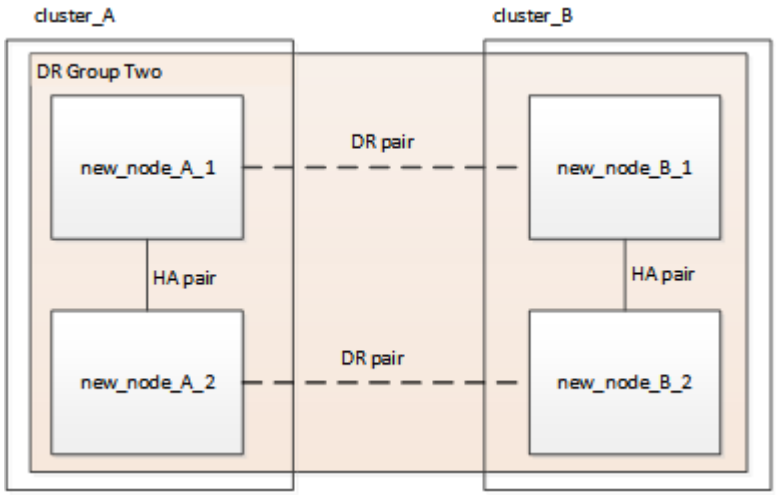
      Vous pouvez choisir de mettre en miroir l'agrégat lors de sa création ou après sa création.

   b. Effectuez toutes les étapes de la section "Déplacez les LIF de données non-SAN et les LIF de gestion du cluster vers les nouveaux nœuds".
   c. Effectuez toutes les étapes de la section "Supprimez les LIFs SAN qui ne sont plus nécessaires des nœuds d'origine".
5. Suivez les étapes de la procédure de suppression de l'ancien groupe DR.

   "Suppression d'un groupe de reprise après incident"

   Après avoir supprimé l'ancien groupe DR (groupe DR un), la configuration s'affiche comme illustré dans

l'image suivante :



Actualisation d'une configuration IP MetroCluster à quatre ou huit nœuds (ONTAP 9.8 et versions ultérieures)

Vous pouvez utiliser cette procédure pour mettre à niveau les contrôleurs et le stockage dans des configurations à quatre ou huit nœuds.

À partir de ONTAP 9.13.1, vous pouvez mettre à niveau les contrôleurs et le stockage dans une configuration IP MetroCluster à huit nœuds en développant la configuration pour devenir une configuration temporaire à douze nœuds, puis en supprimant les anciens groupes de reprise après incident.

À partir de ONTAP 9.8, vous pouvez mettre à niveau les contrôleurs et le stockage d'une configuration IP MetroCluster à quatre nœuds en développant la configuration pour devenir une configuration temporaire à huit nœuds, puis en supprimant l'ancien groupe DR.

Description de la tâche

- Si vous avez une configuration à huit nœuds, votre système doit exécuter ONTAP 9.13.1 ou une version ultérieure.
- Si vous avez une configuration à quatre nœuds, votre système doit exécuter ONTAP 9.8 ou une version ultérieure.
- Si vous mettez également à niveau les commutateurs IP, vous devez les mettre à niveau avant d'effectuer cette procédure d'actualisation.
- Cette procédure décrit les étapes requises pour actualiser un groupe DR à quatre nœuds. Si vous avez une configuration à huit nœuds (deux groupes DR), vous pouvez actualiser l'un des groupes DR, ou les deux.

  Si vous actualisez les deux groupes DR, vous devez actualiser un groupe DR à la fois.

- Les références aux « anciens nœuds » désignent les nœuds que vous souhaitez remplacer.
- Pour les configurations à huit nœuds, la combinaison de plateformes MetroCluster à huit nœuds source et cible doit être prise en charge.

Si vous actualisez les deux groupes DR, il se peut que la combinaison de plateformes ne soit pas prise en charge après l'actualisation du premier groupe DR. Vous devez actualiser les deux groupes DR pour obtenir une configuration à huit nœuds prise en charge.

- Vous ne pouvez actualiser que des modèles de plate-forme spécifiques en suivant cette procédure dans une configuration MetroCluster IP.
  - Pour plus d'informations sur les combinaisons de mise à niveau de la plate-forme prises en charge, consultez le tableau d'actualisation de l'IP MetroCluster dans "Choix d'une méthode de renouvellement du système".
- Les limites inférieures des plates-formes source et cible s'appliquent. Si vous passez à une plateforme supérieure, les limites de la nouvelle plateforme ne s'appliquent qu'à la fin de la mise à jour technologique de tous les groupes de reprise après incident.
- Si vous effectuez une mise à jour technologique sur une plateforme dont les limites sont inférieures à celles de la plateforme source, vous devez ajuster et réduire les limites à atteindre ou à une valeur inférieure aux limites de la plateforme cible avant d'effectuer cette procédure.

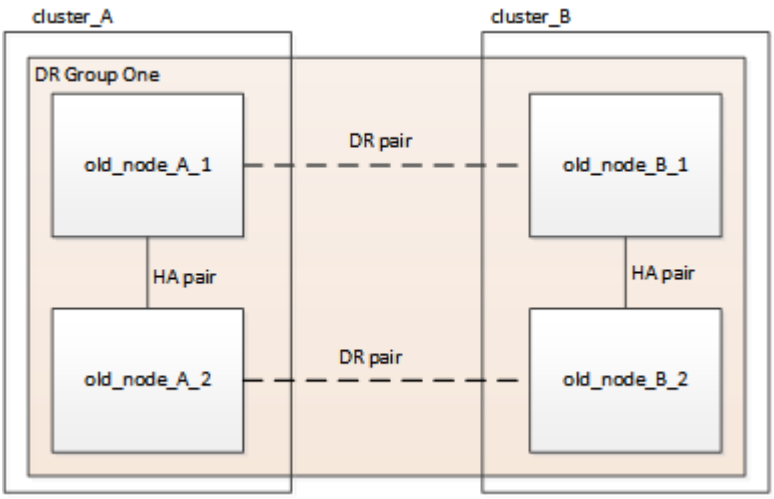
Étapes

1. Vérifiez qu'un domaine de diffusion par défaut est créé sur les anciens nœuds.

   Lorsque vous ajoutez de nouveaux nœuds à un cluster existant sans broadcast domain par défaut, les LIFs de node-management sont créées pour les nouveaux nœuds à l'aide d'UUID (Universal unique identifier) à la place des noms attendus. Pour plus d'informations, consultez l'article de la base de connaissances "Les LIF de gestion de nœuds sur les nouveaux nœuds ajoutés sont générées avec des noms UUID".

2. Collecte des informations des anciens nœuds.

   À ce stade, la configuration à quatre nœuds apparaît comme illustré sur l'image suivante :



   La configuration à huit nœuds s'affiche comme illustré dans l'image suivante :

3. Pour éviter la génération automatique de dossiers de demande de support, envoyez un message AutoSupport pour indiquer que la mise à niveau est en cours.

   a. Lancer la commande suivante :
   `system node autosupport invoke -node * -type all -message "MAINT=10h`

Upgrading *old-model* to *new-model*"

L'exemple suivant spécifie une fenêtre de maintenance de 10 heures. Selon votre plan, il est possible que vous souhaitiez accorder plus de temps.

Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Répétez la commande sur le cluster partenaire.

4. Supprimez la configuration MetroCluster existante du logiciel disjoncteur d'attache, du médiateur ou d'autres logiciels pouvant initier le basculement.

Si vous utilisez…	Utilisez cette procédure…

Disjoncteur d'attache	a. Utiliser l'interface de ligne de commande Tiebreaker `monitor remove` Commande permettant de supprimer la configuration MetroCluster.
	
	Dans l'exemple suivant, « cluster_A » est supprimé du logiciel :
	
	`NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.`
	
	b. Vérifiez que la configuration MetroCluster a été supprimée correctement à l'aide de l'interface de ligne de commande de Tiebreaker `monitor show -status` commande.
	
	`NetApp MetroCluster Tiebreaker :> monitor show -status`

Médiateur	Exécutez la commande suivante depuis l'invite ONTAP : `metrocluster configuration-settings mediator remove`
Applications tierces	Reportez-vous à la documentation du produit.

5. Effectuez toutes les étapes de la section "Développement d'une configuration IP MetroCluster" pour ajouter les nouveaux nœuds et stockage à la configuration.

   Une fois la procédure d'extension terminée, la configuration temporaire s'affiche comme illustré dans les images suivantes :

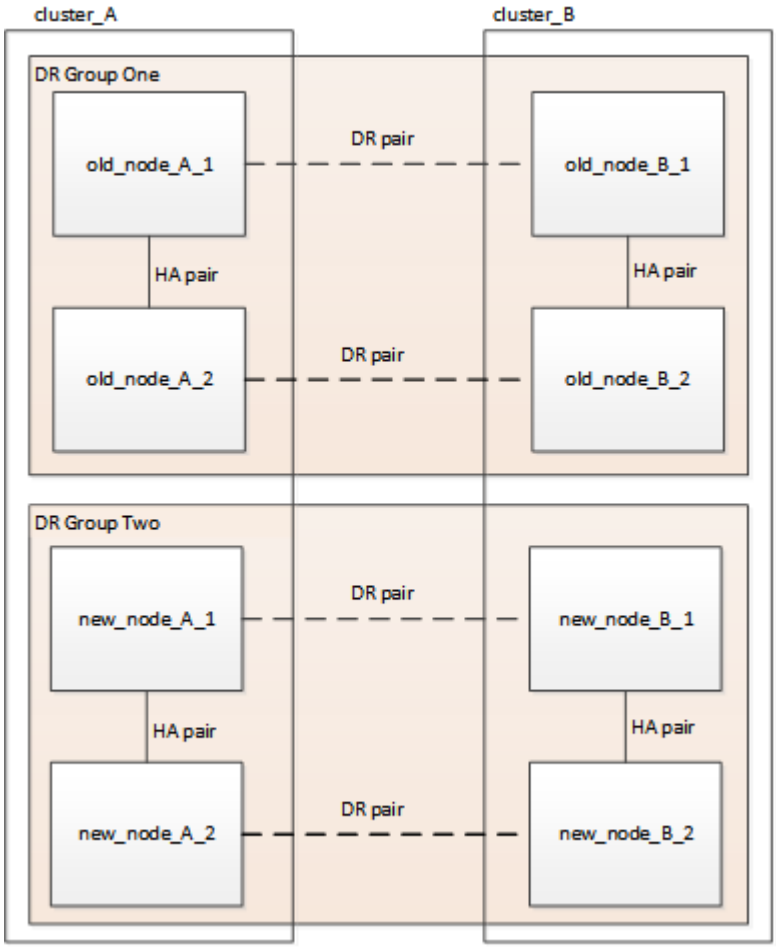


Figure 1. Configuration temporaire à huit nœuds

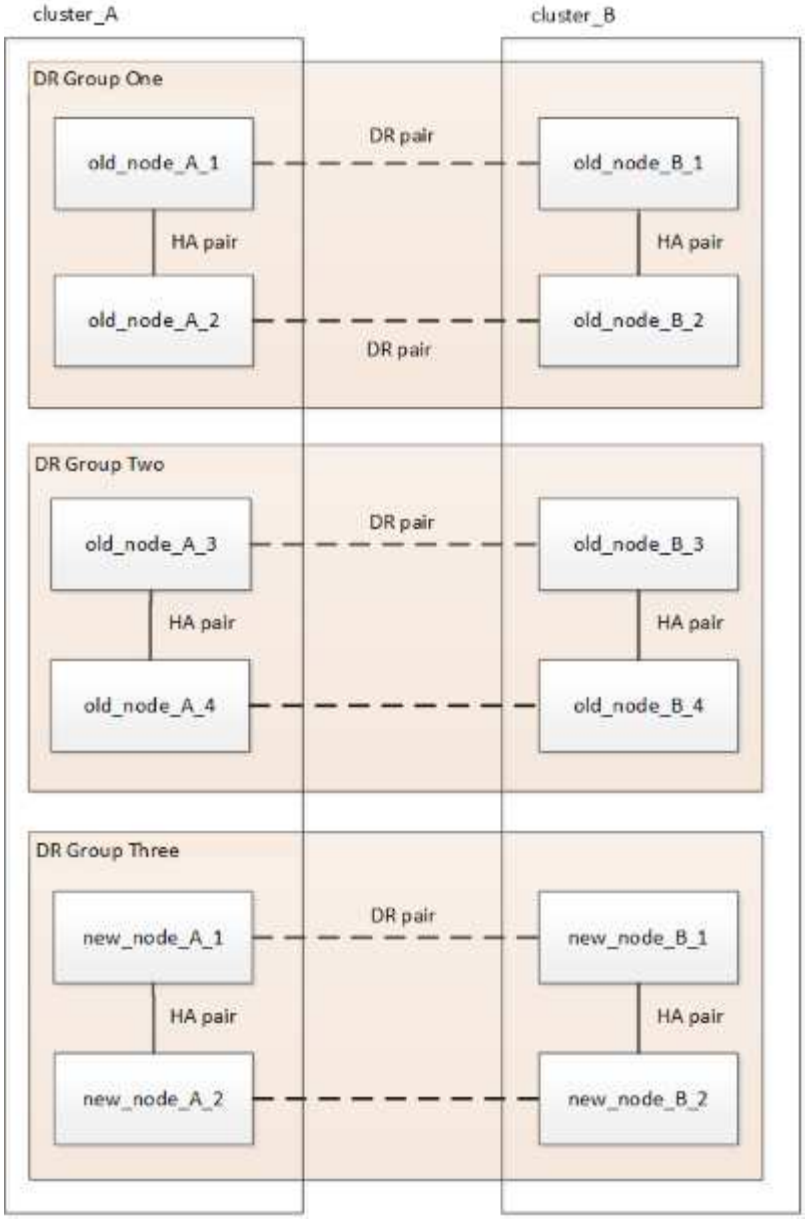


Figure 2. Configuration temporaire à douze nœuds

6. Vérifier que le basculement est possible et que les nœuds sont connectés en exécutant la commande suivante sur les deux clusters :

   `storage failover show`

```
cluster_A::> storage failover show
                                    Takeover
Node           Partner              Possible    State Description
-------------- -------------------- ---------   ------------------
Node_FC_1      Node_FC_2              true      Connected to Node_FC_2
Node_FC_2      Node_FC_1              true      Connected to Node_FC_1
Node_IP_1      Node_IP_2              true      Connected to Node_IP_2
Node_IP_2      Node_IP_1              true      Connected to Node_IP_1
```

7. Déplacez les volumes CRS.

   Suivez les étapes de la section "Déplacement d'un volume de métadonnées dans les configurations MetroCluster".

8. Déplacez les données des anciens nœuds vers les nouveaux nœuds en procédant comme suit :
   a. Effectuez toutes les étapes de la section "Création d'un agrégat et déplacement des volumes vers les nouveaux nœuds".

      Vous pouvez choisir de mettre en miroir l'agrégat lors de sa création ou après sa création.

   b. Effectuez toutes les étapes de la section "Déplacez les LIF de données non-SAN et les LIF de cluster-management vers les nouveaux nœuds".
9. Modifiez l'adresse IP de l'homologue de cluster des nœuds transférés pour chaque cluster :
   a. Identifiez l'homologue cluster_A à l'aide de `cluster peer show` commande :

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

      i. Modifiez l'adresse IP du poste cluster_A :

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

   b. Identifiez l'homologue cluster_B à l'aide de `cluster peer show` commande :

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

      i. Modifiez l'adresse IP de l'homologue cluster_B :

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

   c. Vérifiez que l'adresse IP de l'homologue de cluster est mise à jour pour chaque cluster :

      i. Vérifiez que l'adresse IP est mise à jour pour chaque cluster à l'aide de `cluster peer show`

`-instance` commande.

Le `Remote Intercluster Addresses` Dans les exemples suivants, le champ affiche l'adresse IP mise à jour.

Exemple pour cluster_A :

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_B
                     Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+ Exemple pour cluster_B.

```
cluster_B::> cluster peer show -instance

                        Peer Cluster Name: cluster_A
            Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
             IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. Suivez les étapes de la section "Suppression d'un groupe de reprise après incident" Pour supprimer l'ancien groupe DR.
11. Si vous souhaitez actualiser les deux groupes DR dans une configuration à huit nœuds, vous devez répéter la procédure complète pour chaque groupe DR.

    Après avoir supprimé l'ancien groupe DR, la configuration s'affiche comme illustré dans les images suivantes :

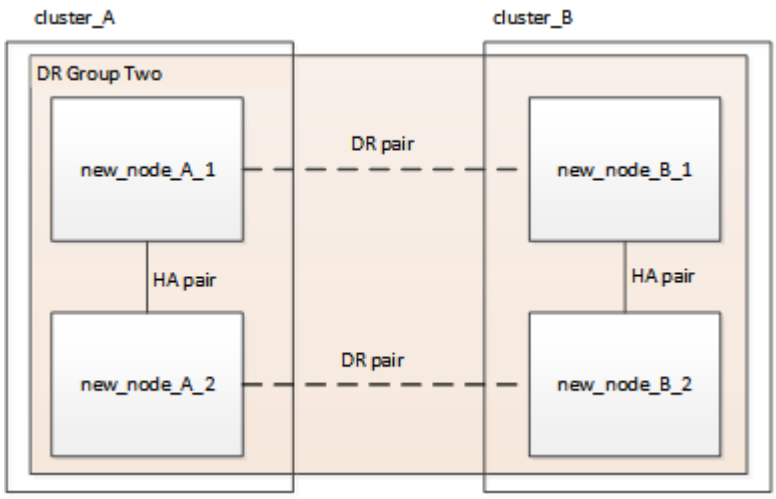


Figure 3. Configuration à quatre nœuds

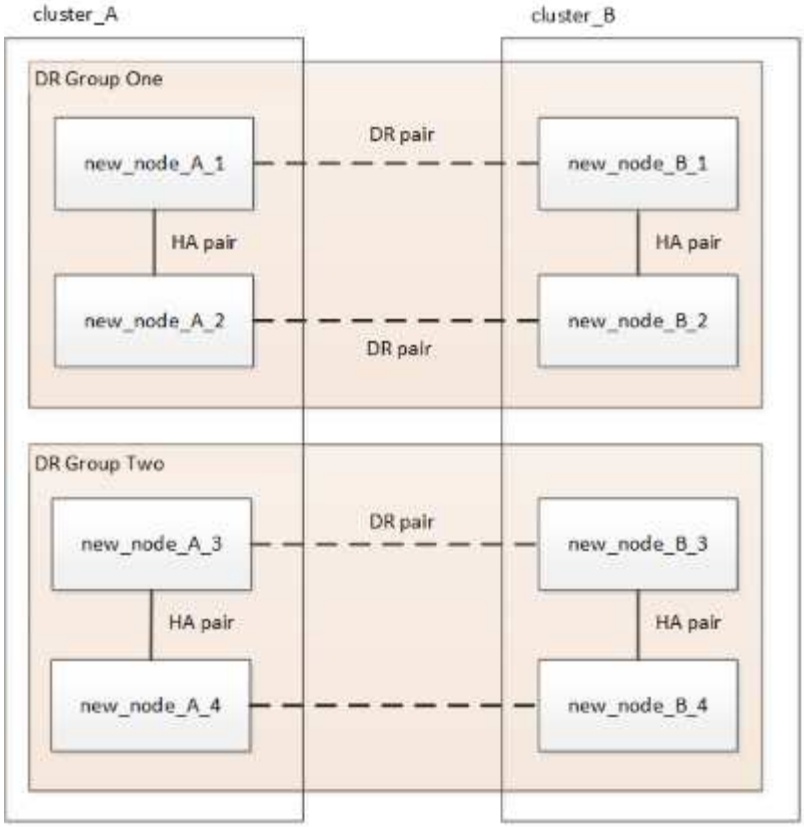


Figure 4. Configuration à huit nœuds

12. Vérifier le mode opérationnel de la configuration MetroCluster et effectuer un contrôle MetroCluster.
    a. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

       `metrocluster show`

    b. Vérifiez que tous les nœuds attendus s'affichent :

       `metrocluster node show`

    c. Exécutez la commande suivante :

       `metrocluster check run`

    d. Afficher les résultats de la vérification MetroCluster :

       `metrocluster check show`

13. Restaurer la surveillance si nécessaire, en suivant la procédure de configuration.

Si vous utilisez…	Suivre cette procédure
Disjoncteur d'attache	"Ajout des configurations MetroCluster" Dans le *MetroCluster Tiebreaker installation et configuration*.

Médiateur	"Configuration du service médiateur ONTAP à partir d'une configuration IP MetroCluster" Dans *MetroCluster IP installation and Configuration*.
Applications tierces	Reportez-vous à la documentation du produit.

14. Pour reprendre la génération automatique de dossier de support, envoyez un message AutoSupport pour indiquer que la maintenance est terminée.
    a. Exécutez la commande suivante :

    ```
    system node autosupport invoke -node * -type all -message MAINT=end
    ```

    b. Répétez la commande sur le cluster partenaire.

Étendez une configuration FC MetroCluster à deux nœuds à une configuration à quatre nœuds

Extension d'une configuration FC MetroCluster à deux nœuds à une configuration à quatre nœuds

L'extension d'une configuration FC MetroCluster à deux nœuds à une configuration FC MetroCluster à quatre nœuds implique d'ajouter un contrôleur à chaque cluster pour former une paire haute disponibilité sur chaque site MetroCluster, puis d'actualiser la configuration FC MetroCluster.

Avant de commencer

- Les nœuds doivent exécuter ONTAP 9 ou version ultérieure dans une configuration FC MetroCluster.

  Cette procédure n'est pas prise en charge sur les versions antérieures de ONTAP ou dans les configurations MetroCluster IP.

- Si les plateformes de votre configuration à deux nœuds ne sont pas prises en charge dans ONTAP 9.2 et que vous envisagez une mise à niveau vers des plateformes prises en charge dans ONTAP 9.2 *et* étendre vers un cluster à quatre nœuds, vous devez mettre à niveau les plateformes de la configuration à deux nœuds *avant* d'étendre la configuration MetroCluster FC.
- La configuration FC MetroCluster existante doit être saine.
- L'équipement que vous ajoutez doit être pris en charge et répondre à toutes les exigences décrites dans les procédures suivantes :

  "Installation et configuration de la solution Fabric-Attached MetroCluster"

  "Installation et configuration d'Stretch MetroCluster"

- Vous devez disposer de ports de commutateurs FC disponibles pour prendre en charge les nouveaux contrôleurs et les nouveaux ponts.
- Vérifiez qu'un domaine de diffusion par défaut est créé sur les anciens nœuds.

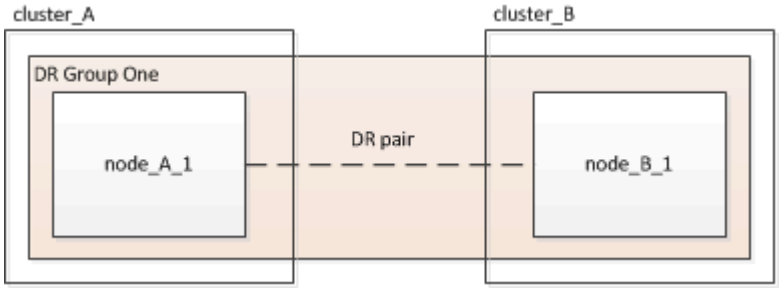
  Lorsque vous ajoutez de nouveaux nœuds à un cluster existant sans broadcast domain par défaut, les

LIFs de node-management sont créées pour les nouveaux nœuds à l'aide d'UUID (Universal unique identifier) à la place des noms attendus. Pour plus d'informations, consultez l'article de la base de connaissances "Les LIF de gestion de nœuds sur les nouveaux nœuds ajoutés sont générées avec des noms UUID".

- Vous avez besoin du mot de passe d'administration et de l'accès à un serveur FTP ou SCP.

Description de la tâche

- Cette procédure s'applique uniquement aux configurations MetroCluster FC.
- Cette procédure est perturbatrice et s'effectue en quatre heures environ.
- Avant d'effectuer cette procédure, la configuration MetroCluster FC se compose de deux clusters à un seul nœud :



À l'issue de cette procédure, la configuration MetroCluster FC se compose de deux paires HA, une sur chaque site :

- Les deux sites doivent être étendus de la même manière.

  Une configuration MetroCluster ne peut pas comprendre un nombre irrégulier de nœuds.

- Cette procédure peut prendre plus d'une heure par site, avec un temps supplémentaire pour des tâches telles que l'initialisation des disques et le démarrage réseau des nouveaux nœuds.

  Le temps nécessaire à l'initialisation des disques dépend de la taille des disques.

- Cette procédure utilise le workflow suivant :

Vérification de l'état de la configuration du MetroCluster

Vous devez identifier les contrôleurs existants et confirmer les relations de reprise sur incident entre eux, que les contrôleurs sont en mode normal et que les agrégats sont mis en miroir.

Étapes

1. Afficher le détail des nœuds dans la configuration MetroCluster depuis n'importe quel nœud de la configuration :

   ```
   metrocluster node show -fields node,dr-partner,dr-partner-systemid
   ```

   Le résultat suivant indique que cette configuration MetroCluster dispose d'un seul groupe de reprise sur incident et d'un seul nœud dans chaque cluster.

```
cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
systemid

dr-group-id  cluster         node            dr-partner      dr-partner-
systemid
-----------  -------------   -------         ----------
-------------------
1            cluster_A       controller_A_1  controller_B_1  536946192
1            cluster_B       controller_B_1  controller_A_1  536946165
2 entries were displayed.
```

2. Afficher l'état de la configuration MetroCluster :

   `metrocluster show`

   Le résultat suivant indique que les nœuds existants dans la configuration MetroCluster sont en mode normal :

```
cluster_A::> metrocluster show

Configuration: two-node-fabric

Cluster                         Entry Name             State
------------------------------ ----------------------
---------------------
Local: cluster_A               Configuration State    configured
                               Mode                   normal
                               AUSO Failure Domain    auso-on-cluster-
disaster
Remote: controller_B_1_siteB
                               Configuration State    configured
                               Mode                   normal
                               AUSO Failure Domain    auso-on-cluster-
disaster
```

3. Vérifier l'état des agrégats de chaque nœud de la configuration MetroCluster :

   `storage aggregate show`

   Le résultat suivant indique que les agrégats du cluster_A sont en ligne et en miroir :

```
cluster_A::> storage aggregate show

Aggregate                Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

Envoi d'un message AutoSupport personnalisé avant d'ajouter des nœuds à la configuration MetroCluster

Vous devez émettre un message AutoSupport pour informer le support technique de NetApp que les opérations de maintenance sont en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Connectez-vous au cluster au site_A.
2. Appelez un message AutoSupport indiquant le début de la maintenance :

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   Le `maintenance-window-in-hours` le paramètre spécifie la longueur de la fenêtre de maintenance et peut être un maximum de 72 heures. Si vous effectuez la maintenance avant que le temps ne s'soit écoulé, vous pouvez lancer la commande suivante pour indiquer que la période de maintenance a pris fin :

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Répétez cette étape sur le site du partenaire.

Segmentation des nouveaux ports de contrôleur lors de l'ajout d'un module de contrôleur dans une configuration Fabric-Attached MetroCluster

La segmentation des commutateurs FC doit s'adapter aux nouvelles connexions du contrôleur. Si vous avez utilisé les fichiers RCF (Reference Configuration File) fournis par NetApp pour configurer vos commutateurs, le zoning est préconfiguré et vous n'avez pas besoin d'apporter de modifications.

Si vous avez configuré manuellement vos commutateurs FC, vous devez vérifier que la segmentation est correcte pour les connexions initiateurs des nouveaux modules de contrôleur. Voir les sections sur la segmentation dans "Installation et configuration de la solution Fabric-Attached MetroCluster".

Ajout d'un nouveau module de contrôleur à chaque cluster

Ajout d'un nouveau module de contrôleur à chaque cluster

Vous devez ajouter un module de contrôleur à chaque site, créant ainsi une paire haute disponibilité sur chaque site. Il s'agit d'un processus en plusieurs étapes impliquant à la fois des modifications matérielles et logicielles qui doivent être effectuées dans l'ordre approprié sur chaque site.

Description de la tâche

- NetApp doit recevoir le nouveau module de contrôleur dans le cadre du kit de mise à niveau.

  Vérifiez que les cartes PCIe du nouveau module de contrôleur sont compatibles et prises en charge par le nouveau module de contrôleur.

  "NetApp Hardware Universe"

- Votre système doit disposer d'un slot vide disponible pour le nouveau module de contrôleur lors de la mise à niveau vers une paire haute disponibilité à châssis unique (paire haute disponibilité dans laquelle les deux modules de contrôleur résident sur le même châssis).

  Cette configuration n'est pas prise en charge sur tous les systèmes. Les plateformes AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx sont des plateformes avec des configurations de châssis uniques prises en charge dans ONTAP 9. FAS8020, FAS8060, FAS8080 ET FAS9000.

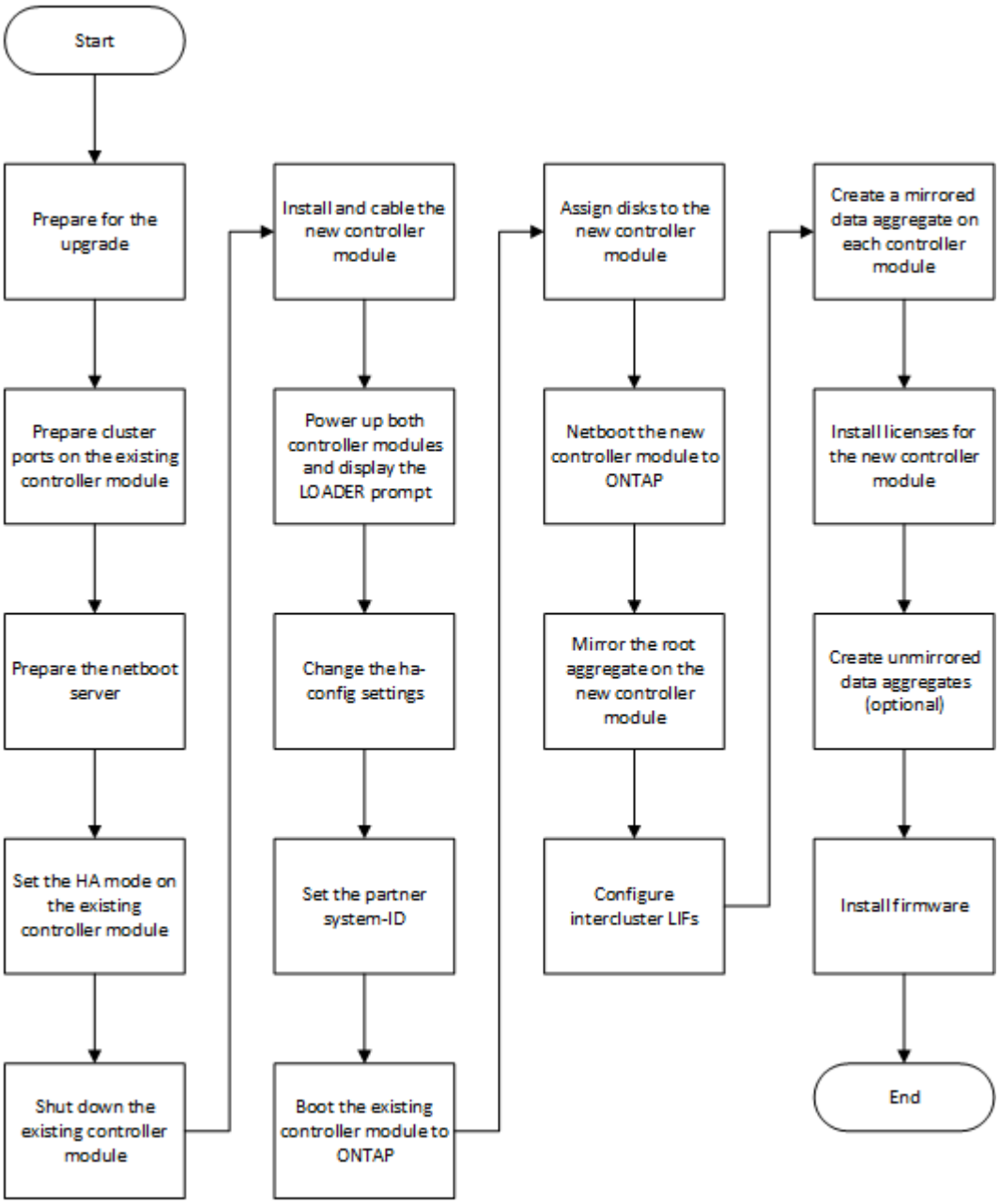
- Vous devez disposer d'espace rack et de câbles pour le nouveau module de contrôleur lors de la mise à niveau vers une paire haute disponibilité à châssis double (paire haute disponibilité dans laquelle les modules de contrôleur résident dans un châssis distinct).

  Cette configuration n'est pas prise en charge sur tous les systèmes.

- Vous devez connecter chaque module de contrôleur au réseau de gestion via son port e0a ou si le système en possède un, vous pouvez vous connecter au port e0M comme port de gestion.
- Ces tâches doivent être répétées sur chaque site.
- Les modules de contrôleur préexistants sont appelés modules de contrôleur *existing*.

  Dans les exemples de cette procédure, l'invite de console est utilisée `existing_ctlr>`.

- Les modules de contrôleur qui sont ajoutés sont appelés *New* Controller modules ; les exemples de cette procédure sont indiqués par l'invite de la console `new_ctlr>`.
- Cette tâche utilise le workflow suivant :



Préparation de la mise à niveau

Avant de procéder à la mise à niveau vers une paire haute disponibilité, vérifiez que votre système fonctionne avec toutes les exigences et que vous disposez de toutes les informations nécessaires.

Étapes

1. Identifiez les disques non assignés ou les disques de spare que vous pouvez affecter au nouveau module de contrôleur à l'aide des commandes suivantes :

   ◦ `storage disk show -container-type spare`

- `storage disk show -container-type unassigned`

2. Procédez comme suit :
   a. Déterminer l'emplacement des agrégats pour le nœud existant :

      `storage aggregate show`

   b. Si l'affectation automatique de la propriété de disque est activée, désactivez-la :

      `storage disk option modify -node node_name -autoassign off`

   c. Eliminer la propriété sur les disques qui ne disposent pas d'agrégats sur eux :

      `storage disk removeowner disk_name`

   d. Répétez l'étape précédente pour autant de disques que nécessaire pour le nouveau nœud.
3. Vérifiez que les câbles sont prêts pour les connexions suivantes :
   - Connexions du cluster

     Si vous créez un cluster sans commutateur à deux nœuds, vous avez besoin de deux câbles pour connecter les modules de contrôleur. Dans le cas contraire, vous devez disposer d'un minimum de quatre câbles, deux pour chaque connexion de module de contrôleur au commutateur cluster-network. Les autres systèmes (comme la série 80xx) disposent par défaut de quatre ou six connexions de cluster.

   - Connexions d'interconnexion HAUTE DISPONIBILITÉ, si le système se trouve dans une paire haute disponibilité à double châssis
4. Vérifiez que vous disposez d'une console de port série disponible pour les modules de contrôleur.
5. Vérifiez que votre environnement répond aux exigences du site et du système.

   "NetApp Hardware Universe"

6. Rassemblez toutes les adresses IP et tous les autres paramètres réseau du nouveau module de contrôleur.

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   `halt`

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   `set-defaults`

3. Enregistrez l'environnement :

   `saveenv`

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   `boot_ontap menu`

5. À l'invite du menu de démarrage, effacez la configuration :

   `wipeconfig`

   Répondez `yes` à l'invite de confirmation.

   Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

   Répondez `yes` à l'invite de confirmation.

Préparation des ports de cluster sur un module de contrôleur existant

Avant d'installer un nouveau module de contrôleur, vous devez configurer les ports de cluster sur le module de contrôleur existant afin que les ports de cluster puissent communiquer avec le nouveau module de contrôleur.

Description de la tâche

Si vous créez un cluster sans commutateur à 2 nœuds (sans commutateurs de réseau de cluster), vous devez activer le mode de mise en réseau sans commutateur.

Pour plus d'informations sur la configuration des ports, des LIF et du réseau dans ONTAP, reportez-vous à "Gestion de réseau".

Étapes

1. Déterminez les ports qui doivent être utilisés comme ports de cluster du nœud.

   Pour obtenir la liste des rôles de port par défaut de votre plate-forme, reportez-vous à la section "Hardware Universe"

   Le *instructions d'installation et de configuration* de votre plateforme disponible sur le site de support NetApp contient des informations sur les ports pour les connexions réseau du cluster.

2. Pour chaque port de cluster, identifier les rôles de port :

   `network port show`

   Dans l'exemple suivant, les ports « e0a », « e0b », « e0c » et « e0d » doivent être remplacés par des ports de cluster :

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. Pour toutes les LIF de données qui utilisent un port de cluster comme port home-port ou port-current, modifier la LIF de manière à utiliser un port data comme port home-port :

   `network interface modify`

   L'exemple suivant modifie le home port d'une LIF de données en un port de données :

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. Pour chaque LIF que vous avez modifiée, restaurez-la sur son nouveau port de base :

   `network interface revert`

   L'exemple suivant rétablit le LIF "datalif1" à son nouveau port d'attache ""e1b"":

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Retirez tous les ports VLAN utilisant les ports de cluster comme ports membres et ifgrps utilisant les ports de cluster comme ports membres.

   a. Supprimez les ports VLAN :
   `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

Par exemple :

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Supprimez les ports physiques des groupes d'interface :

`network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

Par exemple :

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Supprimer les ports VLAN et group d'interface de broadcast domain :

`network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname,..`*

b. Modifiez les ports du groupe d'interface pour utiliser d'autres ports physiques comme membres si nécessaire.:
`ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

6. Vérifiez que les rôles de port ont changé :

`network port show`

L'exemple suivant montre que les ports « e0a », « e0b », « e0c » et « e0d » sont désormais des ports de cluster :

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Ajouter les ports au cluster broadcast domain :

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id`*`,` *`port-id`*`,` *`port-id`*`…`

   Par exemple :

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. Si votre système fait partie d'un cluster commuté, créez des LIFs de cluster sur les ports de cluster : `network interface create`

   L'exemple suivant illustre la création d'une LIF de cluster sur l'un des ports de cluster du nœud. Le `-auto` Paramètre configure la LIF pour qu'elle utilise une adresse IP lien-local.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. Si vous créez un cluster sans commutateur à deux nœuds, activez le mode de mise en réseau sans commutateur :

   a. Passez au niveau de privilège avancé depuis l'un ou l'autre nœuds :

      `set -privilege advanced`

Vous pouvez répondre `y` lorsque vous êtes invité à indiquer si vous souhaitez continuer en mode avancé. L'invite du mode avancé s'affiche (`*>`).

a. Activer le mode de mise en réseau sans commutateur en cluster :

```
network options switchless-cluster modify -enabled true
```

b. Retour au niveau de privilège admin :

```
set -privilege admin
```

> La création d'interface de cluster pour le nœud existant dans un système en cluster sans commutateur à 2 nœuds est terminée une fois la configuration du cluster terminée via un démarrage sur le réseau sur le nouveau module de contrôleur.

Préparation du serveur netboot pour télécharger l'image

Lorsque vous êtes prêt à préparer le serveur netboot, vous devez télécharger l'image exacte du réseau ONTAP depuis le site de support NetApp vers le serveur netboot et noter l'adresse IP.

Description de la tâche

- Vous devez pouvoir accéder à un serveur HTTP à partir du système avant et après avoir ajouté le nouveau module de contrôleur.
- Vous devez avoir accès au site de support NetApp pour télécharger les fichiers système nécessaires pour votre plateforme et votre version de ONTAP.

  "Site de support NetApp"

- Les deux modules de contrôleur de la paire HA doivent exécuter la même version de ONTAP.

Étapes

1. Téléchargez le logiciel ONTAP approprié depuis la section de téléchargement des logiciels du site de support NetApp et stockez le `<ontap_version>_image.tgz` fichier dans un répertoire accessible sur le web.

   Le `<ontap_version>_image.tgz` fichier est utilisé pour effectuer un démarrage sur le réseau de votre système.

2. Accédez au répertoire accessible sur le Web et vérifiez que les fichiers dont vous avez besoin sont disponibles.

Pour…	Alors…

GAMMES FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	Extrayez le contenu du fichier ontap_version_image.tgz dans le répertoire cible :
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Si vous extrayez le contenu sous Windows, utilisez 7-Zip ou WinRAR pour extraire l'image netboot.
	
	Votre liste de répertoires doit contenir un dossier netboot avec un fichier du noyau :
	
	`netboot/kernel`

Tous les autres systèmes	Votre liste de répertoires doit contenir le fichier suivant : `<ontap_version>_image.tgz` Il n'est pas nécessaire d'extraire le contenu du fichier.

3. Déterminez l'adresse IP du module de contrôleur existant.

   Cette adresse est appelée plus loin dans cette procédure *`ip-address-of-existing controller`*.

4. Ping *`ip-address-of-existing controller`* Pour vérifier que l'adresse IP est accessible.

Configuration du mode HA sur le module de contrôleur existant

Vous devez utiliser la commande Storage failover modify pour définir le mode sur le module de contrôleur existant. La valeur du mode est activée ultérieurement, après le redémarrage du module de contrôleur.

Étapes

1. Définissez le mode sur HA :

   `storage failover modify -mode ha -node existing_node_name`

Arrêt du module de contrôleur existant

Vous devez effectuer un arrêt correct du module de contrôleur existant pour vérifier que toutes les données ont été écrites sur le disque. Vous devez également débrancher les alimentations.

Description de la tâche

Vous devez effectuer un arrêt correct du système avant de remplacer les composants du système pour éviter de perdre des données non écrites dans la mémoire NVRAM ou la mémoire NVMEM.

Étapes

1. Arrêtez le nœud depuis l'invite du module de contrôleur existant :

   ```
   halt local -inhibit-takeover true
   ```

   Si vous êtes invité à continuer la procédure d'arrêt, entrez `y` Lorsque vous y êtes invité, puis attendez que le système s'arrête à l'invite DU CHARGEUR.

   Dans un système 80xx, le voyant NVRAM se trouve sur le module de contrôleur à droite des ports réseau, marqué d'un symbole de batterie.

   Cette LED clignote si des données non écrites sont présentes dans la mémoire NVRAM. Si ce voyant clignote en orange après avoir entré la commande halt, vous devez redémarrer votre système et essayer de l'arrêter à nouveau.

2. Si vous n'êtes pas déjà mis à la terre, mettez-vous à la terre correctement.
3. Mettez les blocs d'alimentation hors tension et débranchez-les, en utilisant la méthode appropriée pour votre système et le type d'alimentation :

Si votre système utilise…	Alors…
Blocs d'alimentation CA	Débranchez les câbles d'alimentation de la source d'alimentation, puis retirez les câbles d'alimentation.
Alimentations CC	Débranchez l'alimentation de la source CC, puis retirez les fils CC, si nécessaire.

Installez et câconnectez le nouveau module de contrôleur

Installation et câblage du nouveau module de contrôleur

Vous devez installer physiquement le nouveau module de contrôleur dans le châssis, puis le brancher.

Étapes

1. Si votre système est équipé d'un module d'extension d'E/S (IOXM) et que vous créez une paire haute disponibilité avec châssis unique, vous devez déconnecter et retirer le module IOXM.

   Vous pouvez ensuite utiliser la baie vide pour le nouveau module de contrôleur. Toutefois, la nouvelle configuration ne sera pas équipée des E/S supplémentaires fournies par le module IOXM.

2. Installez physiquement le nouveau module de contrôleur et, si nécessaire, installez des ventilateurs supplémentaires :

Si vous ajoutez un module de contrôleur…	Ensuite, procédez comme suit…

Sur une baie vide pour créer une paire haute disponibilité à châssis unique et le système appartient à l'une des plates-formes suivantes :	a. Retirez la plaque vierge située à l'arrière du châssis, qui recouvre la baie vide contenant le nouveau module de contrôleur. b. Poussez doucement le module de contrôleur à mi-chemin dans le châssis. Pour éviter que le module de contrôleur ne démarre automatiquement, ne le asseyez pas complètement dans le châssis avant que cette procédure ne soit effectuée plus tard.
Dans un châssis distinct de son partenaire haute disponibilité, pour créer une paire haute disponibilité à double châssis lorsque la configuration existante se trouve dans une configuration de module contrôleur-IOX. • FAS8200 • 80xx	Installez le nouveau système sur le rack ou l'armoire système.

3. Câconnectez les connexions du réseau du cluster, si nécessaire :

   a. Identifier les ports du module de contrôleur pour les connexions du cluster

      "Systèmes AFF A320 : installation et configuration"

      "Instructions d'installation et de configuration des systèmes AFF A220/FAS2700"

      "Instructions d'installation et de configuration des systèmes AFF A800"

      "Instructions d'installation et de configuration des systèmes AFF A300"

      "Instructions d'installation et de configuration du système FAS8200"

   b. Si vous configurez un cluster commuté, identifiez les ports que vous utiliserez sur les commutateurs du réseau de cluster.

      Voir la "Guide de configuration des commutateurs clustered Data ONTAP pour les commutateurs Cisco", "^NetApp 10G - Guide d'installation du commutateur Cluster-mode" ou "Guide d'installation du commutateur NetApp 1G Cluster-mode", selon les commutateurs que vous utilisez.

   c. Connectez les câbles aux ports du cluster :

Si le cluster est…	Alors…
Un cluster à 2 nœuds sans commutateur	Connectez directement les ports de cluster sur le module de contrôleur existant aux ports de cluster correspondants sur le nouveau module de contrôleur.

Un cluster commuté	Connectez les ports de cluster de chaque contrôleur aux ports des commutateurs de réseau de cluster identifiés à la sous-étape b.

Câblage des nouveaux ports FC-VI et HBA du module de contrôleur aux commutateurs FC

Les ports FC-VI et HBA (adaptateurs de bus hôte) du nouveau module de contrôleur doivent être câblés aux commutateurs FC du site.

Étapes

1. Reliez les ports FC-VI et les ports HBA à l'aide du tableau correspondant à votre configuration et à votre modèle de commutateur.
   - "Affectation de ports pour les commutateurs FC lors de l'utilisation de ONTAP 9.1 et versions ultérieures"
   - "Affectation des ports pour les commutateurs FC lors de l'utilisation de ONTAP 9.0"
   - "Affectation de ports pour les systèmes utilisant deux ports d'initiateur"

Câblage des nouvelles connexions de peering de cluster du module de contrôleur

Vous devez raccorder le nouveau module de contrôleur au réseau de peering de cluster afin que celui-ci soit connecté au cluster sur le site partenaire.

Description de la tâche

Au moins deux ports sur chaque module de contrôleur doivent être utilisés pour le peering de cluster.

La bande passante minimale recommandée pour les ports et la connectivité réseau est de 1 GbE.

Étapes

1. Identifier et câbler au moins deux ports pour peering de cluster et vérifier qu'ils disposent d'une connectivité réseau avec le cluster partenaire.

Mise sous tension des deux modules de contrôleur et affichage de l'invite DU CHARGEUR

Vous mettez le module de contrôleur existant sous tension et le nouveau module de contrôleur pour afficher l'invite DU CHARGEUR.

Étapes

Mettez les modules de contrôleur sous tension et interrompez le processus de démarrage en suivant les étapes de votre configuration :

Si les modules de contrôleur sont…	Alors…

Dans le même châssis	1. Vérifiez que le nouveau module de contrôleur est entièrement inséré dans la baie. Le module de contrôleur existant doit être complètement inséré dans la baie, car il n'a jamais été retiré du châssis, mais le nouveau module de contrôleur ne doit pas être. 2. Branchez l'alimentation et mettez les blocs d'alimentation sous tension afin que le module de contrôleur existant soit alimenté. 3. Interrompez le processus de démarrage du module de contrôleur existant en appuyant sur Ctrl-C. 4. Poussez fermement le nouveau module de contrôleur dans la baie. Lorsqu'il est bien en place, le nouveau module de contrôleur reçoit l'alimentation et démarre automatiquement. 5. Interrompez le processus de démarrage en appuyant sur Ctrl-C. 6. Serrez la vis moletée sur la poignée de came, le cas échéant. 7. Installez le dispositif de gestion des câbles, le cas échéant. 8. Fixez les câbles au dispositif de gestion des câbles à l'aide du crochet et de la sangle de boucle.
Dans un châssis séparé	1. Allumer les alimentations sur le module de contrôleur existant. 2. Interrompez le processus de démarrage en appuyant sur Ctrl-C. 3. Répétez ces étapes pour le nouveau module de contrôleur

Chaque module de contrôleur doit afficher l'invite DU CHARGEUR (`LOADER>`, `LOADER-A>`, ou `LOADER-B>`).

S'il n'y a pas d'invite DU CHARGEUR, enregistrez le message d'erreur. Si le système affiche le menu de démarrage, redémarrez et essayez à nouveau d'interrompre le processus de démarrage.

Modification du paramètre HA-config sur les modules de contrôleur existants et nouveaux

Lorsque vous développez une configuration MetroCluster, vous devez mettre à jour le paramètre ha-config du module de contrôleur existant et du nouveau module de contrôleur. Vous devez également déterminer l'ID système du nouveau module de contrôleur.

Description de la tâche

Cette tâche est effectuée en mode Maintenance sur les modules de contrôleur existants et nouveaux.

Étapes

1. Modifiez le paramètre ha-config du module de contrôleur existant :

   a. Afficher le paramètre ha-config du module de contrôleur et du châssis existants :

      ```
      ha-config show
      ```

Le paramètre ha-config est "mcc-2n" pour tous les composants car le module de contrôleur était dans une configuration MetroCluster à deux nœuds.

b. Remplacez le paramètre ha-config du module de contrôleur existant par “mcc”:
`ha-config modify controller mcc`

c. Remplacez le paramètre ha-config du châssis existant par `mcc`:

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

d. Récupérer l’ID système du module de contrôleur existant :

```
sysconfig
```

Notez l’ID du système. Vous en avez besoin lorsque vous définissez l’ID de partenaire sur le nouveau module de contrôleur.

a. Quitter le mode Maintenance pour revenir à l’invite DU CHARGEUR :

```
halt
```

2. Modifiez le paramètre ha-config et récupérez l’ID système du nouveau module de contrôleur :

a. Si le nouveau module de contrôleur n’est pas déjà en mode de maintenance, démarrez-le en mode maintenance :

```
boot_ontap maint
```

b. Remplacez le paramètre ha-config du nouveau module de contrôleur par `mcc`:

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

c. Définissez le paramètre ha-config du nouveau châssis sur mcc :

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

d. Récupérer l’ID système du nouveau module de contrôleur :

```
sysconfig
```

Notez l’ID du système. Lorsque vous définissez l’ID de partenaire et affectez des disques au nouveau module de contrôleur,

a. Quitter le mode Maintenance pour revenir à l’invite DU CHARGEUR :

```
halt
```

Définition de l’ID système partenaire pour les deux modules de contrôleur

Vous devez définir l’ID du système partenaire sur les deux modules de contrôleur afin qu’ils puissent former une paire haute disponibilité.

Description de la tâche

Cette tâche s'effectue avec les deux modules de contrôleur à l'invite DU CHARGEUR.

Étapes

1. Définissez l'ID système partenaire sur celui du module de contrôleur existant :

   `setenv partner-sysid sysID_of_new_controller`

2. Définissez l'ID système partenaire sur celui du module de contrôleur existant :

   `setenv partner-sysid sysID_of_existing_controller`

Démarrage du module de contrôleur existant

Vous devez démarrer le module de contrôleur existant sur ONTAP.

Étapes

1. À l'invite DU CHARGEUR, démarrez le module de contrôleur existant sur ONTAP :

   `boot_ontap`

Assignation des disques au nouveau module de contrôleur

Avant de terminer la configuration du nouveau module de contrôleur via netboot, vous devez affecter les disques.

Description de la tâche

Vous devez avoir l'assurance que suffisamment de pièces de rechange, de disques non assignés ou de disques affectés ne faisant pas partie d'un agrégat existant.

"Préparation de la mise à niveau"

Ces étapes sont effectuées sur le module de contrôleur existant.

Étapes

1. Assigner le disque racine au nouveau module de contrôleur :

   `storage disk assign -disk disk_name -sysid new_controller_sysID -force true`

   Si votre modèle de plateforme utilise la fonction de partitionnement de disque avancé, vous devez inclure le paramètre -root true :

   `storage disk assign -disk disk_name -root true -sysid new_controller_sysID -force true`

2. Assigner les disques restants nécessaires au nouveau module de contrôleur en entrant la commande suivante pour chaque disque :

   `storage disk assign -disk disk_name -sysid new_controller_sysID -force true`

3. Vérifiez que les affectations de disques sont correctes :

   `storage disk show -partitionownership*`

Assurez-vous d'avoir affecté tous les disques que vous souhaitez affecter au nouveau nœud.

Démarrage réseau et configuration de ONTAP sur le nouveau module de contrôleur

Vous devez effectuer une séquence d'étapes spécifiques vers netboot et installer le système d'exploitation ONTAP sur le nouveau module de contrôleur lors de l'ajout de modules de contrôleur à une configuration MetroCluster existante.

Description de la tâche

- Cette tâche démarre à l'invite DU CHARGEUR du nouveau module de contrôleur.
- Cette tâche comprend l'initialisation des disques.

  Le temps nécessaire pour initialiser les disques dépend de la taille des disques.

- Le système attribue automatiquement deux disques au nouveau module de contrôleur.

  "Gestion des disques et des agrégats"

Étapes

1. À l'invite DU CHARGEUR, configurez l'adresse IP du nouveau module de contrôleur en fonction de la disponibilité DHCP :

Si DHCP est…	Entrez ensuite la commande suivante…
Disponibilité	**`ifconfig e0M -auto`**
Non disponible	`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. *`netmask`* est le masque de réseau du système de stockage. *`gateway`* est la passerelle du système de stockage. *`dns_addr`* Est l'adresse IP d'un serveur de noms sur votre réseau. *`dns_domain`* Est le nom de domaine DNS (Domain Name System). Si vous utilisez ce paramètre facultatif, vous n'avez pas besoin d'un nom de domaine complet dans l'URL du serveur netboot ; vous n'avez besoin que du nom d'hôte du serveur. D'autres paramètres peuvent être nécessaires pour votre interface. Pour plus de détails, utilisez le `help ifconfig` Commande à l'invite DU CHARGEUR.

2. À l'invite DU CHARGEUR, netboot le nouveau nœud :

Pour…	Exécutez cette commande…
GAMMES FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Tous les autres systèmes	`netboot http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

Le *path_to_the_web-accessible_directory* est l'emplacement du téléchargé `<ontap_version>_image.tgz` fichier.

3. Sélectionnez l'option **installer le nouveau logiciel en premier** dans le menu affiché.

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

   - Vous devez entrer « y » lorsque vous y êtes invité, indiquant que cette procédure n'est pas prise en charge pour la mise à niveau sans interruption sur une paire haute disponibilité.
   - Vous devez entrer « y » lorsque vous êtes averti que ce processus remplace le logiciel ONTAP existant par un nouveau logiciel.
   - Vous devez entrer le chemin comme suit lorsque vous êtes invité à saisir l'URL du fichier image.tgz :

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Entrez « y » lorsque vous y êtes invité concernant la mise à niveau ou le remplacement du logiciel sans interruption.
5. Entrez le chemin d'accès au fichier image.tgz lorsque vous êtes invité à saisir l'URL du package.

   ```
   What is the URL for the package? `http://path_to_web-accessible_directory/image.tgz`
   ```

6. Entrez « n » pour ignorer la récupération de sauvegarde lorsque vous êtes invité à restaurer la configuration de sauvegarde.

```
*************************************************************
*             Restore Backup Configuration                  *
*  This procedure only applies to storage controllers that  *
*  are configured as an HA pair.                            *
*                                                           *
*  Choose Yes to restore the "varfs" backup configuration   *
*  from the SSH server.  Refer to the Boot Device Replacement *
*  guide for more details.                                  *
*  Choose No to skip the backup recovery and return to the  *
*  boot menu.                                               *
*************************************************************

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

7. Entrez « y » lorsque vous êtes invité à redémarrer maintenant.

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

8. Si nécessaire, sélectionnez l'option **Clean configuration et initialisez tous les disques** après le démarrage du nœud.

   Étant donné que vous configurez un nouveau module de contrôleur et que les disques du nouveau module de contrôleur sont vides, vous pouvez répondre « y » lorsque le système vous avertit que cela effacera tous les disques.

   > ⓘ Le temps nécessaire pour initialiser les disques dépend de la taille de vos disques et de votre configuration.

9. Une fois les disques initialisés et que l'assistant de configuration du cluster démarre, configurez le nœud :

   Entrez les informations LIF de node management sur la console.

10. Connectez-vous au nœud, puis entrez le `cluster setup` puis entrez « rejoindre » lorsque vous êtes invité à rejoindre le cluster.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. Répondez aux invites restantes si nécessaire pour votre site.

    Le "Configuration ONTAP" Vous trouverez des informations supplémentaires sur votre version de ONTAP.

12. Si le système se trouve dans une configuration en cluster sans commutateur à deux nœuds, créez les

interfaces de cluster sur le nœud existant à l'aide de la commande network interface create pour créer des LIFs de cluster sur les ports du cluster.

Voici un exemple de commande permettant de créer une LIF de cluster sur un des ports de cluster du nœud. Le paramètre -auto configure la LIF pour qu'elle utilise une adresse IP lien-local.

```
cluster_A::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node_A_1 -home-port e1a -auto true
```

13. Une fois l'installation terminée, vérifiez que le nœud fonctionne correctement et qu'il peut participer au cluster :

    `cluster show`

    L'exemple suivant montre un cluster après la connexion du second nœud (cluster1-02) :

    ```
    cluster_A::> cluster show
    Node                  Health  Eligibility
    --------------------- ------- ------------
    node_A_1              true    true
    node_A_2              true    true
    ```

    Pour modifier les valeurs saisies dans l'assistant Cluster Setup de la machine virtuelle de stockage (SVM) ou d'un SVM nœud, utilisez la commande cluster setup.

14. Vérifiez que quatre ports sont configurés en tant qu'interconnexions de cluster :

    `network port show`

    L'exemple suivant montre les valeurs de sortie de deux modules de contrôleur dans cluster_A :

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

Mettre en miroir l’agrégat racine sur le nouveau contrôleur

Vous devez mettre en miroir l’agrégat racine pour garantir la protection des données lorsque vous ajoutez un contrôleur à une configuration MetroCluster.

Cette tâche doit être effectuée sur le nouveau module de contrôleur.

1. Mettre en miroir l’agrégat racine :

   `storage aggregate mirror` *`aggr_name`*

   La commande suivante met en miroir l’agrégat root pour Controller_A_1 :

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Cela met en miroir l’agrégat, il se compose d’un plex local et d’un plex distant situé sur le site MetroCluster distant.

Configurer les LIFs intercluster

Configuration des LIFs intercluster sur des ports dédiés

Vous pouvez configurer les LIFs intercluster sur des ports dédiés. Cela augmente généralement la bande passante disponible pour le trafic de réplication.

Étapes

1. Lister les ports dans le cluster :

   ```
   network port show
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau en cluster01 :

   ```
   cluster01::> network port show
                                                                   Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Déterminer les ports disponibles pour dédier aux communications intercluster :

   ```
   network interface show -fields home-port,curr-port
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre que les ports « e0e » et « e0f » n'ont pas été affectés aux LIF :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Créer un failover group pour les ports dédiés :

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   L'exemple suivant attribue les ports « e0e » et « e0f » au groupe de basculement « intercluster01 » sur le SVM système « cluster01 » :

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

   `network interface failover-groups show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

Version ONTAP	Commande
9.6 et versions ultérieures	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 et versions antérieures	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » dans le groupe de basculement « intercluster01 » :

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Vérifier que les LIFs intercluster ont été créés :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vérifier que les LIFs intercluster sont redondants :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster -failover`

Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre que les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » sur le port SVM « e0e » basculeront vers le port « e0f ».

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configuration des LIFs intercluster sur des ports data partagés

Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau en cluster01 :

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Création des LIFs intercluster sur le SVM système :

Dans ONTAP 9.6 et plus tard:
`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask`
Dans ONTAP 9.5 et versions antérieures:
`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Vérifier que les LIFs intercluster ont été créés :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vérifier que les LIFs intercluster sont redondants :

Dans ONTAP 9.6 et plus tard:
`network interface show –service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre que les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » sur le port « e0c » basculeront vers le port « e0d ».

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Crée un agrégat de données en miroir sur chaque nœud

Vous devez créer un agrégat de données en miroir sur chaque nœud du groupe de reprise sur incident.

Description de la tâche

- Vous devez savoir quels disques seront utilisés dans le nouvel agrégat.
- Si votre système compte plusieurs types de disques (stockage hétérogène), vous devez comprendre comment vous assurer que le type de disque approprié est sélectionné.
- Les disques sont détenus par un nœud spécifique ; lorsque vous créez un agrégat, tous les disques de cet agrégat doivent être détenus par le même nœud, qui devient le nœud de rattachement de cet agrégat.

  Dans les systèmes utilisant ADP, des agrégats sont créés à l'aide de partitions dans lesquelles chaque disque est partitionné en partitions P1, P2 et P3.

- Les noms d'agrégats doivent être conformes au schéma de nommage que vous avez déterminé lors de la planification de votre configuration MetroCluster.

  "Gestion des disques et des agrégats"

> Pour optimiser les performances et la disponibilité du stockage, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces meilleures pratiques peut avoir un impact négatif sur les performances.

Étapes

1. Afficher la liste des pièces de rechange disponibles :

   `storage disk show -spare -owner` *`node_name`*

2. Créer l'agrégat :

   `storage aggregate create -mirror true`

   Si vous êtes connecté au cluster depuis l'interface de gestion du cluster, vous pouvez créer un agrégat sur n'importe quel nœud du cluster. Pour s'assurer que l'agrégat est créé sur un nœud spécifique, utilisez le `-node` paramètre ou spécifiez les disques qui sont détenus par ce nœud.

   Vous pouvez spécifier les options suivantes :

   - Nœud de rattachement de l'agrégat (c'est-à-dire le nœud qui détient l'agrégat en fonctionnement normal)
   - Liste de disques spécifiques à ajouter à l'agrégat
   - Nombre de disques à inclure

     Dans la configuration minimale prise en charge, dans laquelle un nombre limité de disques sont disponibles, vous devez utiliser l'option force-petits agrégats pour créer un agrégat RAID-DP à trois disques.

   - Style de checksum à utiliser pour l'agrégat
   - Type de disques à utiliser
   - Taille des disques à utiliser
   - Vitesse de conduite à utiliser
   - Type RAID des groupes RAID sur l'agrégat
   - Nombre maximal de disques pouvant être inclus dans un groupe RAID
   - Indique si les disques à régime différent sont autorisés

     Pour plus d'informations sur ces options, reportez-vous au `storage aggregate create` page de manuel.

     La commande suivante crée un agrégat en miroir avec 10 disques :

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Vérifier le groupe RAID et les disques de votre nouvel agrégat :

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Installation des licences pour le nouveau module de contrôleur

Vous devez ajouter des licences pour le nouveau module de contrôleur pour tous les services ONTAP nécessitant des licences standard (verrouillées par des nœuds). Pour les fonctionnalités avec licences standard, chaque nœud du cluster doit disposer de sa

propre clé pour cette fonctionnalité.

Pour plus d'informations sur les licences, consultez l'article de la base de connaissances 3013749 : présentation des licences et références Data ONTAP 8.2 sur le site de support NetApp et *System Administration Reference*.

Étapes

1. Si nécessaire, procurez-vous les clés de licence pour le nouveau nœud sur le site de support NetApp dans la section My support (mon support) de la section My support (licences logicielles).

   Pour plus d'informations sur les remplacements de licences, consultez l'article de la base de connaissances "Processus de remplacement post-carte mère pour la mise à jour des licences sur un système AFF/FAS."

2. Exécutez la commande suivante pour installer chaque clé de licence :

   `system license add -license-code` *`license_key`*

   Le *`license_key`* a 28 chiffres.

3. Répétez cette étape pour chaque licence standard (verrouillée par nœud) requise.

Création d'agrégats de données sans mise en miroir

Vous pouvez choisir de créer des agrégats de données non mis en miroir pour des données ne nécessitant pas la mise en miroir redondante fournie par les configurations MetroCluster.

Description de la tâche

- Vous devez savoir quels disques ou LUN de baie seront utilisés dans le nouvel agrégat.
- Si votre système compte plusieurs types de disques (stockage hétérogène), vous devez comprendre comment vous pouvez vérifier que le type de disque approprié est sélectionné.

> Dans les configurations MetroCluster IP, les agrégats distants sans mise en miroir ne sont pas accessibles après un basculement

> Les agrégats non mis en miroir doivent être locaux au nœud qu'ils possèdent.

- Les disques et les LUN de baie sont détenus par un nœud spécifique. Lorsque vous créez un agrégat, tous les disques de cet agrégat doivent être détenus par le même nœud, qui devient le nœud de rattachement de cet agrégat.
- Les noms d'agrégats doivent être conformes au schéma de nommage que vous avez déterminé lors de la planification de votre configuration MetroCluster.
- *Gestion des disques et des agrégats* contient plus d'informations sur les agrégats en miroir.

Étapes

1. Installez et câisez les tiroirs disques qui contiennent les agrégats non mis en miroir.

   Vous pouvez utiliser les procédures de la documentation *installation et Setup* pour votre plate-forme et vos tiroirs disques.

"Documentation des systèmes matériels ONTAP"

2. Attribuer manuellement tous les disques du nouveau shelf au nœud approprié :

   `disk assign -disk disk-id -owner owner-node-name`

3. Créer l'agrégat :

   `storage aggregate create`

   Si vous êtes connecté au cluster depuis l'interface de gestion du cluster, vous pouvez créer un agrégat sur n'importe quel nœud du cluster. Pour vérifier que l'agrégat est créé sur un nœud spécifique, il est important d'utiliser le `-node` paramètre ou spécifiez les disques qui sont détenus par ce nœud.

   Vous devez également vous assurer d'inclure uniquement les disques du tiroir sans miroir à l'agrégat.

   Vous pouvez spécifier les options suivantes :

   - Nœud de rattachement de l'agrégat (c'est-à-dire le nœud qui détient l'agrégat en fonctionnement normal)
   - Liste de disques spécifiques ou de LUN de baies à ajouter à l'agrégat
   - Nombre de disques à inclure
   - Style de checksum à utiliser pour l'agrégat
   - Type de disques à utiliser
   - Taille des disques à utiliser
   - Vitesse de conduite à utiliser
   - Type RAID des groupes RAID sur l'agrégat
   - Nombre maximal de disques ou de LUN de baies pouvant être inclus dans un groupe RAID
   - Indique si les disques à régime différent sont autorisés

     Pour plus d'informations sur ces options, reportez-vous au `storage aggregate create` page de manuel.

     La commande suivante crée un agrégat sans mise en miroir avec 10 disques :

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

4. Vérifier le groupe RAID et les disques de votre nouvel agrégat :

   `storage aggregate show-status -aggregate aggregate-name`

Informations associées

"Gestion des disques et des agrégats"

Installation du micrologiciel après l'ajout d'un module de contrôleur

Après avoir ajouté le module de contrôleur, vous devez installer la dernière version du micrologiciel sur le nouveau module de contrôleur de sorte que le module de contrôleur fonctionne correctement avec ONTAP.

Étapes

1. Téléchargez la version la plus récente du micrologiciel de votre système et suivez les instructions de téléchargement et d'installation du nouveau micrologiciel.

   "Téléchargements NetApp : firmware système et diagnostics"

Actualisation de la configuration MetroCluster avec de nouveaux contrôleurs

Vous devez actualiser la configuration MetroCluster lors de son extension d'une configuration à deux nœuds à une configuration à quatre nœuds.

Étapes

1. Actualisez la configuration MetroCluster :

   a. Passez en mode de privilège avancé :
   `set -privilege advanced`

   b. Actualisez la configuration MetroCluster :
   `metrocluster configure -refresh true -allow-with-one-aggregate true`

   La commande suivante actualise la configuration de MetroCluster sur tous les nœuds du groupe DR qui contient Controller_A_1 :

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

   a. Revenir en mode de privilège admin :

   `set -privilege admin`

2. Vérifiez l'état de la mise en réseau sur le site A :

   `network port show`

   L'exemple suivant montre l'utilisation du port réseau sur une configuration MetroCluster à quatre nœuds :

```
cluster_A::> network port show
                                                             Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Vérifier la configuration MetroCluster des deux sites de la configuration MetroCluster.

   a. Vérifier la configuration à partir du site A :

      `metrocluster show`

      ```
      cluster_A::> metrocluster show
      Cluster                   Entry Name          State
      ------------------------- ------------------- -----------
       Local: cluster_A         Configuration state configured
                                Mode                normal
                                AUSO Failure Domain auso-on-cluster-
      disaster
      Remote: cluster_B         Configuration state configured
                                Mode                normal
                                AUSO Failure Domain auso-on-cluster-
      disaster
      ```

   b. Vérifier la configuration à partir du site B :

      `metrocluster show`

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

c. Vérifier que les relations de reprise sur incident ont été correctement créées :

`metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner`

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Activation du basculement du stockage sur les deux modules de contrôleur et activation de la haute disponibilité du cluster

Après avoir ajouté de nouveaux modules de contrôleur à la configuration MetroCluster, vous devez activer le basculement du stockage sur les deux modules de contrôleur et activer séparément la haute disponibilité du cluster.

Avant de commencer

La configuration MetroCluster doit avoir déjà été actualisée à l'aide du `metrocluster configure -refresh true` commande.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Activation du basculement du stockage :

   `storage failover modify -enabled true -node existing-node-name`

   La commande unique permet le basculement du stockage sur les deux modules de contrôleur.

2. Vérifiez que le basculement du stockage est activé :

   `storage failover show`

   La sortie doit être similaire à ce qui suit :

   ```
   Node           Partner        Possible State Description
   -------------- -------------- -------- ---------------------
   old-ctlr        new-ctlr      true      Connected to new-ctlr
   new-ctlr        old-ctlr      true      Connected to old-ctlr
   2 entries were displayed.
   ```

3. Activation de la haute disponibilité du cluster :

   `cluster ha modify -configured true`

   La haute disponibilité du cluster (HA) doit être configurée dans un cluster si celui-ci ne contient que deux nœuds et diffère de la haute disponibilité offerte par le basculement du stockage.

Redémarrage des SVM

Après avoir étendu la configuration MetroCluster, vous devez redémarrer les SVM.

Étapes

1. Identifier les SVM à redémarrer :

   `metrocluster vserver show`

   Cette commande affiche les SVM sur les deux clusters MetroCluster.

2. Redémarrer les SVM sur le premier cluster :

   a. Passez en mode privilège avancé, puis appuyez sur **`y`** lorsque vous y êtes invité :

      `set -privilege advanced`

   b. Redémarrage des SVM :

      `vserver start -vserver SVM_name -force true`

   c. Revenir en mode de privilège admin :

```
set -privilege admin
```

3. Répétez l'étape précédente sur le cluster partenaire.
4. Vérifier que les SVM sont bien en état :

```
metrocluster vserver show
```

Étendez une configuration FC MetroCluster à quatre nœuds à une configuration à huit nœuds

Extension d'une configuration FC MetroCluster à quatre nœuds à une configuration à huit nœuds

L'extension d'une configuration FC MetroCluster à quatre nœuds à une configuration FC MetroCluster à huit nœuds implique l'ajout de deux contrôleurs à chaque cluster pour former une seconde paire haute disponibilité sur chaque site MetroCluster, puis l'exécution de la configuration FC MetroCluster.

Description de la tâche

- Les nœuds doivent exécuter ONTAP 9 dans une configuration MetroCluster FC.

  Cette procédure n'est pas prise en charge sur les versions antérieures de ONTAP ou dans les configurations MetroCluster IP.

- La configuration FC MetroCluster existante doit être saine.
- L'équipement que vous ajoutez doit être pris en charge et répondre à toutes les exigences décrites dans "Installation et configuration de la solution Fabric-Attached MetroCluster"
- Vous devez disposer de ports de commutateurs FC disponibles pour prendre en charge les nouveaux contrôleurs et les nouveaux ponts.
- Vous avez besoin du mot de passe d'administration et de l'accès à un serveur FTP ou SCP.
- Cette procédure s'applique uniquement aux configurations MetroCluster FC.
- Cette procédure ne génère aucune interruption et prend environ un jour (sauf le rack et la pile) lors de la mise à zéro des disques.

Avant d'effectuer cette procédure, la configuration FC MetroCluster se compose de quatre nœuds, avec une paire haute disponibilité sur chaque site :

Au terme de cette procédure, la configuration FC MetroCluster est constituée de deux paires HA sur chaque site :

Les deux sites doivent être étendus de la même manière. Une configuration MetroCluster FC ne peut pas comprendre un nombre irrégulier de nœuds.

Combinaisons de plateformes prises en charge lors de l'ajout d'un deuxième groupe de reprise après incident

Le tableau suivant présente les combinaisons de plateformes prises en charge pour les configurations FC

MetroCluster à 8 nœuds.

- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, si vous avez une configuration à huit nœuds, les huit nœuds doivent exécuter la même version de ONTAP.
- Les combinaisons indiquées dans ce tableau s'appliquent uniquement aux configurations à huit nœuds standard ou permanentes.
- Les combinaisons de plates-formes de ce tableau **ne** s'appliquent pas si vous utilisez les procédures de transition ou d'actualisation.
- Tous les nœuds d'un groupe de reprise après incident doivent être du même type et de la même configuration.

		8Node DrGroup 2									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
8Node DrGroup 1	FAS8200										
	AFF A300										
	FAS8300										
	AFF A400										
	ASA A400										
	FAS9000										
	AFF A700										
	FAS9500										
	AFF A900										
	ASA A900										

Détermination de la nouvelle disposition de câblage

Vous devez déterminer le câblage reliant les nouveaux modules de contrôleur et les nouveaux tiroirs disques aux commutateurs FC existants.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Suivre la procédure décrite dans "Installation et configuration de la solution Fabric-Attached MetroCluster" Pour créer une disposition de câblage pour votre type de commutateur, en utilisant l'utilisation des ports pour une configuration MetroCluster à huit nœuds.

   L'utilisation du port de commutateur FC doit correspondre à l'utilisation décrite dans la procédure pour que les fichiers de configuration de référence (RCFs) puissent être utilisés.

   Si votre environnement ne peut pas être câblé de sorte que les fichiers RCF puissent être utilisés, vous devez configurer manuellement le système en suivant les instructions du "Installation et configuration de la solution Fabric-Attached MetroCluster". N'utilisez pas cette procédure si le câblage ne peut pas utiliser les fichiers RCF.

Mise en rack du nouvel équipement

Vous devez installer l'équipement pour les nouveaux nœuds.

Étapes

1. Suivre la procédure décrite dans "Installation et configuration de la solution Fabric-Attached MetroCluster" Pour installer les nouveaux systèmes de stockage, les tiroirs disques et les ponts FC-SAS.

Vérification de l’état de santé de la configuration MetroCluster

Vous devez vérifier l’état de santé de la configuration MetroCluster pour vérifier que celle-ci fonctionne correctement.

Étapes

1. Vérifier que la MetroCluster est configurée et en mode normal sur chaque cluster :

   `metrocluster show`

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
```

2. Vérifier que la mise en miroir est activée sur chaque nœud :

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

3. Vérifier que les composants MetroCluster sont sains :

   `metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Vérifier qu'il n'y a pas d'alerte de santé :

   ```
   system health alert show
   ```

5. Simuler une opération de basculement :

   a. Depuis l'invite d'un nœud, passez au niveau de privilège avancé :
      `set -privilege advanced`

      Vous devez répondre avec **`y`** lorsque vous êtes invité à passer en mode avancé et à afficher l'invite du mode avancé (*>).

   b. Effectuer l'opération de basculement avec le paramètre -Simulate :
      `metrocluster switchover -simulate`

   c. Revenir au niveau de privilège admin :
      `set -privilege admin`

Vérification des erreurs de configuration MetroCluster avec Config Advisor

Vous pouvez accéder au site de support NetApp et télécharger l'outil Config Advisor pour vérifier les erreurs de configuration courantes.

Description de la tâche

Config Advisor est un outil de validation de la configuration et de vérification de l'état de santé. Vous pouvez le déployer sur des sites sécurisés et sur des sites non sécurisés à des fins de collecte des données et d'analyse du système.

Le support pour Config Advisor est limité et n'est disponible qu'en ligne.

Étapes

1. Accédez à la page de téléchargement Config Advisor et téléchargez l'outil.

   "Téléchargement NetApp : Config Advisor"

2. Exécutez Config Advisor, examinez les résultats de l'outil et suivez les recommandations du produit pour résoudre tous les problèmes détectés.

Envoi d'un message AutoSupport personnalisé avant d'ajouter des nœuds à la configuration MetroCluster

Vous devez émettre un message AutoSupport pour informer le support technique de NetApp que les opérations de maintenance sont en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Connectez-vous au cluster au site_A.
2. Appelez un message AutoSupport indiquant le début de la maintenance :

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   Le `maintenance-window-in-hours` le paramètre spécifie la longueur de la fenêtre de maintenance et peut être un maximum de 72 heures. Si la maintenance est terminée avant le temps qui s'est écoulé, vous pouvez passer la commande suivante pour indiquer que la période de maintenance a pris fin :

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Répétez cette étape sur le site du partenaire.

Recâble et zone une structure de commutation pour les nouveaux nœuds

Déconnexion du groupe DR existant de la structure

Vous devez déconnecter les modules de contrôleur existants des commutateurs FC dans la structure.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Désactivez les ports HBA qui connectent les modules de contrôleur existants à la structure du commutateur en cours de maintenance :

   `storage port disable -node` *`node-name`* `-port` *`port-number`*

2. Sur les commutateurs FC locaux, retirer les câbles des ports des ponts HBA, FC-VI et ATTO du module de contrôleur existant.

Vous devez étiqueter les câbles pour faciliter leur identification lorsque vous les recâetez. Seuls les ports ISL doivent rester câblés.

Recâblage et reconfiguration des commutateurs

Vous devez appliquer les fichiers RCF pour reconfigurer votre zoning afin de l'adapter aux nouveaux nœuds.

Si vous ne pouvez pas utiliser les fichiers RCF pour configurer les commutateurs, vous devez configurer les commutateurs manuellement. Voir :

- "Configurez manuellement les commutateurs FC Brocade"
- "Configurez manuellement les commutateurs Cisco FC"

Étapes

1. Recherchez les fichiers RCF correspondant à votre configuration.

   Vous devez utiliser les fichiers RCF pour une configuration à huit nœuds correspondant à votre modèle de commutateur.

2. Appliquez les fichiers RCF en suivant les instructions de la page de téléchargement, en ajustant les paramètres ISL selon vos besoins.
3. Assurez-vous que la configuration du commutateur est enregistrée.
4. Redémarrez les commutateurs FC.
5. Reliez les ponts FC-to-SAS existants et les nouveaux ponts FC-SAS aux commutateurs FC, à l'aide de la disposition de câblage que vous avez créée précédemment.

   L'utilisation du port de commutateur FC doit correspondre à l'utilisation de huit nœuds MetroCluster décrite à la "Installation et configuration de la solution Fabric-Attached MetroCluster" Pour que les fichiers de configuration de référence (RCFs) puissent être utilisés.

6. Vérifiez que les ports sont en ligne à l'aide de la commande appropriée pour votre commutateur.

Changer de fournisseur	Commande
Brocade	affichage du commutateur
Cisco	afficher la description de l'interface

7. Suivre la procédure décrite dans "Installation et configuration de la solution Fabric-Attached MetroCluster" Pour câbler les ports FC-VI des nouveaux contrôleurs et existants, en utilisant la disposition de câblage que vous avez créée précédemment.

   L'utilisation du port de commutateur FC doit correspondre à l'utilisation de huit nœuds MetroCluster décrite à la "Installation et configuration de la solution Fabric-Attached MetroCluster" Pour que les fichiers de configuration de référence (RCFs) puissent être utilisés.

8. Depuis les nœuds existants, vérifier que les ports FC-VI sont en ligne :

   ```
   metrocluster interconnect adapter show
   ```

```
metrocluster interconnect mirror show
```

9. Reliez les ports HBA aux contrôleurs actuels et nouveaux.
10. Sur les modules de contrôleur existants, activer en e-commerce les ports connectés au commutateur en cours de maintenance :

    ```
    storage port enable -node node-name -port port-ID
    ```

11. Démarrer les nouveaux contrôleurs et les démarrer en mode maintenance :

    ```
    boot_ontap maint
    ```

12. Vérifier que seul le stockage qui sera utilisé par le nouveau groupe DR est visible pour les nouveaux modules de contrôleur.

    Aucun du stockage utilisé par l'autre groupe DR ne doit être visible.

13. Revenez au début de ce processus pour raccorder à nouveau le second commutateur de structure.

Configurez ONTAP sur les nouveaux contrôleurs

Effacement de la configuration sur un module de contrôleur

Avant d'utiliser un nouveau module de contrôleur dans la configuration MetroCluster, il faut effacer la configuration existante.

Étapes

1. Si nécessaire, arrêtez le nœud pour afficher l'invite DU CHARGEUR :

   ```
   halt
   ```

2. Dans l'invite DU CHARGEUR, définissez les variables environnementales sur les valeurs par défaut :

   ```
   set-defaults
   ```

3. Enregistrez l'environnement :

   ```
   saveenv
   ```

4. À l'invite DU CHARGEUR, lancez le menu de démarrage :

   ```
   boot_ontap menu
   ```

5. À l'invite du menu de démarrage, effacez la configuration :

   ```
   wipeconfig
   ```

   Répondez `yes` à l'invite de confirmation.

   Le nœud redémarre et le menu de démarrage s'affiche de nouveau.

6. Dans le menu de démarrage, sélectionnez l'option **5** pour démarrer le système en mode Maintenance.

Répondez `yes` à l'invite de confirmation.

Assignation de la propriété des disques dans les systèmes AFF

Si vous utilisez des systèmes AFF dans une configuration avec des agrégats en miroir et que les nœuds ne disposent pas des disques (SSD) correctement affectés, vous devez attribuer la moitié des disques de chaque tiroir à un nœud local et l'autre moitié des disques à son nœud partenaire haute disponibilité. Vous devez créer une configuration dans laquelle chaque nœud a le même nombre de disques dans ses pools de disques locaux et distants.

Description de la tâche

Les contrôleurs de stockage doivent être en mode maintenance.

Cela ne s'applique pas aux configurations qui ne disposent pas d'agrégats en miroir, qui possèdent une configuration active/passive ou qui disposent d'un nombre inégal de disques dans les pools locaux et distants.

Cette tâche n'est pas requise si les disques ont été correctement affectés lorsqu'ils ont été reçus de l'usine.

> Le pool 0 contient toujours les disques qui se trouvent sur le même site que le système de stockage qui les possède, tandis que le pool 1 contient toujours les disques qui sont distants du système de stockage qui les possède.

Étapes

1. Si ce n'est pas le cas, démarrez chaque système en mode maintenance.
2. Assigner les disques aux nœuds situés sur le premier site (site A) :

   Vous devez affecter un nombre égal de disques à chaque pool.

   a. Sur le premier nœud, attribuer systématiquement la moitié des disques de chaque tiroir afin de regrouper 0 et l'autre moitié au pool du partenaire haute disponibilité 0:
   `disk assign -disk *disk-name* -p *pool* -n *number-of-disks*`

      Si le contrôleur de stockage Controller_A_1 dispose de quatre tiroirs, chacun doté de 8 SSD, vous exécutez les commandes suivantes :

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
      ```

   b. Répétez le processus pour le second nœud sur le site local, en affectant systématiquement la moitié des disques de chaque tiroir au pool 1 et l'autre moitié au pool 1 du partenaire haute disponibilité :
   `disk assign -disk *disk-name* -p *pool*`

      Si le contrôleur de stockage Controller_A_1 dispose de quatre tiroirs, chacun doté de 8 SSD, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Assigner les disques aux nœuds situés sur le second site (site B) :

   Vous devez affecter un nombre égal de disques à chaque pool.

   a. Sur le premier nœud du site distant, attribuer systématiquement la moitié des disques de chaque tiroir dans le pool 0 et l'autre moitié dans le pool 0: + du partenaire haute disponibilité `disk assign -disk *disk-name* -p *pool*`

      Si le contrôleur de stockage Controller_B_1 dispose de quatre tiroirs, chacun doté de 8 SSD, vous exécutez les commandes suivantes :

      ```
      *> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
      *> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

      *> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
      *> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
      ```

   b. Répétez le processus pour le second nœud sur le site distant en affectant systématiquement la moitié des disques de chaque tiroir au pool 1 et l'autre moitié au pool 1 du partenaire haute disponibilité :

      `disk assign -disk *disk-name* -p *pool*`

      Si le contrôleur de stockage Controller_B_2 dispose de quatre tiroirs, chacun doté de 8 SSD, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirmez les attributions de disques :

   `storage show disk`

5. Quitter le mode Maintenance :

   `halt`

6. Afficher le menu de démarrage :

```
boot_ontap menu
```

7. Sur chaque nœud, sélectionnez l'option **4** pour initialiser tous les disques.

Assignation de la propriété des disques dans des systèmes non-AFF

Si les nœuds MetroCluster ne sont pas affectés correctement, ou si vous utilisez des tiroirs disques DS460C dans votre configuration, il est nécessaire d'attribuer des disques à chacun des nœuds de la configuration MetroCluster selon le tiroir par tiroir. Vous allez créer une configuration dans laquelle chaque nœud a le même nombre de disques dans ses pools de disques locaux et distants.

Description de la tâche

Les contrôleurs de stockage doivent être en mode maintenance.

Si votre configuration n'inclut pas de tiroirs disques DS460C, cette tâche n'est pas requise si les disques ont été correctement attribués lors de leur réception par l'usine.

> Le pool 0 contient toujours les disques qui se trouvent sur le même site que le système de stockage qui les possède.
>
> Le pool 1 contient toujours les disques distants du système de stockage qui les possèdent.

Si votre configuration inclut des tiroirs disques DS460C, il est conseillé d'attribuer manuellement les disques en suivant les instructions suivantes pour chaque tiroir 12 disques :

Affectez ces disques dans le tiroir…	À ce nœud et pool…
0 - 2	Pool du nœud local 0
3 - 5	Pool 0 du nœud partenaire HA
6 - 8	Partenaire DR du pool du nœud local 1
9 - 11	Partenaire de reprise après incident du pool de partenaires de haute disponibilité 1

Ce modèle d'affectation de disque permet de s'assurer qu'un agrégat est au moins affecté en cas de mise hors ligne d'un tiroir.

Étapes

1. Si ce n'est pas le cas, démarrez chaque système en mode maintenance.
2. Assigner les tiroirs disques aux nœuds situés sur le premier site (site A) :

   Les tiroirs disques du même site que le nœud sont affectés au pool 0 et les tiroirs disques situés sur le site partenaire sont affectés au pool 1.

   Vous devez affecter un nombre égal de tiroirs à chaque pool.

   a. Sur le premier nœud, attribuer systématiquement les tiroirs disques locaux à pool 0 et les tiroirs

disques distants à pool 1 :

`disk assign -shelf local-switch-name:shelf-name.port -p pool`

Si le contrôleur de stockage Controller_A_1 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

b. Répétez le processus pour le second nœud du site local, en affectant systématiquement les tiroirs disques locaux au pool 0 et les tiroirs disques distants au pool 1 :

`disk assign -shelf local-switch-name:shelf-name.port -p pool`

Si le contrôleur de stockage Controller_A_2 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Assigner les tiroirs disques aux nœuds situés sur le second site (site B) :

Les tiroirs disques du même site que le nœud sont affectés au pool 0 et les tiroirs disques situés sur le site partenaire sont affectés au pool 1.

Vous devez affecter un nombre égal de tiroirs à chaque pool.

a. Sur le premier nœud du site distant, attribuer systématiquement ses tiroirs disques locaux à regrouper 0 et ses tiroirs disques distants à pool 1 :

`disk assign -shelf local-switch-nameshelf-name -p pool`

Si le contrôleur de stockage Controller_B_1 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. Répétez le processus pour le second nœud du site distant en affectant systématiquement ses tiroirs disques locaux au pool 0 et ses tiroirs disques distants au pool 1 :

   `disk assign -shelf shelf-name -p pool`

   Si le contrôleur de stockage Controller_B_2 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirmer les attributions de tiroirs :

   `storage show shelf`

5. Quitter le mode Maintenance :

   `halt`

6. Afficher le menu de démarrage :

   `boot_ontap menu`

7. Sur chaque nœud, sélectionnez l'option **4** pour initialiser tous les disques.

Vérification de l'état ha-config des composants

Dans une configuration MetroCluster, l'état ha-config du module de contrôleur et des composants du châssis doit être défini sur **mcc** pour qu'ils s'démarrent correctement.

Description de la tâche

- Le système doit être en mode Maintenance.
- Cette tâche doit être effectuée sur chaque nouveau module de contrôleur.

Étapes

1. En mode Maintenance, afficher l'état HA du module de contrôleur et du châssis :

   `ha-config show`

   L'état HA pour tous les composants doit être « mcc ».

2. Si l'état système affiché du contrôleur n'est pas correct, définissez l'état HA pour le module de contrôleur :

   `ha-config modify controller mcc`

3. Si l'état du système affiché du châssis n'est pas correct, définissez l'état de haute disponibilité du châssis :

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

4. Répétez ces étapes sur l'autre nœud de remplacement.

Démarrage des nouveaux contrôleurs et connexion à leur cluster

Pour associer les nouveaux contrôleurs au cluster, vous devez démarrer chaque nouveau module de contrôleur et utiliser l'assistant de configuration du cluster ONTAP pour identifier le cluster.

Avant de commencer

Vous devez avoir câblé la configuration MetroCluster.

Vous ne devez pas avoir configuré le processeur de service avant d'effectuer cette tâche.

Description de la tâche

Cette tâche doit être effectuée sur chacun des nouveaux contrôleurs des deux clusters de la configuration MetroCluster.

Étapes

1. Si vous ne l'avez pas encore fait, mettez chaque nœud sous tension et laissez-le démarrer complètement.

   Si le système est en mode Maintenance, exécutez le `halt` Commande pour quitter le mode maintenance, puis lancer la commande suivante à partir de l'invite DU CHARGEUR :

   ```
   boot_ontap
   ```

   Le module de contrôleur entre dans l'assistant de configuration des nœuds.

   La sortie doit être similaire à ce qui suit :

   ```
   Welcome to node setup

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
                 Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.
   .
   .
   .
   ```

2. Activer l'outil AutoSupport en suivant les instructions fournies par le système.
3. Répondez aux invites pour configurer l'interface de gestion des nœuds.

   Les invites sont similaires à ce qui suit :

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Vérifier que les nœuds sont configurés en mode haute disponibilité :

   `storage failover show -fields mode`

   Si ce n'est pas le cas, vous devez lancer la commande suivante sur chaque nœud, puis redémarrer le nœud :

   `storage failover modify -mode ha -node localhost`

   Cette commande configure le mode haute disponibilité, mais n'active pas le basculement du stockage. Le basculement du stockage est automatiquement activé lorsque vous émettez le `metrocluster configure` commande plus tard dans le processus de configuration.

5. Vérifiez que quatre ports sont configurés en tant qu'interconnexions de cluster :

   `network port show`

   L'exemple suivant montre les valeurs de sortie de deux contrôleurs du cluster_A. S'il s'agit d'une configuration MetroCluster à deux nœuds, la sortie affiche un seul nœud.

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Comme vous utilisez l'interface de ligne de commandes pour configurer le cluster, quittez l'assistant d'installation des nœuds :

   ```
   exit
   ```

7. Connectez-vous au compte admin à l'aide de `admin` nom d'utilisateur.
8. Démarrez l'assistant de configuration du cluster, puis rejoignez le cluster existant :

   ```
   cluster setup
   ```

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`
```

9. Une fois l'assistant **Cluster Setup** terminé et qu'il quitte, vérifiez que le cluster est actif et que le nœud fonctionne correctement :

   `cluster show`

   L'exemple suivant montre un cluster dans lequel le premier nœud (cluster 1-01) est sain et peut participer :

```
cluster_A::> cluster show
Node                 Health  Eligibility
-------------------- ------- ------------
node_A_1             true    true
node_A_2             true    true
node_A_3             true    true
```

   S'il est nécessaire de modifier les paramètres que vous avez saisis pour le SVM admin ou le SVM node, vous pouvez accéder à l'assistant **Cluster Setup** en utilisant le `cluster setup command`.

Configurer les clusters dans une configuration MetroCluster

Configurer les LIFs intercluster

Configuration des LIFs intercluster sur des ports dédiés

Vous pouvez configurer les LIFs intercluster sur des ports dédiés. Cela augmente généralement la bande passante disponible pour le trafic de réplication.

Étapes

1. Lister les ports dans le cluster :

`network port show`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les ports réseau en cluster01 :

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Déterminer les ports disponibles pour dédier aux communications intercluster :

   `network interface show -fields home-port,curr-port`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre que les ports « e0e » et « e0f » n'ont pas été affectés aux LIF :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Créer un failover group pour les ports dédiés :

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   L'exemple suivant attribue les ports « e0e » et « e0f » au groupe de basculement « intercluster01 » sur le SVM système « cluster01 » :

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

   `network interface failover-groups show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

Version ONTAP	Commande
9.6 et versions ultérieures	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 et versions antérieures	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » dans le groupe de basculement « intercluster01 » :

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Vérifier que les LIFs intercluster ont été créés :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vérifier que les LIFs intercluster sont redondants :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster -failover`

Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre que les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » sur le port SVM « e0e » basculeront vers le port « e0f ».

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configuration des LIFs intercluster sur des ports data partagés

Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau en cluster01 :

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Création des LIFs intercluster sur le SVM système :

Dans ONTAP 9.6 et plus tard:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
Dans ONTAP 9.5 et versions antérieures:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Vérifier que les LIFs intercluster ont été créés :

Dans ONTAP 9.6 et plus tard:
`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vérifier que les LIFs intercluster sont redondants :

Dans ONTAP 9.6 et plus tard:
`network interface show –service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:
`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre que les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » sur le port « e0c » basculeront vers le port « e0d ».

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Mise en miroir des agrégats racine

Pour assurer la protection des données, vous devez mettre en miroir les agrégats racine.

Par défaut, l'agrégat root est créé comme un agrégat de type RAID-DP. Vous pouvez changer l'agrégat racine de RAID-DP à l'agrégat de type RAID4 La commande suivante modifie l'agrégat racine pour l'agrégat de type RAID4 :

```
storage aggregate modify –aggregate aggr_name -raidtype raid4
```

Sur les systèmes non ADP, le type RAID de l'agrégat peut être modifié depuis le RAID-DP par défaut vers le RAID4 avant ou après la mise en miroir de l'agrégat.

Étapes

1. Mettre en miroir l'agrégat racine :

   `storage aggregate mirror` *`aggr_name`*

   La commande suivante met en miroir l'agrégat root pour Controller_A_1 :

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Cela met en miroir l'agrégat, il se compose d'un plex local et d'un plex distant situé sur le site MetroCluster distant.

2. Répétez l'étape précédente pour chaque nœud de la configuration MetroCluster.

Mise en œuvre de la configuration MetroCluster

Vous devez exécuter le `metrocluster configure -refresh true` Commande

pour démarrer la protection des données sur les nœuds que vous avez ajoutés à une configuration MetroCluster.

Description de la tâche

Vous émettez le `metrocluster configure -refresh true` Commande unique sur l'un des nœuds récemment ajoutés pour actualiser la configuration MetroCluster. Il n'est pas nécessaire d'exécuter la commande sur chacun des sites ou nœuds.

Le `metrocluster configure -refresh true` La commande couple automatiquement les deux nœuds avec les ID système les plus bas dans chacun des deux clusters comme partenaires de reprise d'activité. Dans une configuration MetroCluster à quatre nœuds, il existe deux paires de partenaires pour la reprise après incident. La seconde paire DR est créée à partir des deux nœuds avec des ID système plus élevés.

Étapes

1. Actualisez la configuration MetroCluster :

   a. Entrer en mode de privilège avancé :

      `set -privilege advanced`

   b. Actualiser la configuration MetroCluster sur l'un des nouveaux nœuds :
   `metrocluster configure -refresh true`

      L'exemple suivant montre la configuration MetroCluster mise à jour sur les deux groupes de reprise sur incident :

```
controller_A_2::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

+

```
controller_A_4::*> metrocluster configure -refresh true

[Job 740] Job succeeded: Configure is successful.
```

   a. Revenir en mode de privilège admin :

      `set -privilege admin`

2. Vérifiez l'état de la mise en réseau sur le site A :

   `network port show`

   L'exemple suivant montre l'utilisation du port réseau sur une configuration MetroCluster à quatre nœuds :

```
cluster_A::> network port show
                                                                 Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Vérifier la configuration MetroCluster depuis les deux sites en configuration MetroCluster :

   a. Vérifier la configuration à partir du site A :

      `metrocluster show`

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

   a. Vérifier la configuration à partir du site B :
      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

Crée un agrégat de données en miroir sur chaque nœud

Vous devez créer un agrégat de données en miroir sur chaque nœud du groupe de reprise sur incident.

Description de la tâche

- Vous devez savoir quels disques seront utilisés dans le nouvel agrégat.
- Si votre système compte plusieurs types de disques (stockage hétérogène), vous devez comprendre comment vous assurer que le type de disque approprié est sélectionné.
- Les disques sont détenus par un nœud spécifique ; lorsque vous créez un agrégat, tous les disques de cet agrégat doivent être détenus par le même nœud, qui devient le nœud de rattachement de cet agrégat.

  Dans les systèmes utilisant ADP, des agrégats sont créés à l'aide de partitions dans lesquelles chaque disque est partitionné en partitions P1, P2 et P3.

- Les noms d'agrégats doivent être conformes au schéma de nommage que vous avez déterminé lors de la planification de votre configuration MetroCluster.

  "Gestion des disques et des agrégats"

> Pour optimiser les performances et la disponibilité du stockage, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces meilleures pratiques peut avoir un impact négatif sur les performances.

Étapes

1. Afficher la liste des pièces de rechange disponibles :

   ```
   storage disk show -spare -owner node_name
   ```

2. Créer l'agrégat :

   ```
   storage aggregate create -mirror true
   ```

Si vous êtes connecté au cluster depuis l'interface de gestion du cluster, vous pouvez créer un agrégat sur n'importe quel nœud du cluster. Pour s'assurer que l'agrégat est créé sur un nœud spécifique, utilisez le `-node` paramètre ou spécifiez les disques qui sont détenus par ce nœud.

Vous pouvez spécifier les options suivantes :

- Nœud de rattachement de l'agrégat (c'est-à-dire le nœud qui détient l'agrégat en fonctionnement normal)
- Liste de disques spécifiques à ajouter à l'agrégat
- Nombre de disques à inclure

> Dans la configuration minimale prise en charge, dans laquelle un nombre limité de disques sont disponibles, vous devez utiliser l'option force-petits agrégats pour créer un agrégat RAID-DP à trois disques.

- Style de checksum à utiliser pour l'agrégat
- Type de disques à utiliser
- Taille des disques à utiliser
- Vitesse de conduite à utiliser
- Type RAID des groupes RAID sur l'agrégat
- Nombre maximal de disques pouvant être inclus dans un groupe RAID
- Indique si les disques à régime différent sont autorisés

Pour plus d'informations sur ces options, reportez-vous au `storage aggregate create` page de manuel.

La commande suivante crée un agrégat en miroir avec 10 disques :

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Vérifier le groupe RAID et les disques de votre nouvel agrégat :

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Configuration de ponts FC-SAS pour le contrôle de l'état du système

Description de la tâche

- Les outils de surveillance SNMP tiers ne sont pas pris en charge pour les ponts FiberBridge.
- Depuis la version ONTAP 9.8, les ponts FC-SAS sont surveillés par défaut via des connexions intrabande, ce qui n'est pas nécessaire.

Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Étape

1. Dans l'invite de cluster ONTAP, ajoutez le pont au contrôle de l'état de santé :

   a. Ajoutez le pont à l'aide de la commande pour votre version de ONTAP :

Version ONTAP	Commande
9.5 et versions ultérieures	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 et versions antérieures	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   b. Vérifiez que le pont a été ajouté et est correctement configuré :

      `storage bridge show`

      La prise en compte de toutes les données peut prendre jusqu'à 15 minutes en raison de l'intervalle d'interrogation. Le contrôle de l'état du système ONTAP peut contacter et surveiller le pont si la valeur de la colonne « État » est « ok » et si d'autres informations, telles que le nom universel (WWN), sont affichées.

      L'exemple suivant montre que les ponts FC-SAS sont configurés :

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model               Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Déplacement d’un volume de métadonnées dans les configurations MetroCluster

Vous pouvez déplacer un volume de métadonnées d’un agrégat vers un autre dans une configuration MetroCluster. Il peut être nécessaire de déplacer un volume de métadonnées lors de la mise hors service ou non en miroir de l’agrégat source, ou pour d’autres raisons qui ne le sont pas.

Description de la tâche

- Pour effectuer cette tâche, vous devez disposer des privilèges d’administrateur de cluster.
- L’agrégat cible doit être mis en miroir et ne doit pas être en état dégradé.
- L’espace disponible dans l’agrégat cible doit être supérieur au volume de métadonnées que vous déplacez.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Identifiez le volume de métadonnées à déplacer :

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW             -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW             -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identifiez un agrégat cible éligible :

   `metrocluster check config-replication show-aggregate-eligibility`

   La commande suivante identifie les agrégats du cluster_A éligibles aux volumes de métadonnées hôte :

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

Dans l'exemple précédent, Node_A_1_aggr2 et Node_A_2_aggr2 sont éligibles.

4. Lancez l'opération de déplacement de volume :

   `volume move start -vserver` *`svm_name`* `-volume` *`metadata_volume_name`* `-destination -aggregate` *`destination_aggregate_name`*`*`

   La commande suivante déplace le volume de métadonnées « MDV_CRS_14c00d4ac9f311e7922800a0984395f1 » de « Aggregate Node_A_1_aggr1 » à « Aggregate Node_A_1_aggr2 » :

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Vérifiez l'état de l'opération de déplacement de volume :

   ```
   volume move show -volume vol_constituent_name
   ```

6. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Vérification de la configuration MetroCluster

Vous pouvez vérifier que les composants et les relations de la configuration MetroCluster fonctionnent correctement. Vous devez effectuer un contrôle après la configuration initiale et après avoir apporté des modifications à la configuration MetroCluster. Vous devez également effectuer une vérification avant le basculement (prévu) ou le rétablissement.

Description de la tâche

Si le `metrocluster check run` la commande est émise deux fois en peu de temps sur l'un des clusters ou les deux clusters. un conflit peut se produire et la commande risque de ne pas collecter toutes les données. Ensuite `metrocluster check show` les commandes n'affichent pas la sortie attendue.

Étapes

1. Vérifiez la configuration :

   ```
   metrocluster check run
   ```

   La commande s'exécute en arrière-plan et peut ne pas être terminée immédiatement.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Affiche les résultats les plus récents `metrocluster check run` commande :

   ```
   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

   Le `metrocluster check show` les commandes affichent les résultats des plus récentes `metrocluster check run` commande. Vous devez toujours exécuter le `metrocluster check run` avant d'utiliser le `metrocluster check show` commandes de manière à ce que les informations affichées soient à jour.

   L'exemple suivant montre le `metrocluster check aggregate show` Résultat de la commande pour une configuration MetroCluster à quatre nœuds saine :

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
```

```
ok
                    controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2      controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok

18 entries were displayed.
```

L'exemple suivant montre le `metrocluster check cluster show` Résultat de la commande pour une configuration MetroCluster à quatre nœuds saine. Il indique que les clusters sont prêts à effectuer un basculement négocié si nécessaire.

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

Vérification des erreurs de configuration MetroCluster avec Config Advisor

Vous pouvez accéder au site de support NetApp et télécharger l'outil Config Advisor pour vérifier les erreurs de configuration courantes.

Description de la tâche

Config Advisor est un outil de validation de la configuration et de vérification de l'état de santé. Vous pouvez le déployer sur des sites sécurisés et sur des sites non sécurisés à des fins de collecte des données et d'analyse du système.

Le support pour Config Advisor est limité et n'est disponible qu'en ligne.

Étapes

1. Accédez à la page de téléchargement Config Advisor et téléchargez l'outil.

   "Téléchargement NetApp : Config Advisor"

2. Exécutez Config Advisor, examinez les résultats de l'outil et suivez les recommandations du produit pour résoudre tous les problèmes détectés.

Envoi d'un message AutoSupport personnalisé après l'ajout de nœuds à la configuration MetroCluster

Vous devez émettre un message de AutoSupport pour informer le support technique de NetApp que la maintenance est terminée.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Connectez-vous au cluster au site_A.
2. Appeler un message AutoSupport indiquant la fin de la maintenance :

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Répétez cette étape sur le site du partenaire.

Vérification du basculement, de la résolution et du rétablissement

Il est recommandé de vérifier les opérations de basculement, de rétablissement et de rétablissement de la configuration MetroCluster.

Étapes

1. Utilisez les procédures négociées pour le basculement, la réparation et le rétablissement "Gestion et reprise après incident MetroCluster".

Développement d'une configuration IP MetroCluster

Selon votre version de ONTAP, vous pouvez étendre votre configuration MetroCluster IP en ajoutant quatre nouveaux nœuds en tant que nouveau groupe de reprise sur incident.

À partir de ONTAP 9.13.1, vous pouvez développer temporairement une configuration MetroCluster à huit nœuds pour actualiser les contrôleurs et le stockage. Voir "Actualisation d'une configuration IP MetroCluster à quatre ou huit nœuds (ONTAP 9.8 et versions ultérieures)" pour en savoir plus.

Depuis ONTAP 9.9.1, vous pouvez ajouter quatre nouveaux nœuds à la configuration IP de MetroCluster en tant que second groupe de reprise après incident. Cela crée une configuration MetroCluster à huit nœuds.

Avant de commencer

- L'ancien et le nouveau nœud doivent exécuter la même version de ONTAP.
- Cette procédure décrit les étapes requises pour ajouter un groupe DR à quatre nœuds à une configuration IP MetroCluster existante. Si vous actualisez une configuration à huit nœuds, vous devez répéter l'intégralité de la procédure pour chaque groupe de reprise après incident, en l'ajoutant un à la fois.
- Vérifier que les anciens et nouveaux modèles de plate-forme sont pris en charge pour le mélange de plate-forme.

  "NetApp Hardware Universe"

- Vérifiez que les anciens et les nouveaux modèles de plate-forme sont pris en charge par les commutateurs IP.

  "NetApp Hardware Universe"

- Si vous l'êtes "Actualisation d'une configuration IP MetroCluster à quatre ou huit nœuds", les nouveaux nœuds doivent disposer d'un espace de stockage suffisant pour prendre en charge les données des anciens nœuds, ainsi que les disques appropriés pour les agrégats racine et les disques de secours.
- Vérifiez qu'un domaine de diffusion par défaut est créé sur les anciens nœuds.

  Lorsque vous ajoutez de nouveaux nœuds à un cluster existant sans broadcast domain par défaut, les LIFs de node-management sont créées pour les nouveaux nœuds à l'aide d'UUID (Universal unique

identifier) à la place des noms attendus. Pour plus d'informations, consultez l'article de la base de connaissances "Les LIF de gestion de nœuds sur les nouveaux nœuds ajoutés sont générées avec des noms UUID".

Exemple de dénomination dans cette procédure

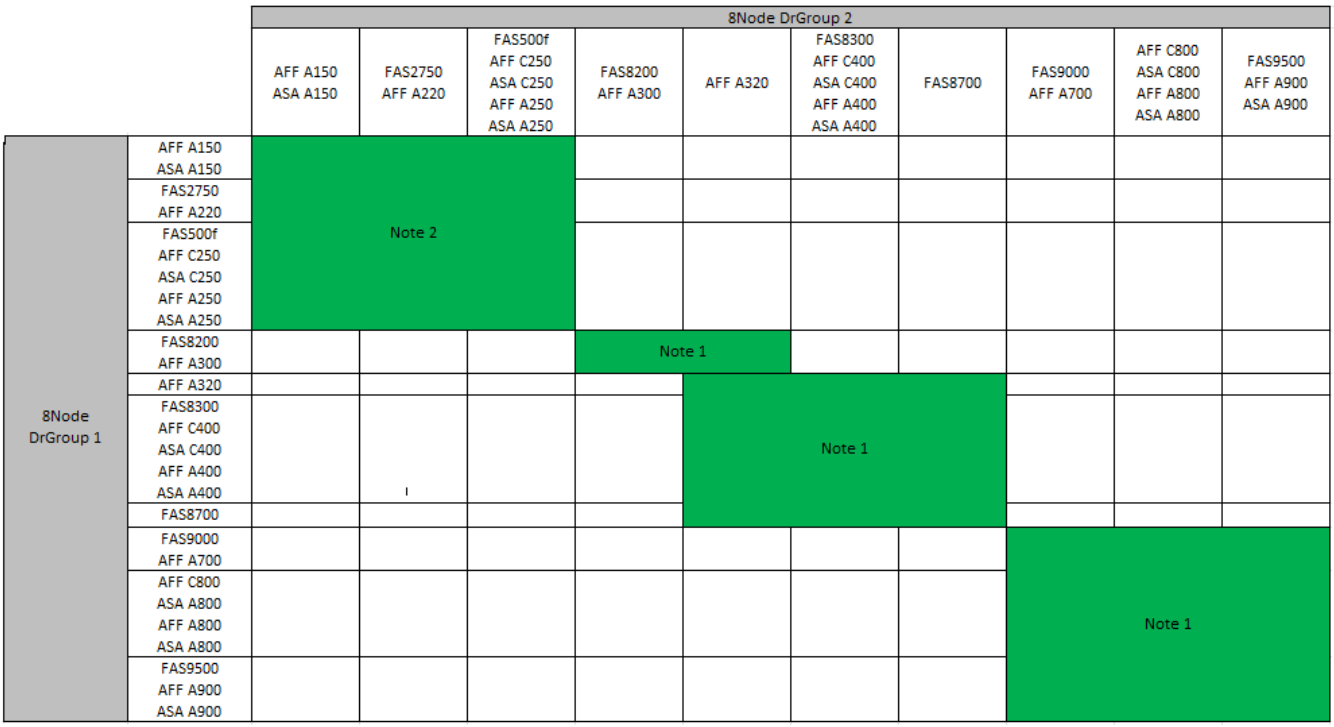
Cette procédure utilise des exemples de noms au cours de l'ensemble pour identifier les groupes de reprise sur incident, les nœuds et les commutateurs impliqués.

Groupes de reprise sur incident	Cluster_A au site_A	Cluster_B au niveau du site_B
dr_group_1-old	• Node_A_1-Old • Node_A_2-Old	• Node_B_1-Old • Node_B_2-Old
dr_group_2-new	• Node_A_3-New • Node_A_4-New	• Node_B_3-New • Node_B_4-New

Combinaisons de plateformes prises en charge lors de l'ajout d'un deuxième groupe de reprise après incident

Le tableau suivant présente les combinaisons de plateformes prises en charge pour les configurations IP à huit nœuds.

- Tous les nœuds de la configuration MetroCluster doivent exécuter la même version de ONTAP. Par exemple, si vous avez une configuration à huit nœuds, les huit nœuds doivent exécuter la même version de ONTAP.
- Les combinaisons de ce tableau s'appliquent uniquement aux configurations 8 nœuds standard ou permanentes.
- Les combinaisons de plates-formes indiquées dans ce tableau **ne** s'appliquent pas si vous utilisez les procédures de transition ou d'actualisation.
- Tous les nœuds d'un groupe de reprise après incident doivent être du même type et de la même configuration.



- **Note 1** : ONTAP 9.9.1 ou version ultérieure (ou la version minimale de ONTAP prise en charge sur la plate-forme) est requise pour ces combinaisons.
- **Note 2** : ONTAP 9.13.1 ou version ultérieure (ou la version minimale de ONTAP prise en charge sur la plate-forme) est requise pour ces combinaisons.

Envoi d'un message AutoSupport personnalisé avant la maintenance

Avant d'effectuer la maintenance, vous devez envoyer un message AutoSupport pour informer le support technique de NetApp que la maintenance est en cours. Informer le support technique que la maintenance est en cours empêche l'ouverture d'un dossier en supposant une interruption de l'activité.

Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

Étapes

1. Pour éviter la génération automatique de dossiers de demande de support, envoyez un message AutoSupport pour indiquer que la mise à niveau est en cours.

   a. Exécutez la commande suivante :

   ```
   system node autosupport invoke -node * -type all -message "MAINT=10h
   Upgrading old-model to new-model"
   ```

   Cet exemple spécifie une fenêtre de maintenance de 10 heures. Selon votre plan, il est possible que vous souhaitiez accorder plus de temps.

   Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Répétez la commande sur le cluster partenaire.

Vérification de l'état de santé de la configuration MetroCluster

Vous devez vérifier l'état et la connectivité de la configuration MetroCluster avant d'effectuer la transition

Étapes

1. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :
   a. Vérifier si le système est multipathed :

      `node run -node node-name sysconfig -a`

   b. Vérifier si des alertes d'intégrité sont disponibles sur les deux clusters :

      `system health alert show`

   c. Vérifier la configuration MetroCluster et que le mode opérationnel est normal :

      `metrocluster show`

   d. Effectuer une vérification MetroCluster :

      `metrocluster check run`

   e. Afficher les résultats de la vérification MetroCluster :

      `metrocluster check show`

   f. Exécutez Config Advisor.

      "Téléchargement NetApp : Config Advisor"

   g. Une fois Config Advisor exécuté, vérifiez les résultats de l'outil et suivez les recommandations fournies dans la sortie pour résoudre tous les problèmes détectés.
2. Vérifiez que le cluster fonctionne correctement :

   `cluster show`

   ```
   cluster_A::> cluster show
   Node           Health  Eligibility
   -------------- ------  -----------
   node_A_1       true    true
   node_A_2       true    true

   cluster_A::>
   ```

3. Vérifier que tous les ports du cluster sont bien :

   `network port show -ipspace Cluster`

```
cluster_A::> network port show -ipspace Cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Vérifier que toutes les LIFs de cluster sont opérationnelles :

   `network interface show -vserver Cluster`

   Chaque LIF de cluster doit afficher « true » pour is Home et avoir un Status Admin/Oper of up/up »

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Vérifiez que la fonction de restauration automatique est activée sur l'ensemble des LIFs du cluster :

   `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Suppression de la configuration des applications de surveillance

Si la configuration existante est contrôlée avec le logiciel MetroCluster Tiebreaker, le médiateur ONTAP ou d'autres applications tierces (par exemple, ClusterLion) qui peuvent lancer un basculement, vous devez supprimer la configuration MetroCluster du logiciel de surveillance avant la mise à niveau.

Étapes

1. Supprimez la configuration MetroCluster existante du logiciel disjoncteur d'attache, du médiateur ou d'autres logiciels pouvant initier le basculement.

Si vous utilisez…	Utilisez cette procédure…
Disjoncteur d'attache	"Suppression des configurations MetroCluster".
Médiateur	Exécutez la commande suivante depuis l'invite ONTAP : `metrocluster configuration-settings mediator remove`
Applications tierces	Reportez-vous à la documentation du produit.

2. Supprimez la configuration MetroCluster existante de toute application tierce pouvant effectuer le basculement.

   Reportez-vous à la documentation de l'application.

Préparation des nouveaux modules de contrôleur

Vous devez préparer les quatre nouveaux nœuds MetroCluster et installer la version correcte de ONTAP.

Description de la tâche

Cette tâche doit être effectuée sur chacun des nouveaux nœuds :

- Node_A_3-New
- Node_A_4-New
- Node_B_3-New
- Node_B_4-New

Dans ces étapes, vous effacez la configuration sur les nœuds et désactivez la zone de la boîte aux lettres sur les nouveaux lecteurs.

Étapes

1. Installez les nouveaux contrôleurs.
2. Reliez les nouveaux nœuds IP MetroCluster aux commutateurs IP, comme indiqué dans la configuration et l'installation de *MetroCluster.*

   "Câblage des commutateurs IP"

3. Configurez les nœuds IP MetroCluster à l'aide des sections suivantes de l'installation et de la configuration *MetroCluster.*
   a. "Collecte des informations requises"
   b. "Restauration des valeurs par défaut du système sur un module de contrôleur"
   c. "Vérification de l'état ha-config des composants"
   d. "Affectation manuelle de lecteurs pour le pool 0 (ONTAP 9.4 et versions ultérieures)"
4. Depuis le mode maintenance, lancer la commande halt pour quitter le mode Maintenance, puis lancer la commande boot_ontap pour démarrer le système et obtenir le setup du cluster.

   Ne terminez pas encore l'assistant de cluster ou l'assistant de nœud pour le moment.

Mettre à niveau les fichiers RCF

Si vous installez un nouveau firmware du commutateur, vous devez installer le micrologiciel du commutateur avant de mettre à niveau le fichier RCF.

Description de la tâche

Cette procédure perturbe le trafic sur le commutateur où le fichier RCF est mis à niveau. Le trafic reprend lorsque le nouveau fichier RCF est appliqué.

Étapes

1. Vérification de l'état de santé de la configuration.
   a. Vérifiez que les composants MetroCluster sont sains :

      ```
      metrocluster check run
      ```

```
cluster_A::*> metrocluster check run
```

L'opération s'exécute en arrière-plan.

b. Après le `metrocluster check run` opération terminée, exécution `metrocluster check show` pour afficher les résultats.

Après environ cinq minutes, les résultats suivants s'affichent :

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id 38
```

b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Préparez les commutateurs IP pour l'application des nouveaux fichiers RCF.

Suivez les étapes pour votre fournisseur de commutateur :

- "Réinitialisation des paramètres d'usine du commutateur IP Broadcom"
- "Réinitialisation des paramètres d'usine du commutateur IP Cisco"

3. Téléchargez et installez le fichier RCF IP, selon votre fournisseur de commutateur.

> Mettre à jour les interrupteurs dans l'ordre suivant : Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

- "Téléchargement et installation des fichiers RCF IP de Broadcom"
- "Téléchargement et installation des fichiers Cisco IP RCF"

Si vous disposez d'une configuration réseau L2 partagée ou L3, il se peut que vous deviez ajuster les ports ISL sur les commutateurs intermédiaire/client. Le mode de port de commutateur peut passer du mode « accès » au mode « réseau ». Ne procédez à la mise à niveau de la deuxième paire de commutateurs (A_2, B_2) que si la connectivité réseau entre les commutateurs A_1 et B_1 est pleinement opérationnelle et que le réseau fonctionne correctement.

Ajout aux clusters des nouveaux nœuds

Vous devez ajouter les quatre nouveaux nœuds IP MetroCluster à la configuration MetroCluster existante.

Description de la tâche

Vous devez effectuer cette tâche sur les deux clusters.

Étapes

1. Ajoutez les nouveaux nœuds IP MetroCluster à la configuration MetroCluster existante.
   a. Associez le premier nouveau nœud IP MetroCluster (node_A_1-New) à la configuration IP MetroCluster existante.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: 172.17.8.93
```

```
172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Associez le second nœud IP MetroCluster (node_A_2-New) à la configuration IP MetroCluster existante.

2. Répétez ces étapes pour joindre le noeud_B_1-New et le noeud_B_2-New à cluster_B.

Configuration des LIFs intercluster, création des interfaces MetroCluster, et mise en miroir des agrégats racines

Vous devez créer des LIF de peering de cluster, créer les interfaces MetroCluster sur les nouveaux nœuds IP MetroCluster.

Description de la tâche

Le port home utilisé dans les exemples est spécifique à la plate-forme. Vous devez utiliser le port d'accueil approprié spécifique à la plate-forme de nœud IP MetroCluster.

Étapes

1. Sur les nouveaux nœuds IP MetroCluster, configurer les LIFs intercluster à l'aide des procédures suivantes :

   "Configuration des LIFs intercluster sur des ports dédiés"

   "Configuration des LIFs intercluster sur des ports data partagés"

2. Sur chaque site, vérifiez que le peering de cluster est configuré :

   ```
   cluster peer show
   ```

   L'exemple suivant montre la configuration de peering de cluster sur cluster_A :

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   L'exemple suivant montre la configuration de peering de cluster sur cluster_B :

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. Créez le groupe DR pour les nœuds IP MetroCluster :

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   Pour plus d'informations sur les paramètres de configuration et les connexions du MetroCluster, reportez-vous aux sections suivantes :

   "Considérations relatives aux configurations MetroCluster IP"

"Création du groupe DR"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Vérifiez que le groupe DR a été créé.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                   Node               DR Partner
Node
----------- ------------------------- ------------------
------------------
1           cluster_A
                                      node_A_1-old        node_B_1-old
                                      node_A_2-old        node_B_2-old
            cluster_B
                                      node_B_1-old        node_A_1-old
                                      node_B_2-old        node_A_2-old
2           cluster_A
                                      node_A_1-new        node_B_1-new
                                      node_A_2-new        node_B_2-new
            cluster_B
                                      node_B_1-new        node_A_1-new
                                      node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Configurez les interfaces IP MetroCluster pour les nœuds IP MetroCluster nouvellement rejoints :

   `metrocluster configuration-settings interface create -cluster-name`

- Certaines plates-formes utilisent un VLAN pour l'interface IP de MetroCluster. Par défaut, chacun des deux ports utilise un VLAN différent : 10 et 20. Vous pouvez également spécifier un VLAN différent (non par défaut) supérieur à 100 (entre 101 et 4095) à l'aide du `-vlan-id parameter` dans le `metrocluster configuration-settings interface create` commande.
- À partir de ONTAP 9.9.1, si vous utilisez une configuration de couche 3, vous devez également spécifier le `-gateway` Paramètre lors de la création des interfaces IP MetroCluster. Reportez-vous à la section "Considérations relatives aux réseaux étendus de couche 3".

Les modèles de plateforme suivants peuvent être ajoutés à la configuration MetroCluster existante si les VLAN utilisés sont de 10/20 ou plus de 100. Si d'autres VLAN sont utilisés, ces plateformes ne peuvent pas être ajoutées à la configuration existante car l'interface MetroCluster ne peut pas être configurée. Si vous utilisez une autre plate-forme, la configuration VLAN n'est pas pertinente car elle n'est pas requise dans ONTAP.

Plateformes AFF	Plateformes FAS
• AVEC AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

Vous pouvez configurer les interfaces IP MetroCluster depuis n'importe quel cluster.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Vérifiez que les interfaces IP MetroCluster sont créées :

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                 Home Port: e1a
                      172.17.28.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                 Home Port: e1a
                      172.17.28.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                 Home Port: e1a
                      172.17.28.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Connectez les interfaces IP MetroCluster :

   `metrocluster configuration-settings connection connect`

   Cette commande peut prendre plusieurs minutes.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Vérifiez que les connexions sont correctement établies : `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                    172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                    172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                    172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.10    DR Auxiliary
completed
            node_B_1-new
                Home Port: e1a
                    172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                    172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                    172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Vérifiez l'affectation automatique et le partitionnement des disques :

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0                546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3                546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5                546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6                546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7                546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10               546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Mettez en miroir les agrégats racine :

`storage aggregate mirror -aggregate aggr0_node_A_1-new`

Cette étape doit être effectuée sur chaque nœud IP MetroCluster.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Vérifier que les agrégats racine sont mis en miroir :

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Finalisation de l’ajout des nouveaux nœuds

Vous devez intégrer le nouveau groupe de reprise après incident à la configuration MetroCluster et créer des agrégats de données en miroir sur les nouveaux nœuds.

Étapes

1. Actualisez la configuration MetroCluster :

   a. Entrer en mode de privilège avancé :

      ```
      set -privilege advanced
      ```

   b. Actualisez la configuration MetroCluster sur l’un des nouveaux nœuds :

```
metrocluster configure
```

L'exemple suivant montre la configuration MetroCluster mise à jour sur les deux groupes de reprise sur incident :

```
cluster_A::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

a. Revenir en mode de privilège admin :

```
set -privilege admin
```

2. Créez des agrégats de données en miroir sur chacun des nouveaux nœuds MetroCluster :

`storage aggregate create -aggregate` *`aggregate-name`* `-node` *`node-name`* `-diskcount` *`no-of-disks`* `-mirror true`

> Vous devez créer au moins un agrégat de données en miroir par site. Il est recommandé d'avoir deux agrégats de données en miroir par site sur des nœuds IP MetroCluster pour héberger les volumes MDV. Cependant, un seul agrégat par site est pris en charge (mais non recommandé). Il est possible qu'un site de MetroCluster dispose d'un seul agrégat de données en miroir et que l'autre site dispose de plusieurs agrégats de données en miroir.

L'exemple suivant montre la création d'un agrégat du node_A_1-New.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
```

```
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. Vérifiez que les nœuds sont ajoutés à leur groupe de reprise après incident.

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Déplacez les volumes MDV_CRS des anciens nœuds vers les nouveaux nœuds du privilège avancé.

   a. Afficher les volumes pour identifier les volumes MDV :

      Si vous disposez d'un seul agrégat de données en miroir par site, déplacez les deux volumes MDV vers cet agrégat unique. Si vous disposez de deux agrégats de données en miroir ou plus, déplacez chaque volume MDV vers un agrégat différent.

      L'exemple suivant montre les volumes MDV dans `volume show` résultat :

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Définissez le niveau de privilège avancé :

```
set -privilege advanced
```

c. Déplacer les volumes MDV, un par un :

```
volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name
```

L'exemple suivant montre la commande et la sortie pour le déplacement de "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" vers "Data_a3" sur "node_A_3".

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Utilisez la commande volume show pour vérifier que le volume MDV a bien été déplacé :

   `volume show mdv-name`

   Le résultat suivant indique que le volume MDV a été déplacé avec succès.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

5. Déplacement d'epsilon d'un ancien nœud vers un nouveau nœud :

   a. Identifier le nœud qui possède actuellement epsilon :

      `cluster show -fields epsilon`

```
cluster_B::*> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Définir epsilon sur false sur l'ancien nœud (node_A_1-Old) :

   `cluster modify -node old-node -epsilon false*`

c. Défini sur true sur le nouveau nœud (node_A_3-New) :

   `cluster modify -node new-node -epsilon true`

d. Vérifier que epsilon a déplacé vers le nœud approprié :

   `cluster show -fields epsilon`

```
cluster_A::*> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

Suppression d'un groupe de reprise après incident

Depuis ONTAP 9.8, vous pouvez supprimer un groupe de reprise après incident d'une configuration MetroCluster à huit nœuds pour créer une configuration MetroCluster à quatre nœuds.

Cette procédure est prise en charge sur ONTAP 9.8 et versions ultérieures. Pour les systèmes qui exécutent ONTAP 9.7 ou une version antérieure, consultez l'article de la base de connaissances

"Comment supprimer un groupe de reprise sur incident d'une configuration MetroCluster"

"Support NetApp"

Une configuration à huit nœuds comprend huit nœuds organisés sous forme de deux groupes de reprise après incident à quatre nœuds.

En supprimant un groupe de reprise sur incident, quatre nœuds restent dans la configuration.

Suppression des nœuds du groupe DR de chaque cluster

Avant de commencer

- Vous devez effectuer cette étape sur les deux clusters.
- Le `metrocluster remove-dr-group` La commande n'est prise en charge que sur ONTAP 9.8 et les versions ultérieures.

Étapes

1. Préparer la suppression du groupe de reprise après incident, si ce n'est pas déjà le cas.

   a. Déplacez tous les volumes de données vers un autre groupe de reprise après incident.

   b. Si le groupe de reprise après incident à supprimer contient des volumes en miroir de partage de charge, ils ne peuvent pas être déplacés. Recréez tous les volumes en miroir de partage de charge dans un autre groupe DR, puis supprimez les volumes en miroir de partage de charge dans le groupe DR à supprimer.

   c. Déplacez tous les volumes de métadonnées MDV_CRS vers un autre groupe DR en suivant la procédure "Déplacement d'un volume de métadonnées dans les configurations MetroCluster" procédure.

   d. Supprimez tous les volumes de métadonnées MDV_aud qui peuvent exister dans le groupe DR à supprimer.

   e. Supprimez tous les agrégats de données du groupe de reprise sur incident à supprimer comme indiqué dans l'exemple suivant :

   ```
   ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
   -fields aggregate ,node
   ClusterA::> aggr delete -aggregate aggregate_name
   ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
   -fields aggregate ,node
   ClusterB::> aggr delete -aggregate aggregate_name
   ```

   Les agrégats racine ne sont pas supprimés.

   f. Déplacez les LIF de données hors ligne. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin down`

   g. Migrez toutes les LIFs de données vers les nœuds d'un autre groupe de reprise après incident. `network interface show -home-node` *`old_node`*

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-node` *`new_node`* `-home-port` *`port-id`*

   h. Remettez en ligne les LIF de données. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin up`

   i. Migrez la LIF de gestion de cluster vers un nœud de rattachement situé dans un autre groupe de reprise après incident.

```
network interface show -role cluster-mgmt

network interface modify -vserver svm-name -lif cluster_mgmt -home-node
new_node -home-port port-id
```

La gestion des nœuds et les LIF inter-cluster ne sont pas migrées.

a. Transférer epsilon vers un nœud dans un autre groupe de reprise après incident si nécessaire.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identifier et supprimer le groupe de reprise sur incident.

a. Identifiez le groupe DR approprié pour la suppression :

```
metrocluster node show
```

b. Supprimer les nœuds du groupe DR :
`metrocluster remove-dr-group -dr-group-id 1`

L'exemple suivant montre la suppression de la configuration du groupe de reprise sur incident sur cluster_A.

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B"to remove the remote nodes in the DR
group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not completed
on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Répétez l'étape précédente sur le cluster partenaire.
4. Si dans une configuration MetroCluster IP, supprimer les connexions MetroCluster sur les nœuds de l'ancien groupe DR.

   Ces commandes peuvent être émises depuis un cluster et s'appliquer à tout le groupe de reprise sur incident sur les deux clusters.

   a. Débrancher les connexions :

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Supprimez les interfaces MetroCluster sur les nœuds de l'ancien groupe DR :

```
metrocluster configuration-settings interface delete
```

c. Supprimez l'ancienne configuration du groupe DR.
`metrocluster configuration-settings dr-group delete`

5. Dissocier les nœuds de l'ancien groupe DR.

Vous devez effectuer cette étape sur chaque cluster.

a. Définissez le niveau de privilège avancé :

```
set -privilege advanced
```

b. Désactiver le basculement du stockage :

```
storage failover modify -node node-name -enable false
```

c. Dissocier le nœud :
`cluster unjoin -node node-name`

Répétez cette étape pour l'autre nœud local de l'ancien groupe DR.

d. Définissez le niveau de privilège admin :
`set -privilege admin`

6. Réactiver la haute disponibilité du cluster dans le nouveau groupe de reprise après incident :

```
cluster ha modify -configured true
```

Vous devez effectuer cette étape sur chaque cluster.

7. Arrêtez, mettez hors tension et retirez les anciens modules de contrôleur et tiroirs de stockage.

Où trouver des informations complémentaires

Pour en savoir plus sur la configuration et le fonctionnement de MetroCluster,

MetroCluster et informations diverses

Informations	Objet
"Documentation MetroCluster"	• Toutes les informations relatives aux MetroCluster

"Installation et configuration de la solution Fabric-Attached MetroCluster"	• Architecture Fabric-Attached MetroCluster • Câblage de la configuration • Configuration des ponts FC-SAS • Configuration des commutateurs FC • Configuration de MetroCluster dans ONTAP
"Installation et configuration d'Stretch MetroCluster"	• Architecture MetroCluster extensible • Câblage de la configuration • Configuration des ponts FC-SAS • Configuration de MetroCluster dans ONTAP
"Gestion et reprise après incident MetroCluster"	• Présentation de la configuration MetroCluster • Basculement, rétablissement et rétablissement • Reprise après incident
"Gérer les composants MetroCluster"	• Instructions relatives à la maintenance dans une configuration MetroCluster FC • Procédure de remplacement ou de mise à niveau du matériel et de mise à niveau du firmware pour les ponts FC-SAS et les commutateurs FC • Ajout à chaud d'un tiroir disque dans une configuration FC MetroCluster étendue ou FAS • Retrait à chaud d'un tiroir disque dans une configuration FC MetroCluster étendue ou FAS • Remplacement du matériel sur un site d'incident dans une configuration MetroCluster FC Stretch ou Fabric-Attached • Extension d'une configuration MetroCluster FC extensible ou Fabric-Attached à deux nœuds à une configuration MetroCluster à quatre nœuds. • Extension d'une configuration MetroCluster FC à quatre nœuds (Fabric-Attached ou Stretch FC) à une configuration MetroCluster FC à huit nœuds.
"Mise à niveau, transition et extension de MetroCluster"	• Mise à niveau ou actualisation d'une configuration MetroCluster • Passer d'une configuration MetroCluster FC à une configuration MetroCluster IP • Extension d'une configuration MetroCluster par l'ajout de nœuds supplémentaires
"Installation et configuration du logiciel MetroCluster Tiebreaker"	• Contrôle de la configuration de MetroCluster avec le logiciel MetroCluster Tiebreaker

"Documentation des systèmes matériels ONTAP" Les procédures standard de maintenance des tiroirs de stockage sont compatibles avec les configurations MetroCluster IP.	• Ajout à chaud d'un tiroir disque • Retrait à chaud d'un tiroir disque
"Transition basée sur la copie"	• Transition des données depuis les systèmes de stockage 7-mode vers les systèmes de stockage en cluster
"Concepts relatifs à ONTAP"	• Fonctionnement des agrégats en miroir

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 DÉLICTUELLE (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.