Installez une configuration MetroCluster IP

ONTAP MetroCluster

NetApp
February 20, 2026

Sommaire

Installez une configuration MetroCluster IP

Flux de travail d'installation IP MetroCluster

Pour installer votre configuration MetroCluster IP, vous devez effectuer un certain nombre de procédures dans le bon ordre.

- "Préparation de l'installation et compréhension de toutes les exigences".
- "Brancher les composants"
- "Configurez le logiciel"
- "Configurez ONTAP médiateur" (en option)
- "Tester la configuration"

La préparation de l'installation de MetroCluster

Matrice de prise en charge des configurations ONTAP MetroCluster

Les différentes configurations MetroCluster présentent des différences clés au niveau des composants requis.

Dans toutes les configurations, chacun des deux sites MetroCluster est configuré en tant que cluster ONTAP. Dans une configuration MetroCluster à deux nœuds, chaque nœud est configuré en tant que cluster à un seul nœud.

Fonction	Configurations IP	Configurations intégrées à la structure		Configurations Stretch	
		Quatre ou huit noeuds	**Deux nœuds**	**Connexion pont à deux noeuds**	**Connexion directe à deux nœuds**
Nombre de contrôleurs	Quatre ou huit[1]	Quatre ou huit	Deux	Deux	Deux
Utilise une structure de stockage avec commutateur FC	Non	Oui.	Oui.	Non	Non
Utilise une structure de stockage avec commutateurs IP	Oui.	Non	Non	Non	Non
Utilise des ponts FC-SAS	Non	Oui.	Oui.	Oui.	Non

Utilise un stockage SAS direct	Oui (local uniquement)	Non	Non	Non	Oui.
Prend en charge ADP	Oui (à partir de ONTAP 9.4)	Non	Non	Non	Non
Prend en charge la haute disponibilité locale	Oui.	Oui.	Non	Non	Non
Prise en charge du basculement automatique non planifié avec ONTAP	Non	Oui.	Oui.	Oui.	Oui.
Prend en charge les agrégats sans miroir	Oui (à partir de ONTAP 9.8)	Oui.	Oui.	Oui.	Oui.
Prend en charge le médiateur ONTAP	Oui (à partir de ONTAP 9.7)	Non	Non	Non	Non
Prise en charge d'MetroCluster Tiebreaker	Oui (pas en combinaison avec le médiateur ONTAP)	Oui.	Oui.	Oui.	Oui.
Supports Toutes les baies SAN	Oui.	Oui.	Oui.	Oui.	Oui.

Notes

1. Vérifiez les points suivants pour les configurations IP MetroCluster à 8 nœuds :
    - Les configurations à huit nœuds sont prises en charge à partir de ONTAP 9.9.1.
    - Seuls les commutateurs MetroCluster validés par NetApp (commandés auprès de NetApp) sont pris en charge.
    - Les configurations utilisant des connexions back-end routées par IP (couche 3) ne sont pas prises en charge.

Prise en charge de toutes les baies SAN dans les configurations MetroCluster

Certaines baies SAN (ASAS) sont prises en charge dans les configurations MetroCluster. Dans la documentation MetroCluster, les informations relatives aux modèles AFF s'appliquent au système ASA correspondant. Par exemple, tous les câbles et autres informations du système AFF A400 s'appliquent également au système ASA AFF A400.

Les configurations de plateforme prises en charge sont répertoriées dans le "NetApp Hardware Universe".

Différences entre le médiateur ONTAP et le logiciel MetroCluster Tiebreaker

Depuis ONTAP 9.7, vous pouvez utiliser le basculement automatique non planifié assisté par médiateur ONTAP dans la configuration IP MetroCluster ou le logiciel MetroCluster Tiebreaker. Il n'est pas nécessaire d'utiliser le logiciel MAUSO ou Tiebreaker ; cependant, si vous choisissez de ne pas utiliser l'un de ces services, vous devez le faire "effectuer une récupération manuelle" en cas d'incident.

Les différentes configurations MetroCluster effectuent un basculement automatique dans plusieurs cas :

- **Configurations FC MetroCluster utilisant la capacité AUSO (non présentes dans les configurations IP MetroCluster)**

  Dans ces configurations, AUSO est lancé en cas de défaillance des contrôleurs, mais le stockage (et les ponts, le cas échéant) reste opérationnel.

- **Configurations IP MetroCluster utilisant ONTAP Mediator (ONTAP 9.7 et versions ultérieures)**

  Dans ces configurations, MAUSO est lancé dans les mêmes circonstances que AUSO, comme décrit ci-dessus, ainsi qu'après une panne complète du site (contrôleurs, stockage et commutateurs).

  "Découvrez comment le médiateur ONTAP prend en charge le basculement automatique non planifié".

- **Configurations IP ou FC MetroCluster utilisant le logiciel disjoncteur d'attache en mode actif**

  Dans ces configurations, il procède au basculement non planifié après une défaillance complète du site.

  Avant d'utiliser le logiciel disjoncteur d'attache, passez en revue "Installation et configuration du logiciel MetroCluster Tiebreaker"

Interopérabilité du médiateur ONTAP avec d'autres applications et appareils

Vous ne pouvez pas utiliser d'applications ou d'appliances tierces pouvant déclencher un basculement en combinaison avec le médiateur ONTAP. En outre, la surveillance d'une configuration MetroCluster avec le logiciel MetroCluster Tiebreaker n'est pas prise en charge avec le programme ONTAP Mediator.

En savoir plus sur le stockage à distance et les configurations IP de MetroCluster

Vous devez comprendre comment les contrôleurs accèdent au stockage distant et comment fonctionnent les adresses IP de MetroCluster.

Accès au stockage distant dans les configurations IP MetroCluster

Dans les configurations IP MetroCluster, seuls les contrôleurs locaux peuvent atteindre les pools de stockage distants sont accessibles via les contrôleurs distants. Les commutateurs IP sont connectés aux ports Ethernet des contrôleurs ; ils ne disposent pas de connexions directes aux tiroirs disques. Si la télécommande est en panne, les contrôleurs locaux ne peuvent pas atteindre leurs pools de stockage distants.

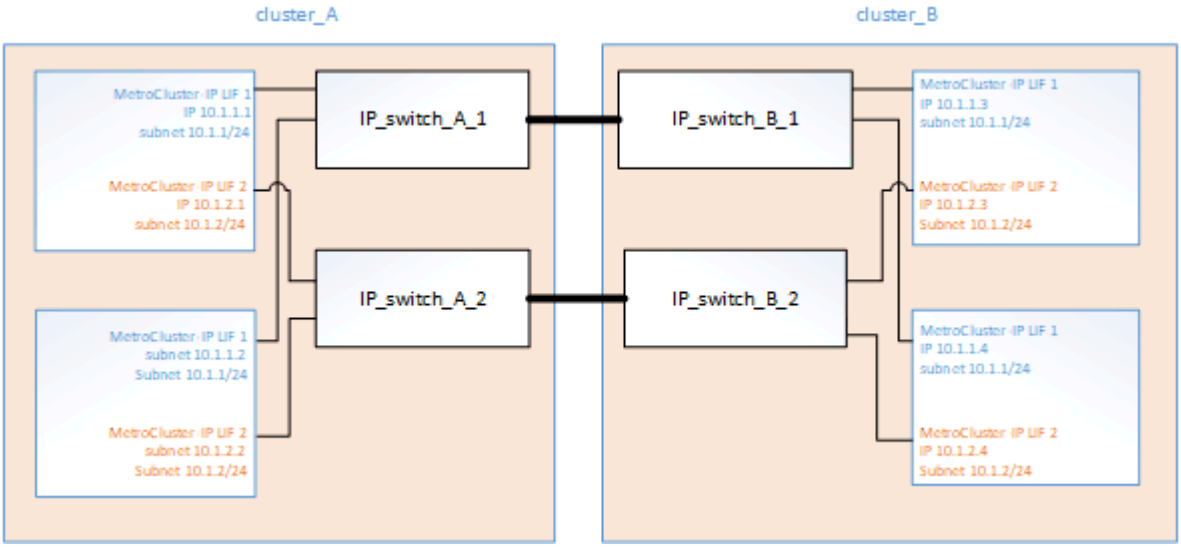
Elle est différente des configurations FC de MetroCluster, dans lesquelles les pools de stockage distants sont connectés aux contrôleurs locaux via la structure FC ou les connexions SAS. Les contrôleurs locaux ont

toujours accès au stockage distant même si les contrôleurs distants sont en panne.

Adresses IP de MetroCluster

Il est important de connaître la mise en œuvre des interfaces et des adresses IP MetroCluster dans une configuration IP MetroCluster, ainsi que les exigences associées.

Dans une configuration MetroCluster IP, la réplication du stockage et du cache non volatile entre les paires haute disponibilité et les partenaires de reprise après incident s'effectue sur des liaisons dédiées à large bande passante dans la structure MetroCluster IP. Les connexions iSCSI sont utilisées pour la réplication du stockage. Ils sont également utilisés pour l'ensemble du trafic intra-cluster au sein des clusters locaux. Le trafic MetroCluster est conservé séparé du trafic intra-cluster à l'aide de sous-réseaux IP et de VLAN séparés. La structure IP de MetroCluster est distincte et différente du réseau de peering de cluster.



La configuration MetroCluster IP nécessite deux adresses IP sur chaque nœud réservé pour la structure IP MetroCluster back-end. Les adresses IP réservées sont attribuées aux interfaces logiques MetroCluster IP (LIF) lors de la configuration initiale et présentent les exigences suivantes :

> Vous devez soigneusement choisir les adresses IP de MetroCluster, car vous ne pouvez pas les modifier après la configuration initiale.

- Ils doivent se trouver dans une plage IP unique.

  Ils ne doivent pas se chevaucher avec un espace IP dans l'environnement.

- Ils doivent résider dans l'un des deux sous-réseaux IP qui les séparent de tout autre trafic.

Ainsi, les nœuds peuvent être configurés avec les adresses IP suivantes :

Nœud	Interface	Adresse IP	Sous-réseau
Nœud_A_1	Interface IP MetroCluster 1	10.1.1.1	10.1.1/24
Nœud_A_1	Interface IP MetroCluster 2	10.1.2.1	10.1.2/24

Nœud_A_2	Interface IP MetroCluster 1	10.1.1.2	10.1.1/24
Nœud_A_2	Interface IP MetroCluster 2	10.1.2.2	10.1.2/24
Nœud_B_1	Interface IP MetroCluster 1	10.1.1.3	10.1.1/24
Nœud_B_1	Interface IP MetroCluster 2	10.1.2.3	10.1.2/24
Nœud_B_2	Interface IP MetroCluster 1	10.1.1.4	10.1.1/24
Nœud_B_2	Interface IP MetroCluster 2	10.1.2.4	10.1.2/24

Caractéristiques des interfaces IP MetroCluster

Les interfaces IP de MetroCluster sont spécifiques aux configurations IP de MetroCluster. Leurs caractéristiques sont différentes des autres types d'interfaces ONTAP :

- Ils sont créés par le `metrocluster configuration-settings interface create` Dans le cadre de la configuration initiale de MetroCluster.

  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".

  Ils ne sont pas créés ou modifiés par les commandes de l'interface réseau.

- Ils n'apparaissent pas dans la sortie du `network interface show` commande.
- Ils ne basculent pas, mais restent associés au port sur lequel ils ont été créés.
- Les configurations IP MetroCluster utilisent des ports Ethernet spécifiques (selon la plateforme) pour les interfaces IP MetroCluster.

  N'utilisez pas d'adresses IP 169.254.17.x ou 169.254.18.x lorsque vous créez des interfaces IP MetroCluster pour éviter les conflits avec les adresses IP d'interface générées automatiquement par le système dans la même plage.

Exigences IP de MetroCluster pour l'attribution automatique des lecteurs et les systèmes ADP

Depuis ONTAP 9.4, les configurations IP de MetroCluster prennent en charge les nouvelles installations à l'aide d'un partitionnement de disque avancé et d'une affectation automatique des disques.

Lors de l'utilisation d'ADP avec des configurations IP MetroCluster , il convient de tenir compte des points suivants :

- ONTAP 9.4 et versions ultérieures sont nécessaires pour utiliser ADP avec les configurations IP MetroCluster sur les systèmes AFF et ASA.
- ADPv2 est pris en charge dans les configurations MetroCluster IP.
- L'agrégat racine doit se trouver dans la partition 3 pour tous les noeuds des deux sites.
- Le partitionnement et l'affectation des disques s'effectuent automatiquement lors de la configuration initiale des sites MetroCluster.
- Les affectations de disque du pool 0 sont effectuées en usine.
- La racine non symétrisée est créée à l'usine.
- L'affectation de la partition des données se fait sur le site du client pendant la procédure de configuration.
- Dans la plupart des cas, l'affectation des disques et le partitionnement sont effectués automatiquement pendant les procédures de configuration.
- Un disque et toutes ses partitions doivent être la propriété de nœuds d'une même paire haute disponibilité. La propriété de partition ou de disque au sein d'un seul disque ne peut pas être mélangée entre la paire haute disponibilité locale et le partenaire de reprise après incident ou le partenaire auxiliaire de reprise après incident.

  Exemple de configuration prise en charge :

Lecteur/partition	Propriétaire
Lecteur :	`ClusterA-Node01`
Partition 1 :	`ClusterA-Node01`
Partition 2 :	`ClusterA-Node02`
Partition 3 :	`ClusterA-Node01`

Lors de la mise à niveau de ONTAP 9.4 vers 9.5, le système reconnaît les affectations de disques existantes.

Partitionnement automatique

ADP est exécuté automatiquement lors de la configuration initiale du système.

Depuis ONTAP 9.5, l'assignation automatique des disques doit être activée avec `storage disk option modify -autoassign on` commande.

Vous devez définir l'état ha-config sur `mccip` avant le provisionnement automatique, assurez-vous que les tailles de partition correctes sont sélectionnées pour permettre une taille de volume racine appropriée. Pour plus d'informations, voir "Vérification de l'état ha-config des composants".

Vous pouvez partitionner automatiquement un maximum de 96 disques lors de l'installation. Vous pouvez ajouter des lecteurs supplémentaires après l'installation initiale.

Si vous utilisez des lecteurs internes et externes, vous devez d'abord initialiser le MetroCluster avec uniquement les lecteurs internes utilisant ADP. Vous connectez ensuite manuellement le tiroir externe une fois l'installation ou la configuration terminée.

Vous devez vous assurer que les tiroirs internes disposent du nombre minimal de disques recommandé, comme indiqué dans la Différences d'affectation des disques et ADP par système.

Pour les disques internes et externes, vous devez remplir les tiroirs partiellement pleins comme décrit dans la section Comment remplir les étagères partiellement pleines.

Fonctionnement de l'affectation automatique « tiroir par tiroir »

Si chaque site est doté de quatre tiroirs externes, chaque tiroir est affecté à un nœud différent et à un pool différent, comme illustré ci-dessous :

- Tous les disques du site_A-shelf_1 sont automatiquement affectés au pool 0 du nœud_A_1
- Tous les disques du site_A-shelf_3 sont automatiquement affectés au pool 0 du nœud_A_2
- Tous les disques du site_B-shelf_1 sont automatiquement affectés au pool 0 du nœud_B_1
- Tous les disques du site_B-shelf_3 sont automatiquement affectés au pool 0 du nœud_B_2
- Tous les disques du site_B-shelf_2 sont automatiquement affectés au pool 1 du nœud_A_1
- Tous les disques du site_B-shelf_4 sont automatiquement affectés au pool 1 du nœud_A_2
- Tous les disques du site_A-shelf_2 sont automatiquement affectés au pool 1 du nœud_B_1
- Tous les disques du site_A-shelf_4 sont automatiquement affectés au pool 1 du nœud_B_2

Comment remplir les étagères partiellement pleines

Si votre configuration utilise des tiroirs qui ne sont pas plein (possèdent des baies de disques vides), il faut distribuer les disques de façon homogène dans tout le tiroir, selon les règles d'affectation des disques. La règle d'affectation des disques dépend du nombre de tiroirs sur chaque site MetroCluster.

Si vous utilisez un seul tiroir sur chaque site (ou uniquement le tiroir interne d'un système AFF A800), les disques sont attribués selon une politique de tiroir par trimestre. Si le tiroir n'est pas entièrement rempli, installez les disques de la même manière sur tous les trimestres.

Le tableau suivant montre un exemple de placement de 24 disques dans un tiroir interne de 48 disques. La propriété des disques est également indiquée.

Les baies de 48 disques sont divisées en quatre trimestres :	Installez six disques sur les six premières baies de chaque trimestre…
Premier trimestre : baies 0-11	Baies 0-5
Deuxième trimestre : baies 12-23	Baies 12-17
Trimestre 3 : baies 24-35	Baies 24-29
Trimestre 4 : baies 36-47	Baies 36-41

Le tableau ci-dessous présente un exemple de placement de 16 disques dans un tiroir interne de 24 disques.

Les 24 baies de disque sont divisées en quatre trimestres :	Installez quatre disques dans les quatre premières baies de chaque trimestre…
1er trimestre : baies 0-5	Baies 0-3
Deuxième trimestre : baies 6-11	Baies 6-9
Trimestre 3 : baies 12-17	Baies 12-15
Trimestre 4 : baies 18-23	Baies 18-21

Si vous utilisez deux tiroirs externes sur chaque site, les disques sont attribués selon une règle de demi-tiroir. Si les tiroirs ne sont pas entièrement remplis, installez les disques de la même manière à partir de l'une des extrémités du tiroir.

Par exemple, si vous installez 12 disques dans un tiroir de 24 disques, installez les disques dans les baies 0-5 et 18-23.

Affectation manuelle des lecteurs (ONTAP 9.5)

Dans ONTAP 9.5, il est nécessaire d'effectuer manuellement l'affectation des disques sur les systèmes dotés des configurations de tiroirs suivantes :

- Trois tiroirs externes par site.

  Deux tiroirs sont attribués automatiquement selon une règle d'affectation demi-tiroir, mais le troisième doit être attribué manuellement.

- Plus de quatre tiroirs par site et le nombre total de tiroirs externes n'est pas un multiple de quatre.

  Les tiroirs supplémentaires au-dessus du multiple de quatre le plus proche ne sont pas attribués et les disques doivent être attribués manuellement. Par exemple, si le site comprend cinq tiroirs externes, vous devez attribuer manuellement le tiroir cinq.

Vous n'avez qu'à attribuer manuellement un seul disque sur chaque tiroir non attribué. Les autres disques du tiroir sont ensuite attribués automatiquement.

Affectation manuelle des lecteurs (ONTAP 9.4)

Dans ONTAP 9.4, il est nécessaire d'effectuer manuellement l'affectation des disques sur les systèmes dotés des configurations de tiroirs suivantes :

- Moins de quatre tiroirs externes par site.

  Les disques doivent être affectés manuellement pour assurer une affectation symétrique des disques, chaque pool ayant un nombre égal de disques.

- Plus de quatre tiroirs externes par site et le nombre total de tiroirs externes n'est pas un multiple de quatre.

  Les tiroirs supplémentaires au-dessus du multiple de quatre le plus proche ne sont pas attribués et les disques doivent être attribués manuellement.

Lors de l'attribution manuelle de disques, vous devez affecter des disques de manière symétrique, avec un nombre égal de disques affectés à chaque pool. Par exemple, si la configuration compte deux tiroirs de stockage sur chaque site, un tiroir pour la paire haute disponibilité locale et un tiroir pour la paire haute disponibilité distante :

- Assigner la moitié des disques du site_A-shelf_1 au pool 0 du noeud_A_1.
- Assigner la moitié des disques du site_A-shelf_1 au pool 0 du noeud_A_2.
- Assigner la moitié des disques du site_A-shelf_2 au pool 1 du nœud_B_1.
- Assigner la moitié des disques du site_A-shelf_2 au pool 1 du nœud_B_2.
- Affecter la moitié des disques du site_B-shelf_1 au pool 0 du nœud_B_1.
- Affecter la moitié des disques du site_B-shelf_1 au pool 0 du nœud_B_2.
- Assigner la moitié des disques du site_B-shelf_2 au pool 1 du nœud_A_1.
- Assigner la moitié des disques du site_B-shelf_2 au pool 1 du nœud_A_2.

Ajout de tiroirs à une configuration existante

L'assignation automatique des disques prend en charge l'ajout symétrique des tiroirs à une configuration existante.

Lorsque de nouveaux tiroirs sont ajoutés, le système applique la même règle d'affectation aux nouveaux tiroirs. Par exemple, avec un seul tiroir par site, si un tiroir supplémentaire est ajouté, les systèmes appliquent les règles d'affectation de tiroir de trimestre au nouveau tiroir.

Informations associées

"Composants IP MetroCluster et conventions de nom requis"

"Gestion des disques et des agrégats"

Les différences d'affectation des disques et des disques ADP par système dans les configurations IP MetroCluster

Le fonctionnement du partitionnement de disque avancé et de l'affectation automatique des disques dans les configurations IP MetroCluster varie en fonction du modèle du système.

> 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. L'agrégat racine est créé à l'aide de partitions P3.

Veuillez prendre connaissance des exigences suivantes avant d'utiliser les tableaux :

- Vous devez respecter les limites de MetroCluster concernant le nombre maximal de disques pris en charge et les autres directives. Reportez-vous à la "NetApp Hardware Universe" .
- Si vous réutilisez un rack de disque externe, vérifiez que la propriété du disque sur le rack a été supprimée avant de le connecter au contrôleur. Se référer à"Supprimer la propriété ONTAP d'un disque" .

Affectation d'un disque ou d'un disque ADP sur les systèmes AFF A320

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Un tiroir est utilisé par la paire haute disponibilité locale. Le second tiroir est utilisé par la paire haute disponibilité distante. Les partitions sur chaque tiroir sont utilisées pour créer l'agrégat racine. Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	24 disques	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Affectation des disques et ADP sur les systèmes AFF A150, ASA A150 et AFF A220

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	Disques internes uniquement	Les disques internes sont répartis en quatre groupes identiques. Chaque groupe est automatiquement affecté à un pool distinct et chaque pool est affecté à un contrôleur distinct dans la configuration. **Remarque :** la moitié des lecteurs internes restent non affectés avant la configuration de MetroCluster.	Deux trimestres sont utilisés par la paire haute disponibilité locale. Les deux autres trimestres sont utilisés par la paire haute disponibilité distante. L'agrégat racine inclut les partitions suivantes dans chaque plex : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Nombre minimal de disques pris en charge (par site)	16 disques internes	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct. Deux trimestres d'un shelf peuvent avoir le même pool. Le pool est choisi en fonction du nœud propriétaire du trimestre : • Si le noeud local est détenu par le noeud local, pool0 est utilisé. • Si le nœud distant est propriétaire, pool1 est utilisé. Par exemple : un tiroir de Q1 à Q4 peut avoir les attributions suivantes : • Q1 : pool0 nœud_A_1 • Q2 : pool0 nœud_A_2 • Q3 : node_B_1 pool1 • Q4 :node_B_2 pool1 **Remarque :** la moitié des lecteurs internes restent non affectés avant la configuration de MetroCluster.	Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Deux partitions de données • Deux partitions de parité • Pas de pièces de rechange

Affectation des disques et de l'ADP sur les systèmes AFF A250, AFF C250, ASA A250, ASA C250, FAS500f, AFF A20, AFF A30 et AFF C30

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques (disques externes uniquement, pas de disques internes)	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Un tiroir est utilisé par la paire haute disponibilité locale. Le second tiroir est utilisé par la paire haute disponibilité distante. Les partitions sur chaque tiroir sont utilisées pour créer l'agrégat racine. L'agrégat racine inclut les partitions suivantes dans chaque plex : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
	48 disques (disques externes et internes)	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct. Les disques des tiroirs externes sont divisés en quatre groupes égaux (trimestres). Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	16 disques internes	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Deux partitions de données • Deux partitions de parité • Pas de partitions de rechange

ADP et affectation des disques sur les systèmes AFF A50 et AFF C60

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques (disques externes uniquement, pas de disques internes)	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	La paire haute disponibilité locale utilise un tiroir. La paire haute disponibilité distante utilise le second tiroir. Les partitions sur chaque tiroir sont utilisées pour créer l'agrégat racine. L'agrégat racine inclut les partitions suivantes dans chaque plex : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
	48 disques (disques externes et internes)	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct. Les disques des tiroirs externes sont divisés en quatre groupes égaux (trimestres). Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	24 disques internes	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Deux partitions de données • Deux partitions de parité • Pas de partitions de rechange

Affectation des disques et ADP sur les systèmes AFF A300

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Un tiroir est utilisé par la paire haute disponibilité locale. Le second tiroir est utilisé par la paire haute disponibilité distante. Les partitions sur chaque tiroir sont utilisées pour créer l'agrégat racine. L'agrégat racine inclut les partitions suivantes dans chaque plex : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	24 disques	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut les partitions suivantes : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Affectation des disques et des données sur les systèmes AFF C400, AFF A400, ASA C400 et ASA A400

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	96 disques	Les disques sont automatiquement affectés selon le type tiroir par tiroir.	Chacun des deux plexes de l'agrégat racine inclut : • 20 partitions de données • Deux partitions de parité • Deux partitions de rechange

Nombre minimal de disques pris en charge (par site)	24 disques	Les disques sont divisés en quatre groupes égaux (quarts). Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Affectation des disques et ADP sur les systèmes AFF A700

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	96 disques	Les disques sont automatiquement affectés selon le type tiroir par tiroir.	Chacun des deux plexes de l'agrégat racine inclut : • 20 partitions de données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	24 disques	Les disques sont divisés en quatre groupes égaux (quarts). Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

ADP et affectation des disques sur les systèmes AFF C800, ASA C800, ASA A800 et AFF A800

Directive	Nombre de disques par site	Règles d'affectation de disques	Disposition ADP pour l'agrégat racine

Minimum de disques recommandés (par site)	Disques internes et 96 disques externes	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct. Les disques des tiroirs externes sont automatiquement affectés selon le tiroir par tiroir, tous les disques de chaque tiroir étant affectés à l'un des quatre nœuds de la configuration MetroCluster.	Chacun des deux plexes de l'agrégat racine inclut : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange **Note:** l'agrégat racine est créé avec 12 partitions racine sur le shelf interne.
Nombre minimal de disques pris en charge (par site)	24 disques internes	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Trois partitions de données • Deux partitions de parité • Une partition de rechange **Note:** l'agrégat racine est créé avec 12 partitions racine sur le shelf interne.

Affectation des disques et des ADP sur les systèmes AFF A70, AFF A90 et AFF C80

Directive	Nombre de disques par site	Règles d'affectation de disques	Disposition ADP pour l'agrégat racine
Minimum de disques recommandés (par site)	Disques internes et 96 disques externes	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct. Les disques des tiroirs externes sont automatiquement affectés selon le tiroir par tiroir, tous les disques de chaque tiroir étant affectés à l'un des quatre nœuds de la configuration MetroCluster.	Chacun des deux plexes de l'agrégat racine inclut : • Huit partitions pour les données • Deux partitions de parité • Deux partitions de rechange

Nombre minimal de disques pris en charge (par site)	24 disques internes	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Affectation des disques et ADP sur les systèmes AFF A900, ASA A900 et AFF A1K

Directive	Tiroirs par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	96 disques	Les disques sont automatiquement affectés selon le type tiroir par tiroir.	Chacun des deux plexes de l'agrégat racine inclut : • 20 partitions de données • Deux partitions de parité • Deux partitions de rechange
Nombre minimal de disques pris en charge (par site)	24 disques	Les disques sont divisés en quatre groupes égaux (quarts). Chaque tiroir est automatiquement attribué à un pool distinct.	Chacun des deux plexes de l'agrégat racine inclut : • Trois partitions de données • Deux partitions de parité • Une partition de rechange

Affectation des disques sur les systèmes FAS2750

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	24 disques internes et 24 disques externes	Les étagères internes et externes sont divisées en deux moitiés égales. Chaque moitié est automatiquement attribuée à un autre pool	Sans objet

Minimum de disques pris en charge (par site) (configuration haute disponibilité active/passive)	Disques internes uniquement	Affectation manuelle requise	Sans objet

Affectation des disques sur les systèmes FAS8200

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	48 disques	Les disques des tiroirs externes sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Sans objet
Minimum de disques pris en charge (par site) (configuration haute disponibilité active/passive)	24 disques	Affectation manuelle requise.	Sans objet

Affectation des disques sur les systèmes FAS500f

Les mêmes règles et instructions d'affectation des disques pour les systèmes AFF C250 et AFF A250 s'appliquent aux systèmes FAS500f. Pour plus d'informations sur l'affectation des disques sur les systèmes FAS500f, reportez-vous au [ADP_FAS500f] tableau.

Affectation des disques sur les systèmes FAS9000, FAS9500, FAS70 et FAS90

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine
Minimum de disques recommandés (par site)	96 disques	Les disques sont automatiquement affectés selon le type tiroir par tiroir.	Sans objet
Nombre minimal de disques pris en charge (par site)	24 disques	Les disques sont divisés en quatre groupes égaux (quarts). Chaque tiroir est automatiquement attribué à un pool distinct.	Sans objet

Affectation des disques sur les systèmes FAS50

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques (disques externes uniquement, pas de disques internes)	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Sans objet
	48 disques (disques externes et internes)	Les partitions internes sont divisées en quatre groupes égaux (quarts). Chaque trimestre est attribué automatiquement à un pool distinct. Les disques des tiroirs externes sont divisés en quatre groupes égaux (trimestres). Chaque tiroir est automatiquement attribué à un pool distinct.	Sans objet
Nombre minimal de disques pris en charge (par site)	24 disques	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Sans objet

Attribution de disque sur les systèmes FAS50 avec cache Flash

À partir d' ONTAP 9.18.1, le cache Flash est pris en charge sur les systèmes FAS50 pour les configurations IP MetroCluster .

- Vous ne pouvez pas avoir à la fois des agrégats de données et l'agrégat racine avec des disques Flash Cache sur le châssis interne.
- Les emplacements 0 et 23 sont utilisés pour les disques Flash Cache.
- Si vous réutilisez un rack de disque externe, vérifiez que la propriété du disque sur le rack a été supprimée avant de le connecter au contrôleur. Se référer à"Supprimer la propriété ONTAP d'un disque" .

Directive	Nombre de disques par site	Règles d'affectation de disques	Mise en page ADP pour la partition racine

Minimum de disques recommandés (par site)	48 disques (disques externes uniquement, pas de disques internes)	Les disques de chaque tiroir externe sont divisés en deux groupes égaux (moitiés). Chaque demi-tiroir est automatiquement attribué à un pool distinct.	Sans objet
	36 disques (12 disques internes et 24 disques externes – avec les agrégats de données sur le plateau externe et l'agrégat racine sur le plateau interne)	Les disques internes sont divisés en quatre groupes égaux (quartiers). Chaque trimestre est automatiquement attribué à un groupe distinct. Les disques situés sur les étagères externes sont divisés en quatre groupes égaux (quartiers). Chaque quart d'étagère est automatiquement affecté à un pool distinct. **Remarques :** • Si vous utilisez des disques internes et externes, vous devez d'abord installer ONTAP et configurer le cluster local avec uniquement les disques internes. Vous connectez ensuite manuellement l'étagère externe une fois votre tâche d'installation ou de configuration terminée. • Un minimum de 12 disques internes est requis pour l'agrégat racine. Vous devez placer les disques internes racine dans l'emplacement 1. Par exemple, pour 12 disques internes, utilisez les emplacements 1-3, 6-8, 12-14 et 18-20.	Sans objet

Nombre minimal de disques pris en charge (par site)	24 disques durs externes	Les lecteurs sont répartis en quatre groupes égaux. Chaque tiroir est automatiquement attribué à un pool distinct.	Sans objet

Exigences relatives au peering de cluster dans les configurations IP MetroCluster

Chaque site MetroCluster est configuré comme homologue de son site partenaire. Vous devez connaître les conditions préalables et les instructions de configuration des relations de peering. C'est important lorsque vous décidez d'utiliser des ports partagés ou dédiés pour ces relations.

Informations associées

"Configuration cluster et SVM peering express"

Conditions préalables au peering de clusters

Avant de configurer le peering de cluster, vous devez vérifier que la connectivité entre le port, l'adresse IP, le sous-réseau, le pare-feu et les exigences de nommage des clusters sont respectées.

Les besoins en connectivité

Chaque LIF intercluster du cluster local doit pouvoir communiquer avec chaque LIF intercluster sur le cluster distant.

Bien qu'il ne soit pas nécessaire, il est généralement plus simple de configurer les adresses IP utilisées pour les LIF intercluster dans le même sous-réseau. Les adresses IP peuvent résider dans le même sous-réseau que les LIF de données ou dans un autre sous-réseau. Le sous-réseau utilisé dans chaque cluster doit respecter les exigences suivantes :

- Le sous-réseau doit disposer de suffisamment d'adresses IP disponibles pour allouer à une LIF intercluster par nœud.

  Par exemple, dans un cluster à quatre nœuds, le sous-réseau utilisé pour la communication intercluster doit disposer de quatre adresses IP disponibles.

Chaque nœud doit disposer d'un LIF intercluster avec une adresse IP sur le réseau intercluster.

Les LIF intercluster peuvent disposer d'une adresse IPv4 ou IPv6.

> ONTAP 9 vous permet de migrer vos réseaux de peering d'IPv4 vers IPv6 en autorisant, éventuellement, la présence simultanée des deux protocoles sur les LIF intercluster. Dans les versions précédentes, toutes les relations intercluster pour un cluster entier étaient au format IPv4 ou IPv6. Cela signifiait que le changement de protocole était potentiellement source de perturbation.

Configuration requise pour les ports

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Les ports doivent répondre aux exigences suivantes :

- Tous les ports utilisés pour communiquer avec un cluster distant donné doivent se trouver dans le même IPspace.

  Vous pouvez utiliser plusieurs IPspaces pour gérer plusieurs clusters dans un même cluster. Une connectivité à maillage complet par paire est requise uniquement au sein d'un IPspace.

- Le broadcast domain utilisé pour les communications intercluster doit inclure au moins deux ports par nœud afin que la communication intercluster puisse basculer d'un port vers un autre.

  Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).

- Tous les ports doivent être câblés.
- Tous les ports doivent être en état de santé.
- Les paramètres MTU des ports doivent être cohérents.

Exigences relatives au pare-feu

Les pare-feu et la politique de pare-feu intercluster doivent autoriser les protocoles suivants :

- Service ICMP
- TCP aux adresses IP de toutes les LIFs intercluster sur les ports 10000, 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

La politique de pare-feu intercluster par défaut permet l'accès via le protocole HTTPS et à partir de toutes les adresses IP (0.0.0.0/0). Vous pouvez modifier ou remplacer la stratégie si nécessaire.

Considérations relatives à l'utilisation de ports dédiés

Pour déterminer si l'utilisation d'un port dédié pour la réplication intercluster est la bonne solution réseau intercluster, vous devez tenir compte des configurations et des exigences telles que le type de LAN, la bande passante WAN disponible, l'intervalle de réplication, le taux de changement et le nombre de ports.

Pour déterminer si l'utilisation d'un port dédié est la meilleure solution réseau intercluster, prenez en compte les aspects suivants de votre réseau :

- Si la quantité de bande passante WAN disponible est similaire à celle des ports LAN et que l'intervalle de réplication est tel que la réplication se produit pendant que l'activité client est régulière, alors vous devez dédier des ports Ethernet à la réplication intercluster pour éviter les conflits entre la réplication et les protocoles de données.
- Si l'utilisation du réseau générée par les protocoles de données (CIFS, NFS et iSCSI) est telle que l'utilisation du réseau dépasse 50 %, alors dédier des ports à la réplication pour permettre des performances non dégradées en cas de basculement sur un nœud.
- Lorsque des ports physiques 10 GbE ou plus rapides sont utilisés pour les données et la réplication, vous pouvez créer des ports VLAN pour la réplication et dédier les ports logiques à la réplication intercluster.

  La bande passante du port est partagée entre tous les VLAN et le port de base.

- Tenez compte du taux de modification des données et de l'intervalle de réplication et de l'espace requis pour déterminer si la quantité de données qui doit être répliquée sur chaque intervalle nécessite suffisamment de bande passante. Cela peut générer des conflits avec les protocoles de données en cas de partage de ports de données.

Points à prendre en compte lors du partage de ports de données

Lors de la détermination du partage d'un port de données pour la réplication intercluster est la bonne solution réseau intercluster, vous devez tenir compte des configurations et des exigences telles que le type de LAN, la bande passante WAN disponible, l'intervalle de réplication, le taux de changement et le nombre de ports.

Prenez en compte les aspects suivants de votre réseau pour déterminer si le partage de ports de données est la meilleure solution de connectivité intercluster :

- Pour un réseau haut débit, tel qu'un réseau 40 Gigabit Ethernet (40-GbE), une quantité suffisante de bande passante LAN locale peut être disponible pour effectuer la réplication sur les mêmes ports 40 GbE utilisés pour l'accès aux données.

  Dans la plupart des cas, la bande passante WAN disponible est bien inférieure à celle du réseau LAN 10 GbE.

- Le partage des ports de données peut être dû à tous les nœuds du cluster pour répliquer des données et partager la bande passante WAN disponible.
- Le partage de ports pour les données et la réplication élimine le nombre de ports supplémentaires requis pour dédier des ports à la réplication.
- La taille maximale de l'unité de transmission (MTU) du réseau de réplication sera la même que celle utilisée sur le réseau de données.
- Tenez compte du taux de modification des données et de l'intervalle de réplication et de l'espace requis pour déterminer si la quantité de données qui doit être répliquée sur chaque intervalle nécessite suffisamment de bande passante. Cela peut générer des conflits avec les protocoles de données en cas de partage de ports de données.
- Lorsque les ports de données pour la réplication intercluster sont partagés, les LIFs intercluster peuvent être migrés vers n'importe quel autre port intercluster du même nœud afin de contrôler le port de données spécifique utilisé pour la réplication.

Exigences ISL

Exigences de liaison inter-commutateurs pour les configurations IP MetroCluster

Vérifiez que votre réseau et votre configuration IP MetroCluster sont conformes à toutes les exigences de liaison inter-commutateurs (ISL). Même si certaines exigences ne s'appliquent pas à votre configuration, vous devez toujours connaître toutes les exigences ISL pour mieux comprendre la configuration globale.

Le tableau suivant présente les sujets traités dans cette section.

Titre	Description
"Commutateurs validés par NetApp et compatibles MetroCluster"	Décrit les exigences relatives au commutateur. S'applique à tous les switchs utilisés dans les configurations MetroCluster, y compris aux switchs Back-end.

Titre	Description
"Considérations relatives aux liens ISL"	Décrit les exigences ISL. S'applique à toutes les configurations MetroCluster, indépendamment de la topologie réseau et que vous utilisiez des switchs validés par NetApp ou des switchs compatibles MetroCluster.
"Considérations relatives au déploiement de MetroCluster dans des réseaux partagés de couche 2 ou 3"	Décrit la configuration requise pour les réseaux partagés de couche 2 ou 3. S'applique à toutes les configurations, à l'exception des configurations MetroCluster utilisant des switchs validés par NetApp et des liens ISL directement connectés.
"Considérations relatives à l'utilisation de commutateurs compatibles MetroCluster"	Décrit la configuration requise pour les switchs compatibles MetroCluster. S'applique à toutes les configurations MetroCluster qui n'utilisent pas de switchs validés par NetApp.
"Exemples de topologies réseau MetroCluster"	Le fournit des exemples de topologies réseau MetroCluster différentes. S'applique à toutes les configurations MetroCluster.

Commutateurs validés NetApp et compatibles MetroCluster dans une configuration IP MetroCluster

Tous les switchs utilisés dans votre configuration, y compris les switchs Back-end, doivent être certifiés NetApp ou compatibles MetroCluster.

Commutateurs validés NetApp

Un commutateur est validé par NetApp s'il répond aux exigences suivantes :

- Le switch est fourni par NetApp dans le cadre de la configuration IP MetroCluster
- Le commutateur est répertorié dans le "NetApp Hardware Universe" Comme commutateur pris en charge sous *MetroCluster-over-IP-connections*
- Le commutateur n'est utilisé que pour connecter des contrôleurs IP MetroCluster et, dans certaines configurations, des tiroirs disques NS224
- Le commutateur est configuré à l'aide du fichier RCF (Reference Configuration File) fourni par NetApp

Tout switch qui ne répond pas à ces exigences n'est **pas** un switch validé par NetApp.

Commutateurs compatibles MetroCluster

Un commutateur conforme à MetroCluster n'est pas validé par NetApp, mais peut être utilisé dans une configuration MetroCluster IP si elle répond à certaines exigences et directives de configuration.

NetApp ne fournit pas de services de support pour la résolution de problèmes ni la configuration pour un switch non validé conforme à MetroCluster.

Exigences relatives aux liaisons inter-commutateurs (ISL) sur les configurations IP MetroCluster

Les liens ISL (Inter-Switch Links) transportant le trafic MetroCluster sur toutes les

configurations IP MetroCluster et les topologies réseau ont certaines exigences. Ces exigences s'appliquent à tous les liens ISL transportant du trafic MetroCluster, que les liens ISL soient directs ou partagés entre les commutateurs des clients.

Exigences ISL de MetroCluster

Ce qui suit s'applique aux liens ISL sur toutes les configurations MetroCluster IP :

- Les deux tissus doivent avoir le même nombre de liens ISL.
- Les liens ISL sur une structure doivent tous être de la même vitesse et de la même longueur.
- Les liens ISL des deux tissus doivent être de la même vitesse et de la même longueur.
- La différence de distance maximale prise en charge entre le tissu 1 et le tissu 2 est de 20 km ou 0,2 ms.
- Les liens ISL doivent avoir la même topologie. Par exemple, ils doivent tous être des liens directs, ou si la configuration utilise WDM, ils doivent tous utiliser WDM.
- La vitesse ISL minimale requise dépend du modèle de plate-forme :
  - À compter de ONTAP 9.18.1, les plateformes disposant d'un port dorsal IP MetroCluster à 100Gbps requièrent une vitesse de liaison ISL minimale de 100Gbps. L'utilisation d'une vitesse ISL différente nécessite une Feature Product Variance Request (FPVR). Pour déposer une FPVR, contactez votre équipe commerciale NetApp.

    > Les mises à niveau vers ONTAP 9.18.1 et versions ultérieures sur les plateformes qui ne répondent pas actuellement à l'exigence ISL de 100Gbps ne sont pas bloquées et peuvent être effectuées. Cependant, NetApp recommande fortement aux clients de migrer vers une connectivité ISL de 100Gbps afin de maintenir les niveaux de performance et de disponibilité attendus.

  - Sur toutes les autres plateformes, la vitesse de liaison ISL minimale prise en charge est de 10 Gbit/s.
- Il doit y avoir au moins un port ISL 10Gbps par structure.

Limites de latence et de perte de paquets sur les liens ISL

Ce qui suit s'applique au trafic aller-retour entre les commutateurs IP MetroCluster sur site_A et site_B, avec la configuration MetroCluster en état de fonctionnement stable :

- Comme la distance entre deux sites MetroCluster augmente, la latence augmente, généralement dans la plage de 1 ms temps de retard aller-retour par 100 km (62 miles). La latence dépend également de l'accord de niveau de service (SLA) du réseau en termes de bande passante des liaisons ISL, de débit de paquets et de gigue sur le réseau. La faible bande passante, la gigue élevée et les baisses aléatoires de paquets entraînent différents mécanismes de récupération par les commutateurs ou le moteur TCP sur les modules de contrôleur, pour une livraison réussie des paquets. Ces mécanismes de restauration peuvent augmenter la latence globale. Pour plus d'informations sur la latence de trajet aller-retour et les exigences de distance maximale pour votre configuration, reportez-vous au "Hardware Universe :"
- Tout périphérique qui contribue à la latence doit être pris en compte.
- Le "Hardware Universe :" indique la distance en km Vous devez allouer 1 ms par 100 km. La distance maximale est définie par ce qui est atteint en premier, soit par le temps aller-retour maximal (RTT) en ms, soit par la distance en km Par exemple, si *le Hardware Universe* indique une distance de 300 km, en se traduisant par 3 ms, votre ISL ne peut pas dépasser 300 km et la RTT maximale ne peut pas dépasser 3 ms, selon la première éventualité atteinte.
- La perte de paquets doit être inférieure ou égale à 0.01 %. La perte maximale de paquets est la somme de

toutes les pertes sur toutes les liaisons sur le chemin entre les nœuds MetroCluster et la perte sur les interfaces IP MetroCluster locales.

- La valeur de gigue prise en charge est de 3 ms pour un aller-retour (ou 1,5 ms pour un aller-simple).
- Le réseau doit allouer et maintenir la quantité de bande passante SLA requise pour le trafic MetroCluster, indépendamment des microrafales et des pics de trafic.
- Si vous utilisez ONTAP 9.7 ou une version ultérieure, le réseau intermédiaire entre les deux sites doit fournir une bande passante minimale de 4,5 Gbit/s pour la configuration IP de MetroCluster.

Considérations relatives à l'émetteur-récepteur et au câble

Tous les SFP ou SFP pris en charge par le fournisseur de l'équipement sont pris en charge pour les liens ISL de MetroCluster. Les SFP et QSFP fournis par NetApp ou le fournisseur de l'équipement doivent être pris en charge par le commutateur et le micrologiciel du commutateur.

Lorsque vous connectez les contrôleurs aux commutateurs et aux liens ISL du cluster local, vous devez utiliser les émetteurs-récepteurs et les câbles fournis par NetApp avec le MetroCluster.

Lorsque vous utilisez une carte QSFP-SFP, la configuration du port en mode de vitesse écorché ou natif dépend du modèle du commutateur et du micrologiciel. Par exemple, pour utiliser un adaptateur QSFP-SFP avec des commutateurs Cisco 9336C exécutant le micrologiciel NX-OS 9.x ou 10.x, vous devez configurer le port en mode de vitesse natif.

Si vous configurez une FCR, vérifiez que vous sélectionnez le mode de vitesse correct ou utilisez un port avec un mode de vitesse approprié.

Utilisation de xWDM, TDM et de périphériques de cryptage externes

Lorsque vous utilisez des périphériques xWDM/TDM ou des périphériques fournissant un cryptage dans une configuration IP MetroCluster, votre environnement doit satisfaire aux exigences suivantes :

- Lors de la connexion des commutateurs IP MetroCluster au xWDM/TDM, les périphériques de cryptage externes ou l'équipement xWDM/TDM doivent être certifiés par le fournisseur pour le commutateur et le micrologiciel. La certification doit couvrir le mode de fonctionnement (tel que l'agrégation et le cryptage).
- La latence et la gigue globales de bout en bout, y compris le cryptage, ne peuvent pas dépasser la quantité maximale indiquée dans le IMT et dans cette documentation.

Nombre pris en charge de liens ISL et de câbles de dérivation

Le tableau suivant indique le nombre maximal de liens ISL pris en charge qui peuvent être configurés sur un commutateur IP MetroCluster à l'aide de la configuration du fichier de configuration de référence (RCF).

Modèle de commutateur IP MetroCluster	Type de port	Nombre maximal de liens ISL
Commutateurs BES-53248 pris en charge par Broadcom	Ports natifs	4 ISL utilisant 10 Gbits/s ou 25 Gbits/s.
Commutateurs BES-53248 pris en charge par Broadcom	Ports natifs (remarque 1)	2 ISL utilisant 40 Gbit/s ou 100 Gbit/s.
Cisco 3132Q-V	Ports natifs	6 ISL utilisant 40 Gbit/s.

Cisco 3132Q-V	Câbles de dérivation	16 ISL utilisant 10 Gbits/s.
Cisco 3232C	Ports natifs	6 ISL utilisant 40 Gbit/s ou 100 Gbit/s.
Cisco 3232C	Câbles de dérivation	16 ISL utilisant 10 Gbits/s ou 25 Gbits/s.
Cisco 9336C-FX2 (pas de connexion des tiroirs NS224)	Ports natifs	6 ISL utilisant 40 Gbit/s ou 100 Gbit/s.
Cisco 9336C-FX2 (pas de connexion des tiroirs NS224)	Câbles de dérivation	16 ISL utilisant 10 Gbits/s ou 25 Gbits/s.
Cisco 9336C-FX2 (connexion des tiroirs NS224)	Ports natifs (remarque 2)	4 ISL utilisant 40 Gbit/s ou 100 Gbit/s.
Cisco 9336C-FX2 (connexion des tiroirs NS224)	Câbles de dérivation (remarque 2)	16 ISL utilisant 10 Gbits/s ou 25 Gbits/s.
NVIDIA SN2100	Ports natifs (remarque 2)	2 ISL utilisant 40 Gbit/s ou 100 Gbit/s.
NVIDIA SN2100	Câbles de dérivation (remarque 2)	8 ISL utilisant 10 Gbits/s ou 25 Gbits/s.

Remarque 1 : l'utilisation de liens ISL de 40 Gbits/s ou de 100 Gbits/s sur un commutateur BES-53248 nécessite une licence supplémentaire.

Remarque 2 : les mêmes ports sont utilisés pour la vitesse native et le mode de répartition. Vous devez choisir d'utiliser les ports en mode de vitesse native ou en mode écorché lors de la création du fichier RCF.

- Tous les liens ISL d'un commutateur IP MetroCluster doivent être à la même vitesse. L'utilisation simultanée de plusieurs ports ISL à des vitesses différentes n'est pas prise en charge.
- Pour des performances optimales, vous devez utiliser au moins un lien ISL de 40 Gbit/s par réseau. Vous ne devez pas utiliser un lien ISL de 10 Gbits/s par réseau pour les systèmes FAS9000, AFF A700 ou d'autres plateformes haute capacité.

NetApp vous recommande de configurer un petit nombre de liens ISL à large bande passante plutôt qu'un grand nombre de liens ISL à faible bande passante. Par exemple, il est préférable de configurer un lien ISL de 40 Gbits/s au lieu de quatre liens ISL de 10 Gbits/s. Lorsque plusieurs liens ISL sont utilisés, l'équilibrage statistique de la charge peut avoir un impact sur le débit maximal. Un équilibrage inégal peut réduire le débit à celui d'un lien ISL unique.

Conditions requises pour déployer les configurations IP MetroCluster dans les réseaux partagés de couche 2 ou de couche 3

Selon vos besoins, vous pouvez utiliser des réseaux partagés de couche 2 ou 3 pour déployer MetroCluster.

À partir de ONTAP 9.6, les configurations IP MetroCluster avec commutateurs pris en charge peuvent partager des réseaux existants pour des liaisons inter-commutateurs (ISL) au lieu d'utiliser des liens MetroCluster dédiés. Cette topologie est appelée *réseaux de couche 2 partagés*.

Depuis ONTAP 9.9.1, les configurations MetroCluster IP peuvent être implémentées avec des connexions back-end IP-routées (couche 3). Cette topologie est appelée *réseaux de couche 3 partagés*.

- Toutes les fonctionnalités ne sont pas prises en charge dans toutes les topologies réseau.
- Vous devez vérifier que vous disposez d'une capacité réseau adéquate et que la taille de lien ISL est adaptée à votre configuration. Une faible latence est primordiale pour la réplication des données entre les sites MetroCluster. Les problèmes de latence sur ces connexions peuvent affecter les E/S client
- Toutes les références aux switchs Back-end MetroCluster font référence aux switchs validés par NetApp ou compatibles MetroCluster. Voir "Commutateurs validés par NetApp et compatibles MetroCluster" pour en savoir plus.

Exigences ISL pour les réseaux de couche 2 et 3

Ce qui suit s'applique aux réseaux de couche 2 et 3 :

- Il n'est pas nécessaire que la vitesse et le nombre de liens ISL entre les commutateurs MetroCluster et les commutateurs de réseau intermédiaire correspondent. De même, la vitesse entre les commutateurs de réseau intermédiaire n'a pas besoin de correspondre.

  Par exemple, les commutateurs MetroCluster peuvent se connecter en utilisant un lien ISL de 40 Gbit/s aux commutateurs intermédiaires, tandis que les commutateurs intermédiaires peuvent se connecter en utilisant deux liens ISL de 100 Gbit/s.

- La surveillance du réseau doit être configurée sur le réseau intermédiaire pour surveiller l'utilisation des liens ISL, les erreurs (DROPs, volets de liaison, corruption, etc.), et les défaillances.
- La taille de MTU doit être définie sur 9216 sur tous les ports transportant le trafic MetroCluster de bout en bout.
- Aucun autre trafic ne peut être configuré avec une priorité plus élevée que la classe de service (COS) 5.
- La notification explicite de congestion (ECN) doit être configurée sur tous les chemins transportant le trafic MetroCluster de bout en bout.
- Les liens ISL transportant du trafic MetroCluster doivent être des liaisons natives entre les commutateurs.

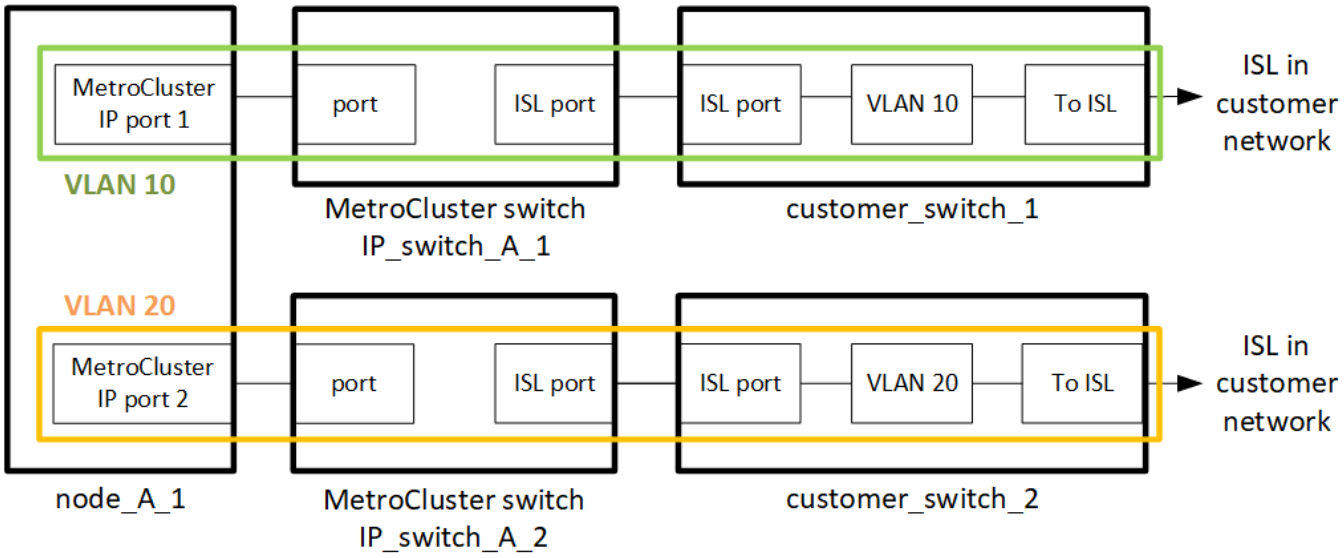
  Les services de partage de liens tels que les liens MPLS (Multi protocole Label Switching) ne sont pas pris en charge.

- Les VLAN de couche 2 doivent s'étendre nativement sur les sites. Le recouvrement VLAN tel que le LAN extensible virtuel (VXLAN) n'est pas pris en charge.
- Le nombre d'interrupteurs intermédiaires n'est pas limité. Cependant, NetApp vous recommande de conserver le nombre de commutateurs au minimum requis.
- Les liens ISL des commutateurs MetroCluster sont configurés avec les éléments suivants :
  - Switch port mode 'trunk' dans le cadre d'un port-Channel LACP
  - La taille de MTU est 9216
  - Aucun VLAN natif n'est configuré

- Seuls les VLAN transportant le trafic MetroCluster intersite sont autorisés
- Le VLAN par défaut du commutateur n'est pas autorisé

Considérations relatives aux réseaux de couche 2

Les switchs backend MetroCluster sont connectés au réseau du client.



Les commutateurs intermédiaires fournis par le client doivent répondre aux exigences suivantes :

- Le réseau intermédiaire doit fournir les mêmes VLAN entre les sites. Cela doit correspondre aux VLAN MetroCluster définis dans le fichier RCF.
- RcfFileGenerator ne permet pas la création d'un fichier RCF à l'aide de VLAN non pris en charge par la plate-forme.
- Le RcfFileGenerator peut restreindre l'utilisation de certains ID de VLAN, par exemple, s'ils sont destinés à une utilisation ultérieure. En règle générale, les VLAN réservés sont jusqu'à 100 inclus.
- Les VLAN de couche 2 dont les ID correspondent aux VLAN MetroCluster doivent s'étendre sur le réseau partagé.

Configuration VLAN dans ONTAP

Vous ne pouvez spécifier le VLAN qu'au cours de la création de l'interface. Vous pouvez configurer les VLAN 10 et 20 par défaut, ou les VLAN compris entre 101 et 4096 (ou le nombre pris en charge par le fournisseur du commutateur, selon le nombre le plus faible). Une fois les interfaces MetroCluster créées, vous ne pouvez pas modifier l'ID du VLAN.

Certains fournisseurs de commutateurs peuvent réserver l'utilisation de certains VLAN.

Les systèmes suivants ne nécessitent pas de configuration VLAN dans ONTAP. Le VLAN est spécifié par la configuration des ports de commutateur :

- FAS8200 ET AFF A300
- AFF A320
- FAS9000 et AFF A700
- AFF A800, ASA A800, AFF C800 et ASA C800

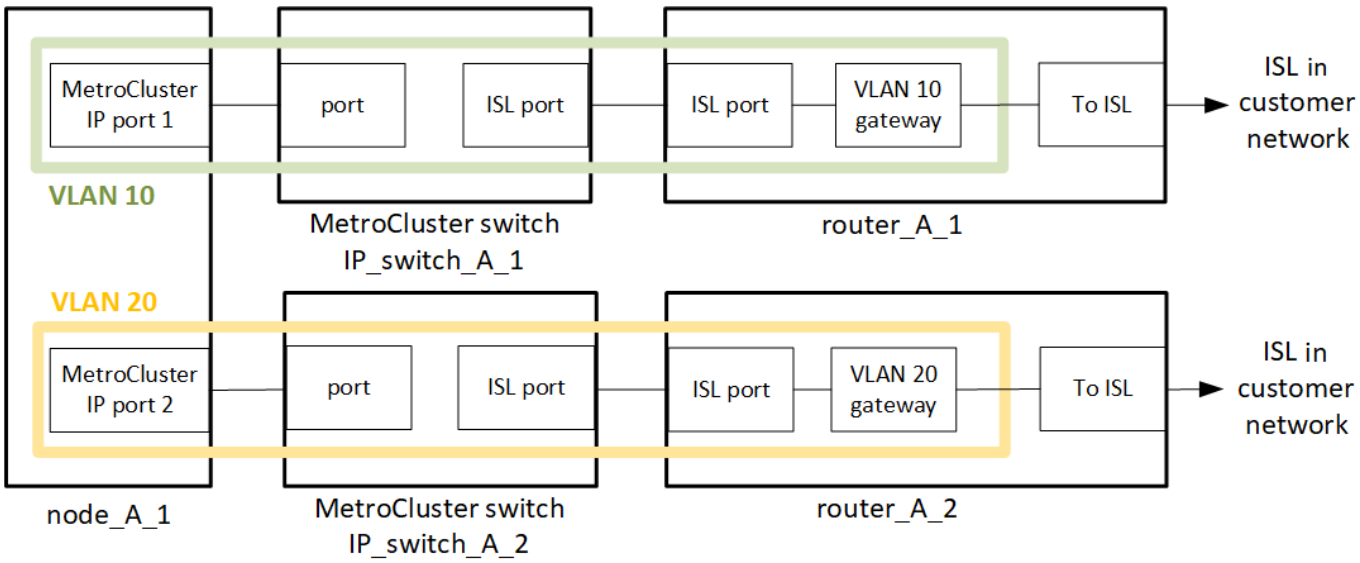
Les systèmes répertoriés ci-dessus peuvent être configurés à l'aide des VLAN 100 et inférieurs. Cependant, certains VLAN de cette plage peuvent être réservés pour une utilisation autre ou future.

Pour tous les autres systèmes, vous devez configurer le VLAN lorsque vous créez les interfaces MetroCluster dans ONTAP. Les restrictions suivantes s'appliquent :

- Le VLAN par défaut est 10 et 20
- Si vous utilisez ONTAP 9.7 ou une version antérieure, vous ne pouvez utiliser que les VLAN 10 et 20 par défaut.
- Si vous utilisez ONTAP 9.8 ou une version ultérieure, vous pouvez utiliser les VLAN 10 et 20 par défaut et un VLAN supérieur à 100 (101 et supérieur) peut également être utilisé.

Considérations relatives aux réseaux de couche 3

Les commutateurs back-end MetroCluster sont connectés au réseau IP routé, soit directement aux routeurs (comme indiqué dans l'exemple simplifié suivant), soit via d'autres commutateurs.



L'environnement MetroCluster est configuré et câblé sous la forme d'une configuration IP MetroCluster standard, comme décrit dans la "Configurer les composants matériels de MetroCluster". Lorsque vous effectuez la procédure d'installation et de câblage, vous devez effectuer les étapes spécifiques à une configuration de couche 3. Ce qui suit s'applique aux configurations de couche 3 :

- Vous pouvez connecter les commutateurs MetroCluster directement au routeur ou à un ou plusieurs commutateurs intermédiaires.
- Vous pouvez connecter les interfaces IP MetroCluster directement au routeur ou à l'un des commutateurs intermédiaires.
- Le VLAN doit être étendu au périphérique de passerelle.
- Vous utilisez le `-gateway parameter` Pour configurer l'adresse IP de l'interface MetroCluster avec une adresse de passerelle IP.
- Les ID de VLAN pour les VLAN MetroCluster doivent être les mêmes sur chaque site. Cependant, les sous-réseaux peuvent être différents.
- Le routage dynamique n'est pas pris en charge pour le trafic MetroCluster.

- Les fonctions suivantes ne sont pas prises en charge :
  - Configurations MetroCluster à 8 nœuds
  - Actualisation d'une configuration MetroCluster à quatre nœuds
  - Transition de MetroCluster FC à MetroCluster IP
- Deux sous-réseaux sont requis sur chaque site MetroCluster : un sur chaque réseau.
- L'affectation auto-IP n'est pas prise en charge.

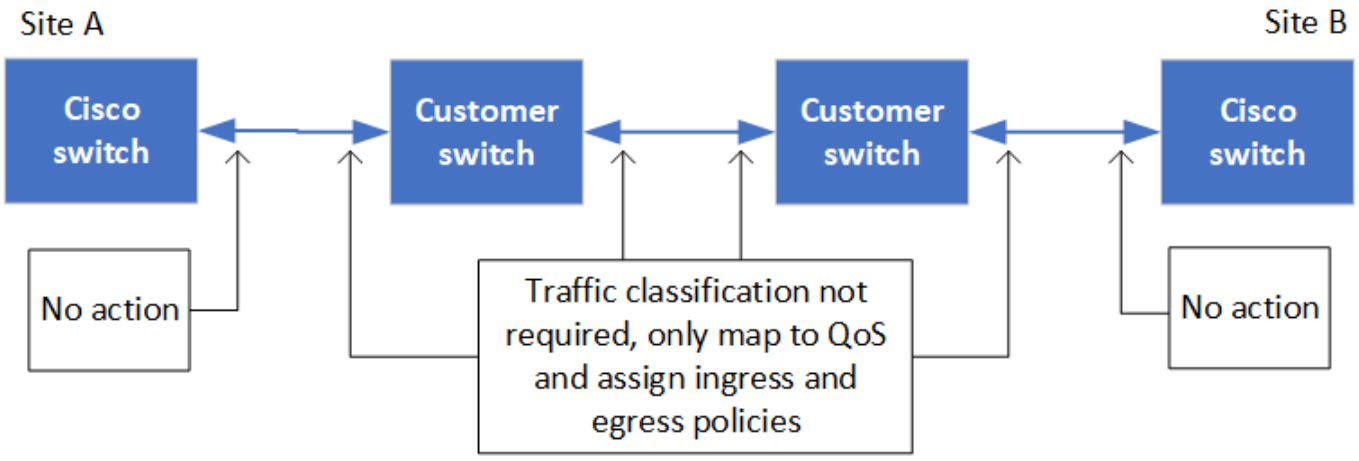
Lorsque vous configurez des routeurs et des adresses IP de passerelle, vous devez répondre aux exigences suivantes :

- Deux interfaces sur un nœud ne peuvent pas avoir la même adresse IP de passerelle.
- Les interfaces correspondantes sur les paires haute disponibilité sur chaque site doivent avoir la même adresse IP de passerelle.
- Les interfaces correspondantes sur un nœud et ses partenaires DR et aux ne peuvent pas avoir la même adresse IP de passerelle.
- Les interfaces correspondantes sur un nœud et ses partenaires DR et aux doivent avoir le même ID VLAN.

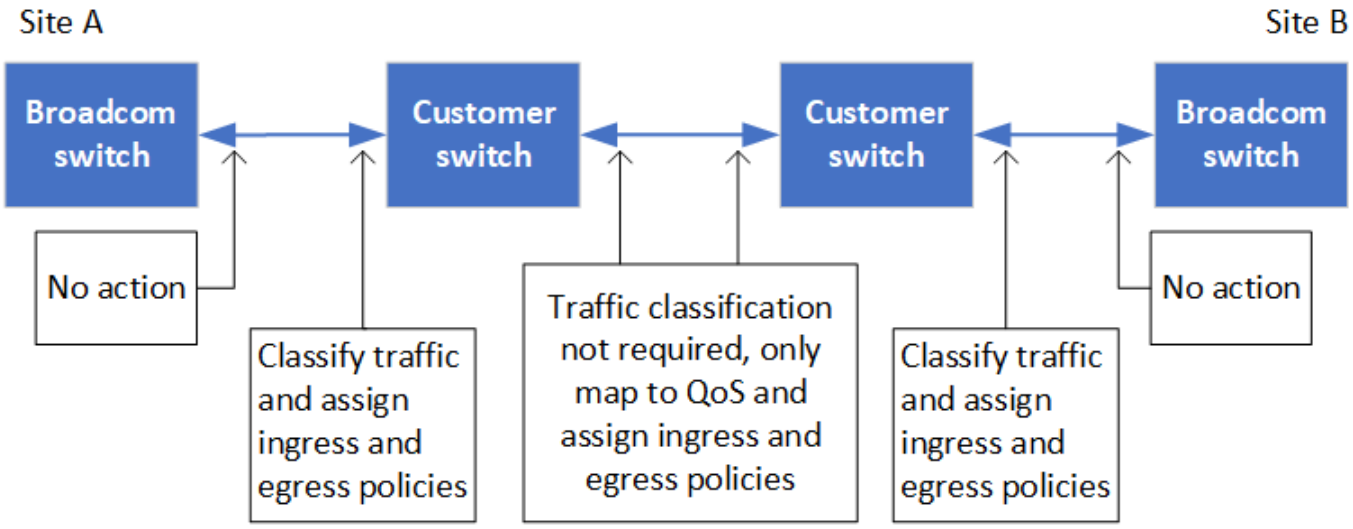
Réglages requis pour les commutateurs intermédiaires

Lorsque le trafic MetroCluster traverse un lien ISL dans un réseau intermédiaire, vérifiez que la configuration des commutateurs intermédiaires garantit que le trafic MetroCluster (RDMA et stockage) répond aux niveaux de service requis sur l'ensemble du chemin entre les sites MetroCluster.

Le schéma suivant présente les paramètres requis lors de l'utilisation de commutateurs Cisco validés par NetApp :



Le diagramme suivant présente les paramètres requis pour un réseau partagé lorsque les commutateurs externes sont des commutateurs IP Broadcom.



Dans cet exemple, les stratégies et mappages suivants sont créés pour le trafic MetroCluster :

- Le `MetroClusterIP_ISL_Ingress` La politique s'applique aux ports du commutateur intermédiaire qui se connecte aux commutateurs IP MetroCluster.

  Le `MetroClusterIP_ISL_Ingress` la stratégie mappe le trafic marqué entrant à la file d'attente appropriée sur le commutateur intermédiaire.

- A `MetroClusterIP_ISL_Egress` La règle s'applique aux ports du commutateur intermédiaire qui se connectent aux liens ISL entre les commutateurs intermédiaires.
- Vous devez configurer les commutateurs intermédiaires avec des mappages d'accès QoS, des classes et des règles correspondants le long du chemin d'accès entre les commutateurs IP MetroCluster. Les commutateurs intermédiaires associent le trafic RDMA à COS5 et le trafic de stockage à COS4.

Les exemples suivants concernent les switchs Cisco Nexus 3232C et 9336C-FX2. Selon le fournisseur et le modèle de votre commutateur, vous devez vérifier que vos commutateurs intermédiaires ont une configuration appropriée.

Configurez le mappage de classes pour le port ISL du commutateur intermédiaire

L'exemple suivant montre les définitions de carte de classe selon que vous devez classer ou faire correspondre le trafic lors de l'entrée.

Classer le trafic à l'entrée :

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

Correspondance du trafic à l'entrée :

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

Créer un mappage de règles d'entrée sur le port ISL du commutateur intermédiaire :

Les exemples suivants montrent comment créer une carte de règles d'entrée selon que vous devez classifier ou faire correspondre le trafic lors de l'entrée.

Classer le trafic à l'entrée :

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Faire correspondre le trafic à l'entrée :

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Configurez la règle de mise en file d'attente de sortie pour les ports ISL

L'exemple suivant montre comment configurer la règle de mise en file d'attente de sortie :

```
policy-map type queuing MetroClusterIP_ISL_Egress
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2
   class type queuing c-out-8q-q5
      priority level 3
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q4
      priority level 4
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q3
      priority level 5
   class type queuing c-out-8q-q2
      priority level 6
   class type queuing c-out-8q-q1
      priority level 7
   class type queuing c-out-8q-q-default
      bandwidth remaining percent 100
      random-detect threshold burst-optimized ecn
```

Ces paramètres doivent être appliqués à tous les commutateurs et liens ISL transportant du trafic MetroCluster.

Dans cet exemple, Q4 et Q5 sont configurés avec `random-detect threshold burst-optimized ecn`. En fonction de votre configuration, vous devrez peut-être définir les seuils minimal et maximal, comme indiqué dans l'exemple suivant :

```
class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
kbytes drop-probability 0 weight 0 ecn
```

Les valeurs minimale et maximale varient en fonction du commutateur et de vos besoins.

Exemple 1 : Cisco

Si votre configuration comporte des commutateurs Cisco, vous n'avez pas besoin de classer sur le premier port d'entrée du commutateur intermédiaire. Vous configurez ensuite les mappages et les règles suivants :

- `class-map type qos match-any c5`
- `class-map type qos match-any c4`

- `MetroClusterIP_ISL_Ingress_Match`

Vous attribuez le `MetroClusterIP_ISL_Ingress_Match` Mappage de règles sur les ports ISL transportant le trafic MetroCluster.

Exemple 2 : Broadcom

Si votre configuration comporte des commutateurs Broadcom, vous devez classer le premier port d'entrée du commutateur intermédiaire. Vous configurez ensuite les mappages et les règles suivants :

- `ip access-list rdma`
- `ip access-list storage`
- `class-map type qos match-all rdma`
- `class-map type qos match-all storage`
- `MetroClusterIP_ISL_Ingress_Classify`
- `MetroClusterIP_ISL_Ingress_Match`

Vous attribuez `the MetroClusterIP_ISL_Ingress_Classify` La stratégie est mappée sur les ports ISL du commutateur intermédiaire qui connecte le commutateur Broadcom.

Vous attribuez le `MetroClusterIP_ISL_Ingress_Match` La stratégie est mappée sur les ports ISL du commutateur intermédiaire qui transportent le trafic MetroCluster mais ne connecte pas le commutateur Broadcom.

Exemples de topologie de réseau de configuration IP MetroCluster

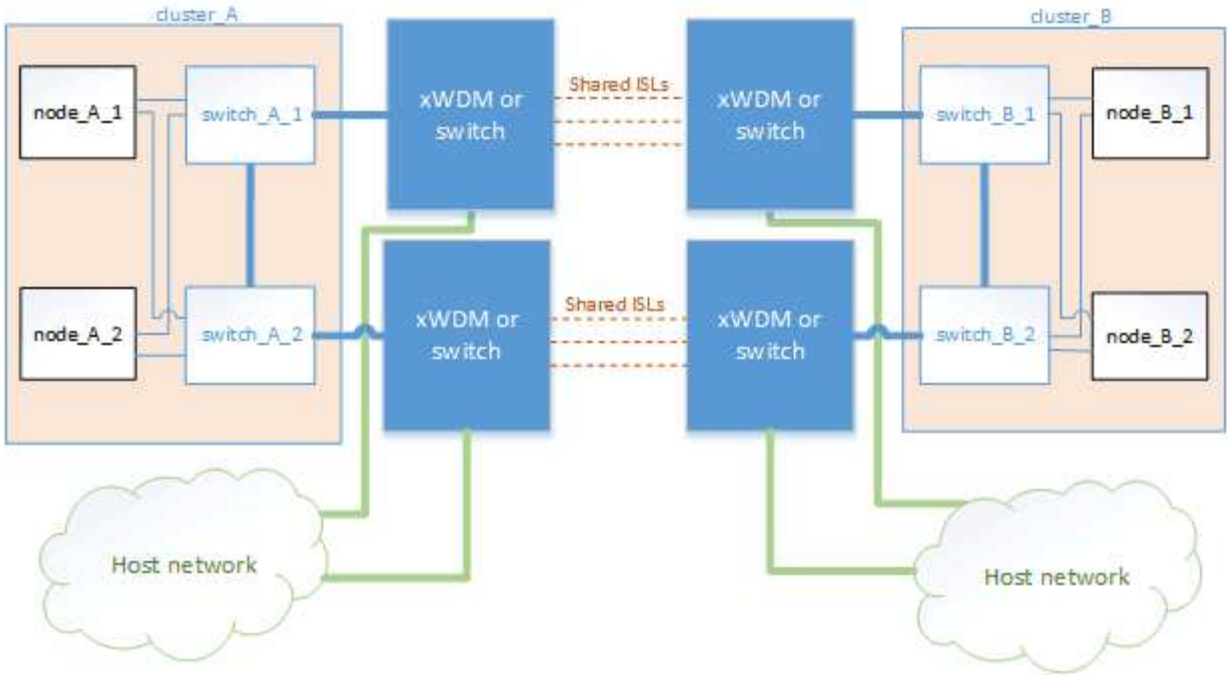
À partir de ONTAP 9.6, certaines configurations réseau supplémentaires sont prises en charge pour les configurations IP de MetroCluster. Cette section fournit des exemples de configurations réseau prises en charge. Toutes les topologies prises en charge ne sont pas répertoriées.

Dans ces topologies, on suppose que les réseaux ISL et intermédiaire sont configurés conformément aux exigences décrites dans le "Considérations relatives aux liens ISL".

> Si vous partagez un lien ISL avec un trafic non MetroCluster, vous devez vérifier que le MetroCluster dispose en permanence de la bande passante minimale requise.

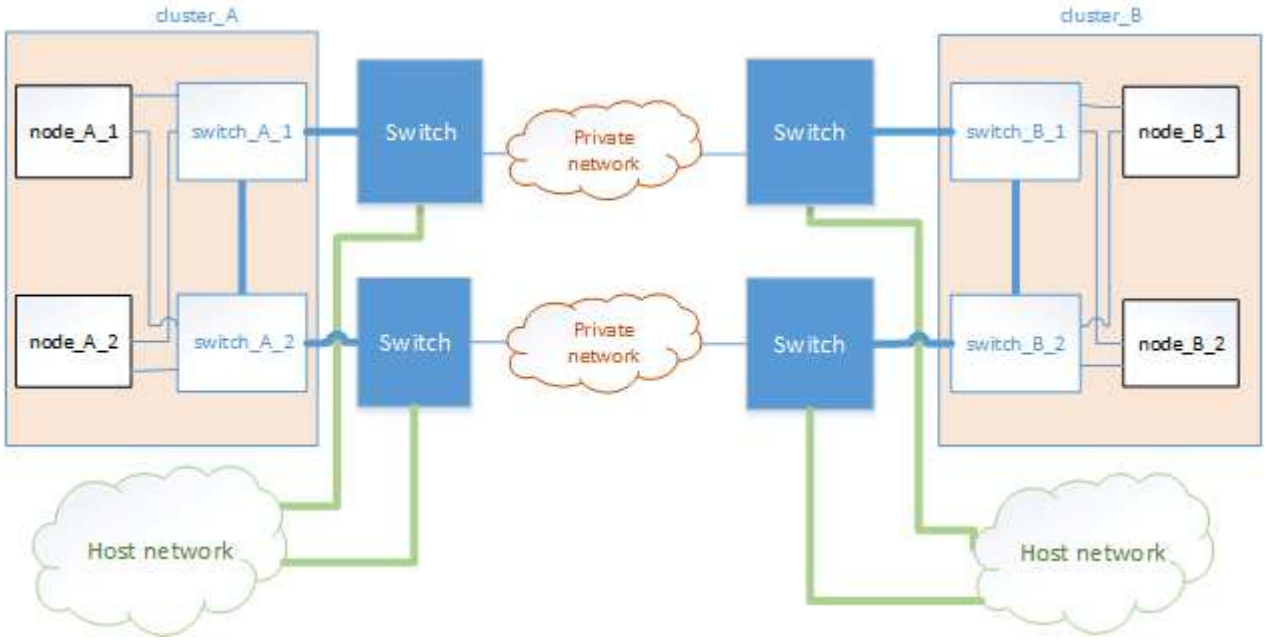
Configuration réseau partagée avec liens directs

Dans cette topologie, deux sites distincts sont connectés par des liens directs. Ces liaisons peuvent être entre les périphériques ou commutateurs xWDM et TDM. La capacité des liens ISL n'est pas dédiée au trafic MetroCluster, mais elle est partagée avec un autre trafic non MetroCluster.



Infrastructure partagée avec réseaux intermédiaires

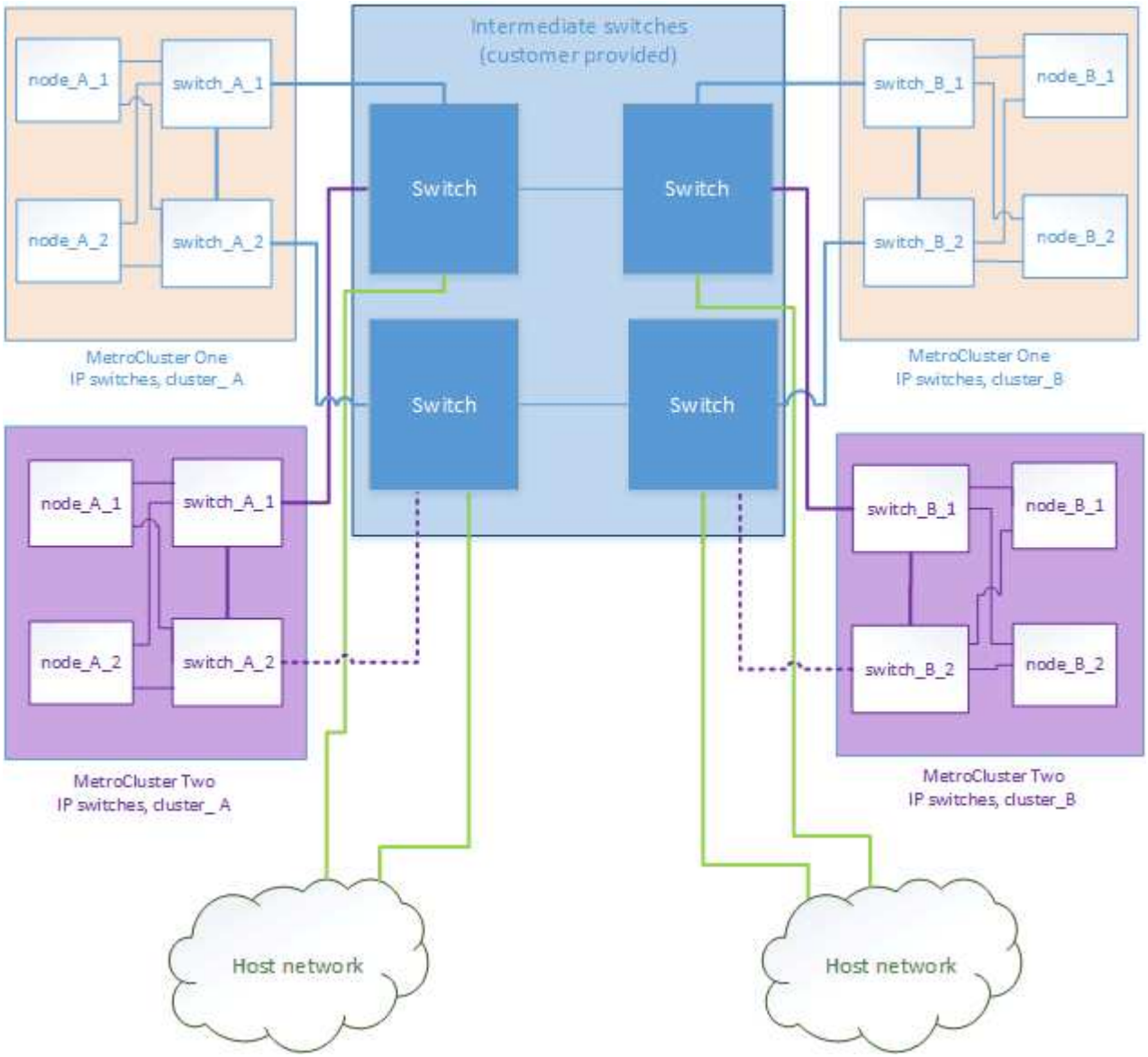
Dans cette topologie, les sites MetroCluster ne sont pas directement connectés, mais MetroCluster et le trafic hôte traversent un réseau. Le réseau peut se composer d'une série de commutateurs et de commutateurs xWDM et TDM, mais contrairement à la configuration partagée avec des liens ISL directs, les liens ne sont pas directs entre les sites. En fonction de l'infrastructure entre les sites, toute combinaison de configurations réseau est possible.



Plusieurs configurations MetroCluster partageant un réseau intermédiaire

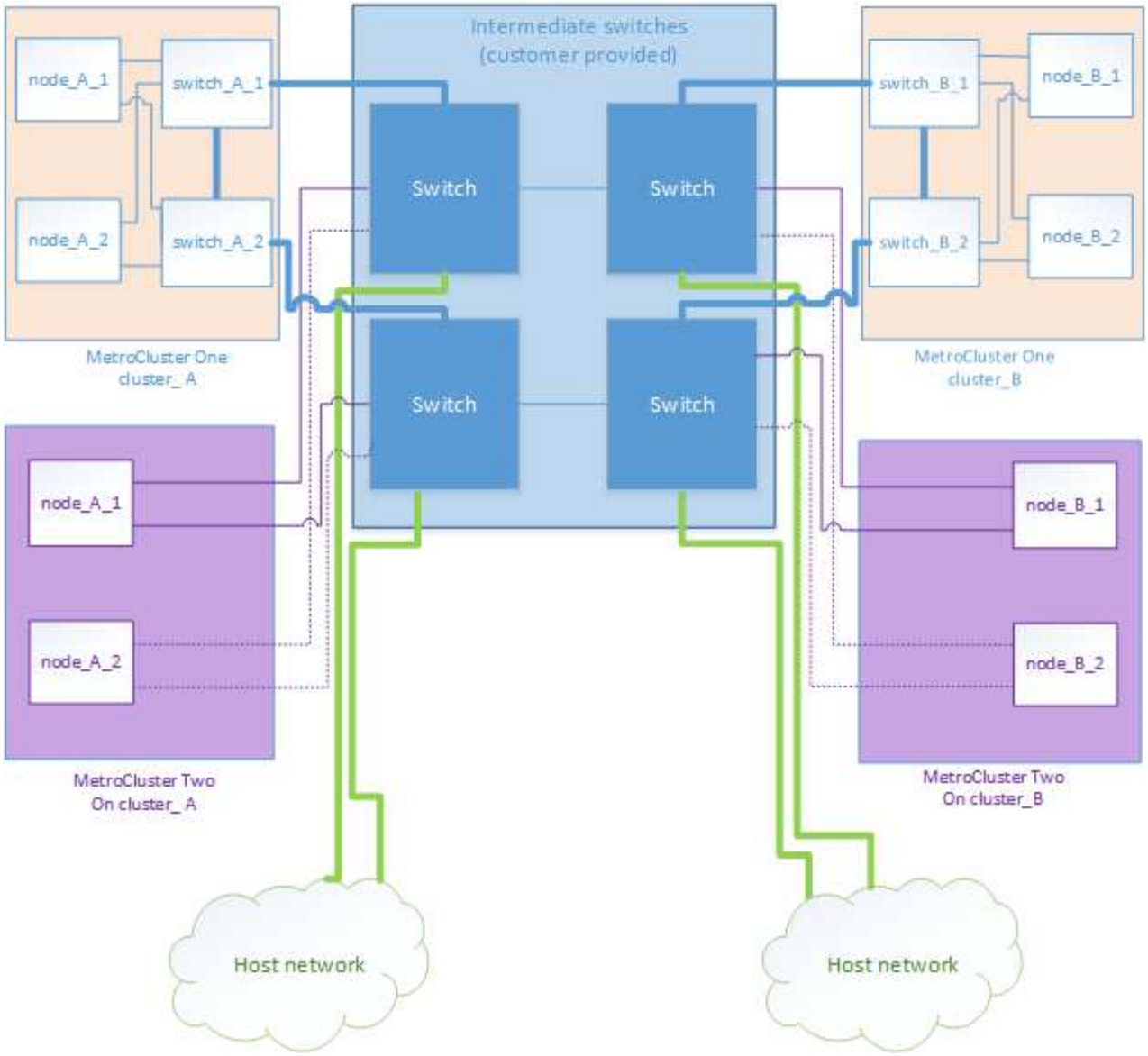
Dans cette topologie, deux configurations MetroCluster distinctes partagent le même réseau intermédiaire. Dans l'exemple, MetroCluster un commutateur_A_1 et MetroCluster deux commutateurs_A_1 se connectent tous deux au même commutateur intermédiaire.

« MetroCluster One » ou « MetroCluster Two » peut être une configuration MetroCluster à huit nœuds ou deux configurations MetroCluster à quatre nœuds.



Combinaison d'une configuration MetroCluster à l'aide de switchs validés NetApp et d'une configuration à l'aide de switchs compatibles MetroCluster

Deux configurations MetroCluster distinctes partagent le même commutateur intermédiaire, où un MetroCluster est configuré à l'aide de commutateurs validés NetApp dans une configuration de couche 2 partagée (MetroCluster ONE), et l'autre MetroCluster est configuré à l'aide de commutateurs compatibles MetroCluster qui se connectent directement aux commutateurs intermédiaires (MetroCluster Two).



Considérations relatives à l'utilisation de commutateurs conformes à MetroCluster

Exigences et limitations pour les commutateurs compatibles MetroCluster

Depuis ONTAP 9.7, les configurations IP MetroCluster peuvent utiliser des commutateurs compatibles avec MetroCluster. Il s'agit de commutateurs non validés par NetApp, mais conformes aux spécifications NetApp. Cependant, NetApp ne fournit pas de services de dépannage ou de prise en charge de la configuration pour les commutateurs non validés. Vous devez connaître les exigences générales et les limites lorsque vous utilisez des switchs compatibles MetroCluster.

Switchs compatibles MetroCluster par rapport aux switchs validés NetApp

Un commutateur est validé par NetApp s'il répond aux exigences suivantes :

- Le switch est fourni par NetApp dans le cadre de la configuration IP MetroCluster
- Le commutateur est répertorié dans le "NetApp Hardware Universe" Comme commutateur pris en charge

sous *MetroCluster-over-IP-connections*

- Le commutateur n'est utilisé que pour connecter des contrôleurs IP MetroCluster et, dans certaines configurations, des tiroirs disques NS224
- Le commutateur est configuré à l'aide du fichier RCF (Reference Configuration File) fourni par NetApp

Tout switch qui ne répond pas à ces exigences n'est **pas** un switch validé par NetApp.

Un commutateur conforme à MetroCluster n'est pas validé par NetApp, mais peut être utilisé dans une configuration MetroCluster IP si elle répond à certaines exigences et directives de configuration.

NetApp ne fournit pas de services de support pour la résolution de problèmes ni la configuration pour un switch non validé conforme à MetroCluster.

Exigences générales pour les commutateurs compatibles MetroCluster

Le commutateur qui connecte les interfaces IP MetroCluster doit répondre aux exigences générales suivantes :

- Les switchs doivent prendre en charge la qualité de service (QoS) et la classification du trafic.
- Les commutateurs doivent prendre en charge la notification explicite de congestion (ECN).
- Les switchs doivent prendre en charge une règle d'équilibrage de la charge pour préserver l'ordre sur le chemin.
- Les commutateurs doivent prendre en charge le contrôle de débit L2 (L2FC).
- Le port du commutateur doit fournir un taux dédié et ne doit pas être suralloué.
- Les câbles et émetteurs-récepteurs reliant les nœuds aux commutateurs doivent être fournis par NetApp. Ces câbles doivent être pris en charge par le fournisseur du commutateur. Si vous utilisez un câblage optique, il est possible que l'émetteur-récepteur du commutateur ne soit pas fourni par NetApp. Vous devez vérifier qu'il est compatible avec l'émetteur-récepteur du contrôleur.
- Les commutateurs qui connectent les nœuds MetroCluster peuvent transporter du trafic non-MetroCluster.
- Seules les plateformes offrant des ports dédiés pour des interconnexions de cluster sans commutateur peuvent être utilisées avec un commutateur conforme à MetroCluster. Les plateformes telles que FAS2750 et AFF A220 ne peuvent pas être utilisées, car le trafic MetroCluster et le trafic d'interconnexion MetroCluster partagent les mêmes ports réseau.
- Le commutateur conforme à MetroCluster ne doit pas être utilisé pour les connexions locales du cluster.
- L'interface IP MetroCluster peut être connectée à n'importe quel port de commutateur pouvant être configuré pour répondre aux exigences.
- Quatre commutateurs IP sont requis, deux pour chaque structure de commutateur. Si vous utilisez des directeurs, vous pouvez utiliser un seul directeur de chaque côté, mais les interfaces IP MetroCluster doivent se connecter à deux lames différentes dans deux domaines de défaillance différents sur ce directeur.
- Les interfaces MetroCluster d'un nœud doivent se connecter à deux commutateurs ou lames réseau. Les interfaces MetroCluster d'un nœud ne peuvent pas être connectées au même réseau, au même commutateur ou au même serveur lame.
- Le réseau doit répondre aux exigences décrites dans les sections suivantes :
  - "Considérations relatives aux liens ISL"
  - "Considérations relatives au déploiement de MetroCluster sur des réseaux partagés de couche 2 ou 3"

- L’unité de transmission maximale (MTU) de 9216 doit être configurée sur tous les commutateurs qui transportent le trafic IP MetroCluster.
- La restauration vers ONTAP 9.6 ou une version antérieure n’est pas prise en charge.

Tout switch intermédiaire que vous utilisez entre les switchs qui connecte les interfaces IP MetroCluster sur les deux sites doit répondre aux exigences et être configuré comme indiqué dans la "Considérations relatives au déploiement de MetroCluster sur des réseaux partagés de couche 2 ou 3".

Limites lors de l’utilisation de switchs compatibles MetroCluster

Vous ne pouvez pas utiliser de configuration ou de fonctionnalité qui nécessite que les connexions de cluster locales soient connectées à un commutateur. Par exemple, vous ne pouvez pas utiliser les configurations et procédures suivantes avec un commutateur compatible MetroCluster :

- Configurations MetroCluster à 8 nœuds
- Passez des configurations FC MetroCluster aux configurations IP MetroCluster
- Mise à jour d’une configuration IP MetroCluster à quatre nœuds
- Les plateformes partagent une interface physique pour le trafic MetroCluster et le cluster local. Reportez-vous à la section "Vitesses réseau propres à la plateforme et modes de port des commutateurs pour les commutateurs compatibles avec MetroCluster" pour les vitesses prises en charge.

Vitesses réseau et modes de port de commutation spécifiques à la plate-forme ONTAP pour les commutateurs compatibles MetroCluster

Si vous utilisez des commutateurs compatibles MetroCluster, vous devez connaître les vitesses réseau spécifiques à la plate-forme et les conditions requises pour le mode des ports de commutation.

Le tableau suivant indique les vitesses réseau spécifiques à la plateforme et les modes de port de commutation pour les switchs compatibles MetroCluster. Vous devez configurer le mode de port du commutateur conformément au tableau.

- Des valeurs manquantes indiquent que la plateforme ne peut pas être utilisée avec un switch compatible MetroCluster.
- Les systèmes AFF A30, AFF C30, AFF C60 et FAS50 nécessitent un adaptateur QSFP à SFP+ sur la carte située sur le contrôleur pour prendre en charge une vitesse de réseau de 25 Gbit/s.

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-
AFF A20	25Gbps	trunk mode
AFF A30	25Gbps or 100Gbps	trunk mode
AFF C30	25Gbps or 100Gbps	trunk mode
AFF C60	25Gbps or 100Gbps	trunk mode
FAS50	25Gbps or 100Gbps	trunk mode
AFF A50	100Gbps	trunk mode
AFF A70	100Gbps	trunk mode
AFF A90	100Gbps	trunk mode
AFF A1K	100Gbps	trunk mode
AFF C80	100Gbps	trunk mode
FAS70	100Gbps	trunk mode
FAS90	100Gbps	trunk mode

Exemples de configuration de commutateur IP MetroCluster

Découvrez les différentes configurations de ports de switch.

> Les exemples suivants utilisent des valeurs décimales et suivent le tableau qui s'applique aux commutateurs Cisco. Selon le fournisseur du commutateur, il se peut que vous ayez besoin de valeurs différentes pour DSCP. Reportez-vous au tableau correspondant au fournisseur du commutateur pour confirmer la valeur correcte.

Valeur DSCP	Décimale	Hex	Signification
101 000	16	0x10	CS2
011 000	24	0x18	CS3
100 000	32	0x20	CS4
101 000	40	0x28	CS5

Port de commutateur connectant une interface MetroCluster

- Classification du trafic RDMA (Remote Direct Memory Access) :
  - Correspondance : port TCP 10006, source, destination ou les deux
  - Correspondance facultative : COS 5
  - Correspondance facultative : DSCP 40
  - Définissez DSCP 40
  - Définissez COS 5
  - Facultatif : mise en forme du débit à 20 Gbit/s.
- Classification du trafic iSCSI :
  - Correspondance : port TCP 62500, source, destination ou les deux
  - Correspondance facultative : COS 4
  - Correspondance facultative : DSCP 32
  - Définissez DSCP 32
  - Définissez COS 4
- L2FlowControl (pause), RX et TX

Ports ISL

- Classification :
  - Correspondance CS 5 ou DSCP 40
    - Définissez DSCP 40
    - Définissez COS 5
  - Correspondance CS 4 ou DSCP 32
    - Définissez DSCP 32

        - Définissez COS 4
- Sortie dans la file d'attente
    - Le groupe CS 4 a un seuil de configuration minimum de 2000 et un seuil maximum de 3000
    - Le groupe CS 5 a un seuil de configuration minimum de 3500 et un seuil maximum de 6500.

> Les seuils de configuration peuvent varier en fonction de l'environnement. Vous devez évaluer les seuils de configuration en fonction de votre environnement.

    - ECN activé pour Q4 et Q5
    - ROUGE activé pour Q4 et Q5

Allocation de la bande passante (ports switchs connectant les interfaces MetroCluster et les ports ISL)

- RDMA, COS 5 / DSCP 40 : 60 %
- ISCSI, COS 4/DSCP 32 : 40 %
- Capacité minimale requise par configuration MetroCluster et réseau : 10 Gbit/s.

> Si vous utilisez des limites de taux, le trafic devrait être **façonné** sans introduire de perte.

Exemples de configuration des ports de commutateur connectant le contrôleur MetroCluster

Les exemples de commandes fournis sont valables pour les commutateurs Cisco NX3232 ou Cisco NX9336. Les commandes varient en fonction du type de commutateur.

Si une fonction ou son équivalent indiqué dans les exemples n'est pas disponible sur le commutateur, celui-ci ne répond pas à la configuration minimale requise et ne peut pas être utilisé pour déployer une configuration MetroCluster. Ceci est vrai pour tout commutateur connecté à une configuration MetroCluster et pour tous les commutateurs intermédiaires.

> Les exemples suivants peuvent uniquement afficher la configuration d'un réseau.

Configuration de base

Un réseau local virtuel (VLAN) doit être configuré dans chaque réseau. L'exemple suivant montre comment configurer un VLAN dans le réseau 10.

Exemple:

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

Exemple:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

Exemples de configuration de la classification

Vous devez configurer des mappages d'accès et de classes pour mapper le trafic RDMA et iSCSI aux classes

appropriées.

Dans l'exemple suivant, tout le trafic TCP vers et depuis le port 65200 est mappé sur la classe de stockage (iSCSI). Tout le trafic TCP depuis et vers le port 10006 est mappé à la classe RDMA. Ces mappages de règles sont utilisés sur les ports de commutateur qui connectent les interfaces MetroCluster.

Exemple:

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
match access-group name rdma
```

Vous devez configurer une stratégie d'entrée. Une politique d'entrée mappe le trafic comme classifié à différents groupes de CS. Dans cet exemple, le trafic RDMA est mappé au groupe CS 5 et le trafic iSCSI est mappé au groupe CS 4. La Ingress policy est utilisée sur les ports de commutateur connectant les interfaces MetroCluster et sur les ports ISL transportant le trafic MetroCluster.

Exemple:

```
policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

NetApp vous recommande de façonner le trafic sur les ports de commutateur qui connectent une interface MetroCluster, comme illustré ci-dessous :

Exemple:

```
policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn
```

Exemples de configuration des ports de nœud

Vous devrez peut-être configurer un port de nœud en mode écorché. Dans l'exemple suivant, les ports 25 et 26 sont configurés en mode écorché 4 x 25 Gbit/s.

Exemple:

```
interface breakout module 1 port 25-26 map 25g-4x
```

Vous devrez peut-être configurer la vitesse du port de l'interface MetroCluster. L'exemple suivant montre comment configurer la vitesse en mode **auto** ou 40 Gbit/s :

Exemple:

```
    speed auto

    speed 40000
```

L'exemple suivant montre un port de commutateur configuré pour connecter une interface MetroCluster. Il s'agit d'un port en mode d'accès dans le VLAN 10, avec un MTU de 9 9216 et fonctionne en vitesse native. Le contrôle de flux (pause) symétrique (envoi et réception) est activé et les règles d'entrée et de sortie MetroCluster sont attribuées.

Exemple:

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown
```

Sur les ports 25 Gbit/s, vous devrez peut-être définir le paramètre correction d'erreur de transfert (FEC) sur « Désactivé », comme illustré dans l'exemple suivant.

Exemple:

```
fec off
```

Exemples de configuration des ports ISL dans l'ensemble du réseau

Un commutateur compatible avec MetroCluster est considéré comme un commutateur intermédiaire, même s'il connecte directement les interfaces MetroCluster. Les ports ISL transportant le trafic MetroCluster sur le commutateur compatible MetroCluster doivent être configurés de la même manière que les ports ISL sur un commutateur intermédiaire. Reportez-vous à la section "Réglages requis sur les commutateurs intermédiaires" pour obtenir des conseils et des exemples.

Certaines cartes de règles sont identiques pour les ports de switch qui connectent les interfaces MetroCluster et les liens ISL transportant le trafic MetroCluster. Vous pouvez utiliser le même mappage de stratégie pour ces deux utilisations de port.

En savoir plus sur les agrégats non mis en miroir dans les configurations IP MetroCluster

Si votre configuration inclut des agrégats sans mise en miroir, vous devez connaître les problèmes d'accès potentiels après les opérations de basculement.

Agrégats non mis en miroir et espaces de noms hiérarchiques

Si vous utilisez des espaces de noms hiérarchiques, vous devez configurer le chemin de jonction de sorte que tous les volumes de ce chemin soient sur des agrégats en miroir uniquement ou sur des agrégats non mis en miroir uniquement. La configuration d'agrégats non mis en miroir et en miroir dans le chemin de jonction peut empêcher l'accès aux agrégats non mis en miroir après le basculement.

Agrégats non mis en miroir et maintenance nécessitant une coupure de courant

Si vous effectuez une commutation négociée pour la maintenance qui nécessite une coupure de courant à l'échelle du site, vous devez d'abord mettre hors ligne manuellement tous les agrégats non mis en miroir appartenant au site sinistré.

Si vous ne mettez pas hors ligne les agrégats non mis en miroir appartenant au site sinistré, les nœuds du site survivant risquent de tomber en panne en raison de paniques multidisques. Cela peut se produire si des agrégats non mis en miroir commutés sont hors ligne ou manquants en raison d'une perte de connectivité au stockage du site sinistré suite à une coupure de courant ou à une perte de ISL.

Agrégats non mis en miroir, volumes de métadonnées CRS et volumes racine SVM de données

Le volume des métadonnées du service de réplication de la configuration (CRS) et les volumes root du SVM de données doivent se trouver sur un agrégat en miroir. Vous ne pouvez pas déplacer ces volumes vers un agrégat non mis en miroir. S'ils se trouvent sur un agrégat non mis en miroir, les opérations de commutation et de retour négociées sont rejetées et le `metrocluster check` la commande renvoie un avertissement.

Agrégats et SVM non miroirs

Vous devez configurer les SVM uniquement sur des agrégats en miroir ou non. La configuration de SVM sur une combinaison d'agrégats en miroir et non en miroir peut entraîner une commutation de plus de 120 secondes. Cela peut entraîner une interruption de données si les agrégats non en miroir ne sont pas mis en ligne.

Agrégats non mis en miroir et SAN

Avant ONTAP 9.9.1, un LUN ne devait pas être situé sur un agrégat non mis en miroir. La configuration d'une LUN sur un agrégat non mis en miroir peut entraîner un basculement supérieur à 120 secondes et une panne de données.

Ajouter des étagères de stockage pour les agrégats non miroirs

Si vous ajoutez des étagères et souhaitez les utiliser pour des agrégats non mis en miroir dans une configuration IP MetroCluster , vous devez procéder comme suit :

1. Avant de démarrer la procédure d'ajout des tiroirs, exécutez la commande suivante :

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Vérifiez que l'assignation automatique des disques est désactivée :

   ```
   disk option show
   ```

3. Suivez les étapes de la procédure pour ajouter les étagères.
4. Attribuez manuellement tous les disques du nouveau tiroir au nœud qui sera propriétaire de l'agrégat ou des agrégats sans miroir.
5. Créez les agrégats :

   ```
   storage aggregate create
   ```

6. Après avoir terminé la procédure, exécutez la commande suivante :

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

7. Vérifiez que l'assignation automatique des disques est activée :

```
disk option show
```

Exigences relatives aux ports de pare-feu pour les configurations IP MetroCluster

Si vous utilisez un pare-feu sur un site MetroCluster, vous devez vous assurer de l'accès à certains ports requis.

Considérations relatives à l'utilisation du pare-feu sur les sites MetroCluster

Si vous utilisez un pare-feu sur un site MetroCluster, vous devez vous assurer de l'accès aux ports requis.

Le tableau suivant montre l'utilisation du port TCP/UDP dans un pare-feu externe placé entre deux sites MetroCluster.

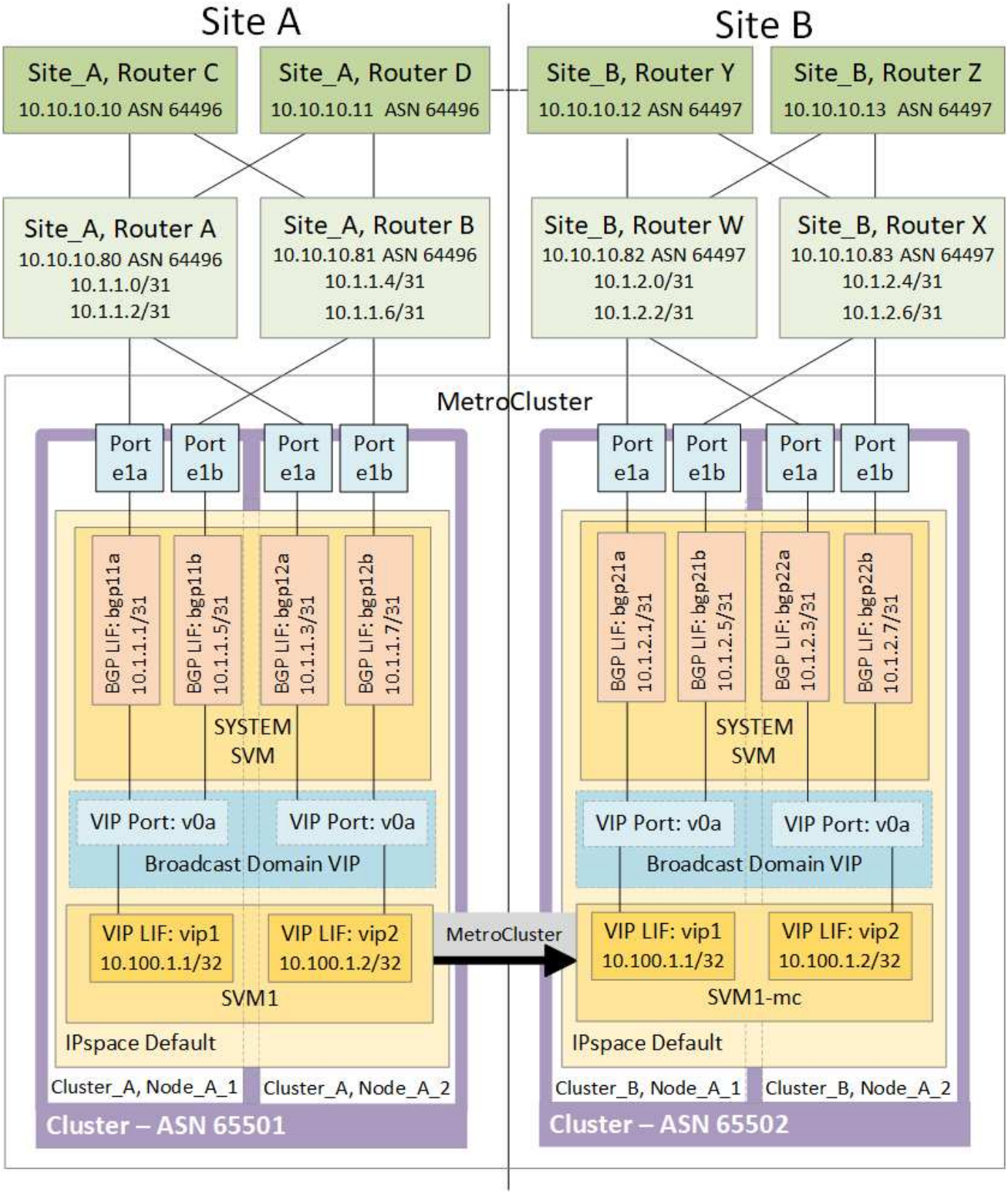
Type de trafic	Port/services
Peering de clusters	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP LIFs intercluster	65200 / TCP 10006 / TCP et UDP
Assistance matérielle	4444 / TCP

En savoir plus sur l'utilisation d'une adresse IP virtuelle et du protocole Border Gateway avec une configuration IP MetroCluster

Depuis ONTAP 9.5, ONTAP prend en charge la connectivité de couche 3 via l'adresse IP virtuelle (VIP) et le protocole BGP (Border Gateway Protocol). L'association des protocoles VIP et BGP pour la redondance dans le réseau frontal avec la redondance MetroCluster interne offre une solution de reprise après incident de couche 3.

Consultez les instructions et l'illustration suivantes lors de la planification de votre solution de couche 3. Pour plus d'informations sur l'implémentation de VIP et BGP dans ONTAP, reportez-vous à la section suivante :

"Configuration des LIFs IP virtuelles (VIP)"



Limitations de ONTAP

ONTAP ne vérifie pas automatiquement que tous les nœuds des deux sites de la configuration MetroCluster sont configurés avec le peering BGP.

ONTAP n'effectue pas l'agrégation de routes, mais annonce en permanence l'ensemble des adresses IP LIF

virtuelles individuelles en tant que routes hôtes uniques.

ONTAP ne prend pas en charge True Anycast : un seul nœud du cluster présente une adresse IP LIF virtuelle spécifique (mais il est accepté par toutes les interfaces physiques, qu'il s'agisse de LIF BGP, à condition que le port physique fasse partie du IPspace correct). Des LIF différentes peuvent migrer indépendamment les unes des autres vers des nœuds d'hébergement différents.

Instructions pour l'utilisation de cette solution de couche 3 avec une configuration MetroCluster

Vous devez configurer correctement votre BGP et votre VIP pour assurer la redondance requise.

Des scénarios de déploiement plus simples sont préférables aux architectures plus complexes (par exemple, un routeur de peering BGP est accessible sur un routeur intermédiaire non BGP). Cependant, ONTAP n'applique pas de restrictions de conception ou de topologie de réseau.

Les LIFs VIP ne couvrent que le réseau front-end/data.

Selon votre version de ONTAP, vous devez configurer les LIF de peering BGP dans le SVM nœud, et non pas dans le SVM système ou données. En 9.8, les LIF BGP sont visibles dans le SVM du cluster (system) et les SVM du nœud ne sont plus présents.

Chaque SVM de données requiert la configuration de toutes les adresses de passerelle de premier saut potentielles (en général, l'adresse IP de peering du routeur BGP), de sorte que le chemin de données de retour est disponible en cas de migration de LIF ou de basculement de MetroCluster.

Les LIF BGP sont spécifiques au nœud, comme les LIF intercluster.- chaque nœud dispose d'une configuration unique, qui n'a pas besoin d'être répliqué sur les nœuds du site de reprise après incident.

L'existence du v0a (v0b, etc.) valide en continu la connectivité, garantissant ainsi la réussite d'une migration ou d'un basculement de LIF (contrairement au niveau L2, où une configuration interrompue n'est visible qu'après l'interruption de service).

Une différence architecturale majeure est que les clients ne doivent plus partager le même sous-réseau IP que le VIP des SVM de données. Un routeur L3 avec les fonctions de résilience et de redondance adaptées à l'entreprise (par exemple VRRP/HSRP) doit être sur le chemin entre le stockage et les clients pour que le VIP fonctionne correctement.

Le processus fiable de mise à jour du protocole BGP permet de faciliter les migrations de LIF, car elles sont légèrement plus rapides et ont moins de risques d'interruption pour certains clients

Vous pouvez configurer le protocole BGP pour détecter certaines classes de comportements erronées du réseau ou du switch plus rapidement que le protocole LACP, s'il est configuré en conséquence.

Le protocole BGP (EBGP) externe utilise des nombres différents COMME des nœuds ONTAP et des routeurs de peering. Il est le déploiement privilégié pour faciliter l'agrégation et la redistribution des routes sur les routeurs. Le protocole BGP interne (IBGP) et l'utilisation de réflecteurs de routage ne sont pas impossibles mais hors du champ d'application d'une configuration VIP simple.

Après le déploiement, il faut vérifier que la SVM de données est accessible lorsque la LIF virtuelle associée est migrée entre tous les nœuds sur chaque site (y compris le basculement MetroCluster) afin de vérifier la configuration correcte des routes statiques vers le même SVM de données.

VIP fonctionne pour la plupart des protocoles IP (NFS, SMB, iSCSI).

Configurer les composants matériels de MetroCluster

En savoir plus sur les interconnexions des composants matériels dans une configuration IP MetroCluster

Lors de la planification de votre configuration IP MetroCluster, vous devez connaître les composants matériels et les interconnexions.

Principaux éléments matériels

Une configuration MetroCluster IP inclut les éléments matériels clés suivants :

- Contrôleurs de stockage

  Les contrôleurs de stockage sont configurés en tant que clusters à deux nœuds.

- Réseau IP

  Ce réseau IP interne assure la connectivité pour deux utilisations distinctes :

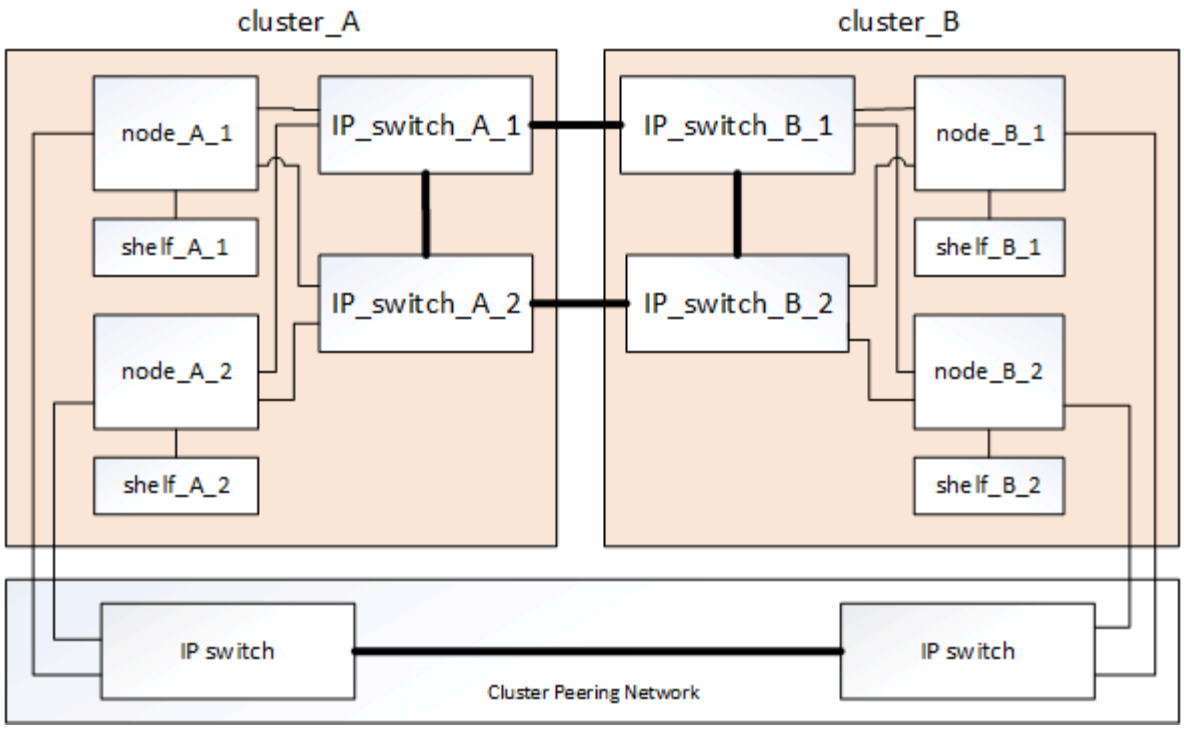
  - Connectivité standard du cluster pour les communications intra-cluster.

    Il s'agit de la même fonctionnalité de commutateur de cluster que celle utilisée dans les clusters ONTAP avec commutateur non MetroCluster.

  - Connectivité back-end MetroCluster pour la réplication des données de stockage et du cache non volatile.

- Réseau de peering de cluster

  Le réseau de peering de cluster assure la connectivité en miroir de la configuration du cluster, y compris la configuration de la machine virtuelle de stockage (SVM). La configuration de l'ensemble des SVM sur un cluster est mise en miroir sur le cluster partenaire.



Groupes de reprise après incident

Une configuration MetroCluster IP se compose d'un groupe de reprise sur incident de quatre nœuds.

L'illustration ci-dessous présente l'organisation des nœuds dans une configuration MetroCluster à quatre nœuds :

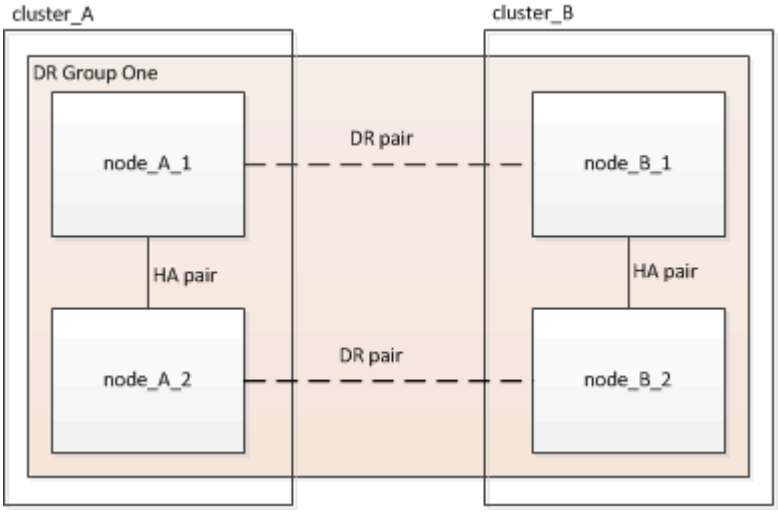
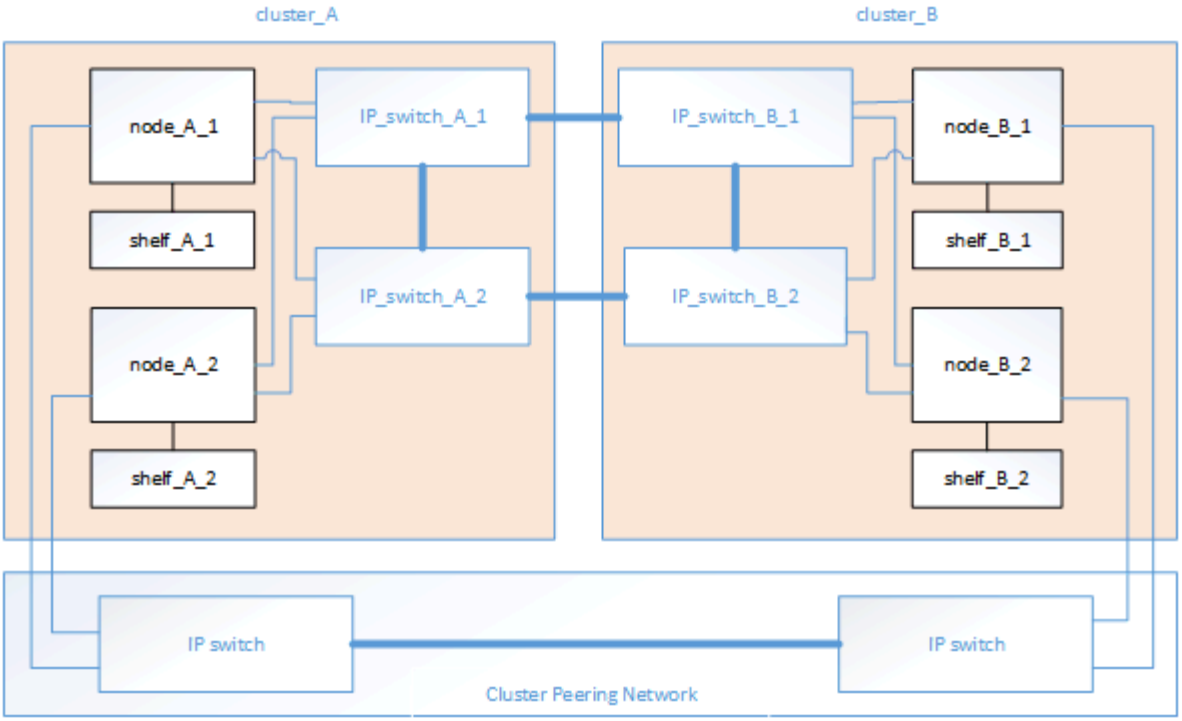


Illustration des paires haute disponibilité locales dans une configuration MetroCluster

Chaque site MetroCluster se compose de contrôleurs de stockage configurés en tant que paire haute disponibilité. Ceci permet la redondance locale afin que, en cas de panne d'un contrôleur de stockage, son partenaire de haute disponibilité local puisse reprendre le contrôle. Il est possible de gérer de telles défaillances sans effectuer de basculement MetroCluster.

Les opérations de basculement et de rétablissement de la haute disponibilité locale sont exécutées à l'aide des commandes de basculement du stockage, de la même manière qu'une configuration non MetroCluster.

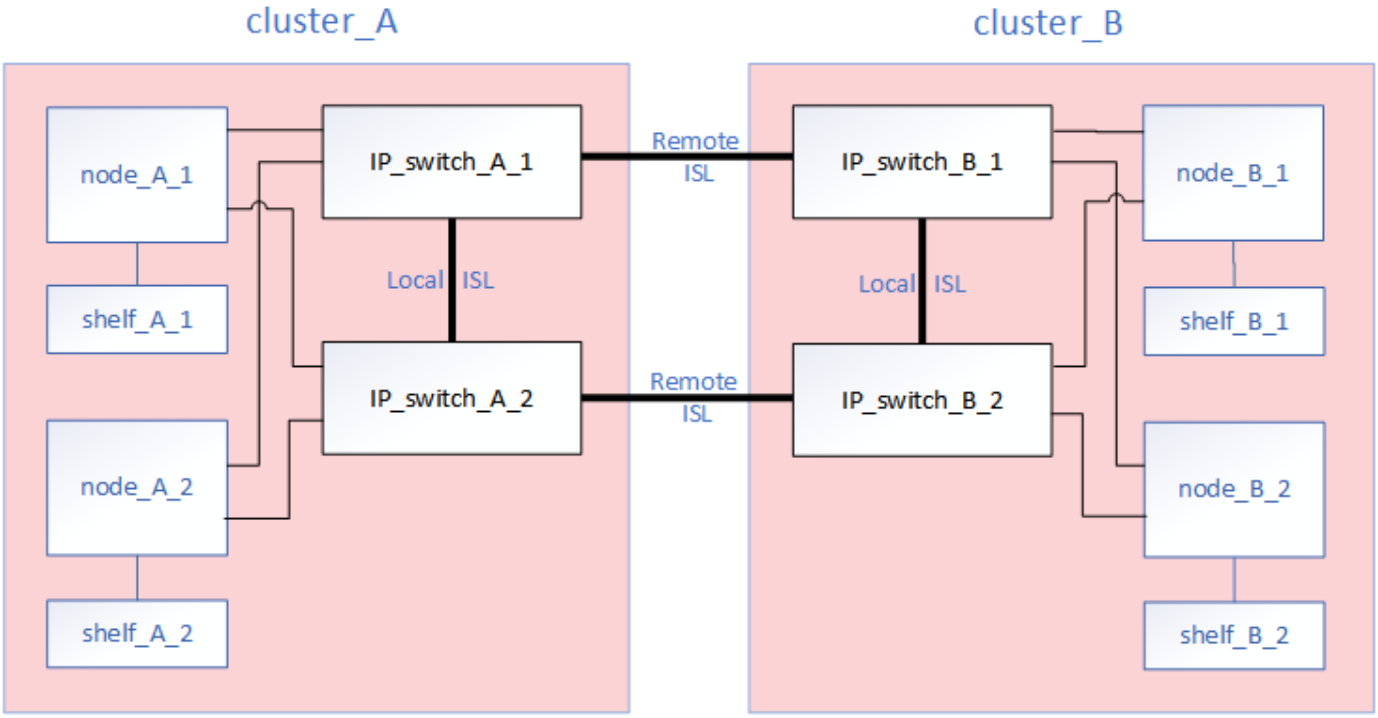


Informations associées

"Concepts relatifs à ONTAP"

Illustration du réseau d'interconnexion de cluster et IP de MetroCluster

Les clusters ONTAP incluent généralement un réseau d'interconnexion de cluster pour le trafic entre les nœuds du cluster. Dans les configurations IP MetroCluster, ce réseau est également utilisé pour le trafic de réplication des données entre les sites MetroCluster.

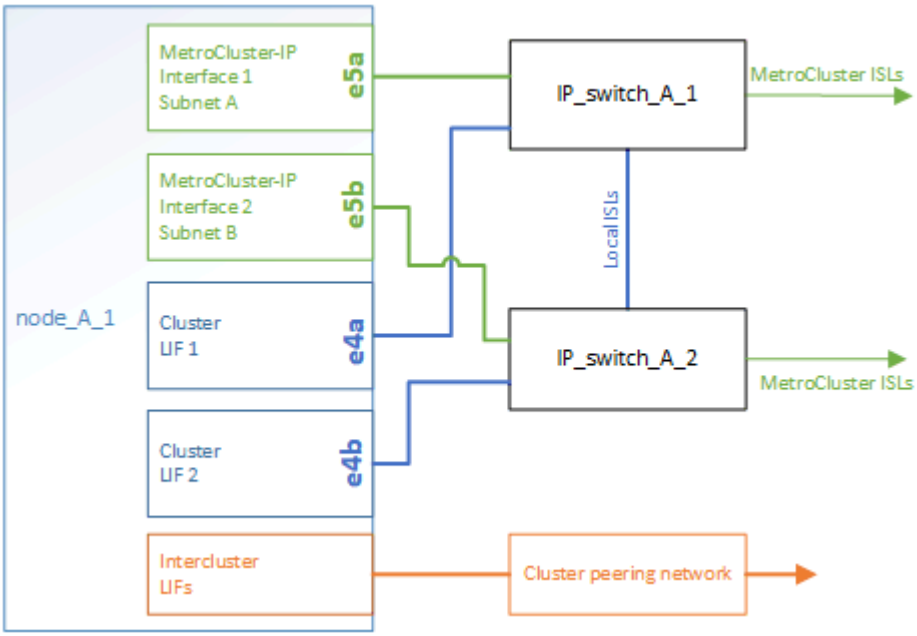


Chaque nœud de la configuration IP MetroCluster dispose d'interfaces dédiées pour la connexion au réseau IP

back-end :

- Deux interfaces IP MetroCluster
- Deux interfaces locales du cluster

L'illustration suivante montre ces interfaces. L'utilisation des ports correspond à un système AFF A700 ou FAS9000.



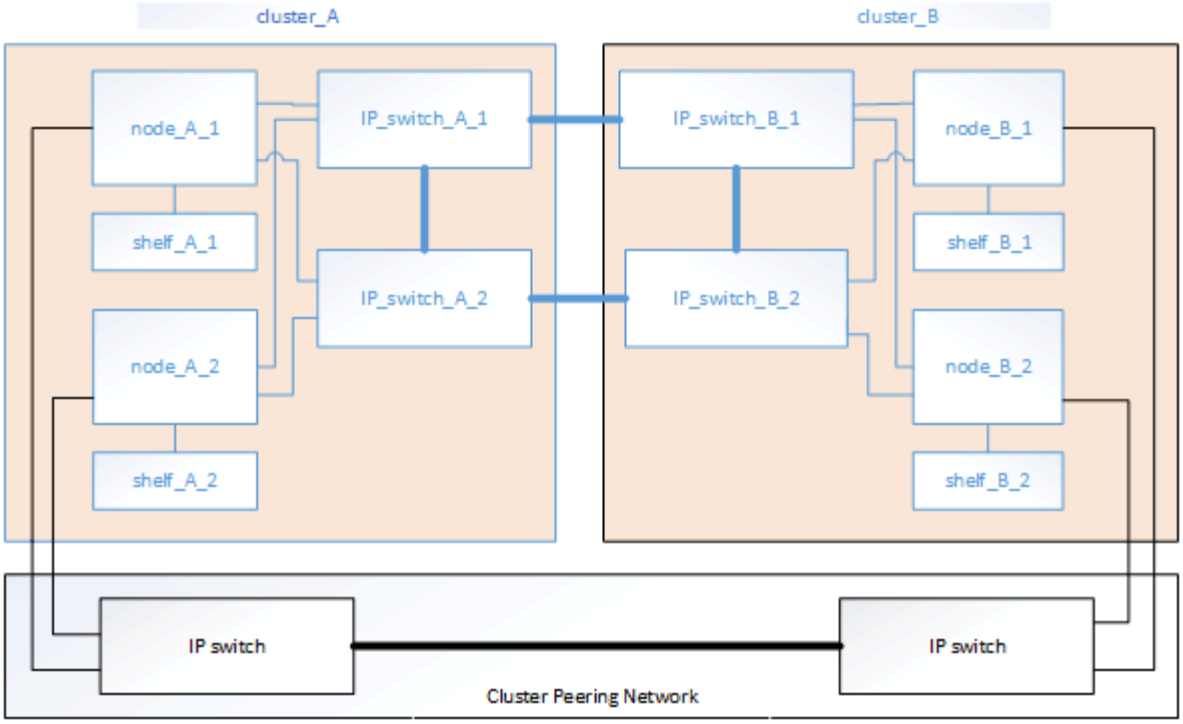
Informations associées

"Considérations relatives aux configurations MetroCluster IP"

Illustration du réseau de peering de cluster

Les deux clusters de la configuration MetroCluster sont peering via un réseau de peering de cluster fourni par le client. Le peering de clusters prend en charge la mise en miroir synchrone des machines virtuelles de stockage (SVM, anciennement appelées vServers) entre les sites.

Les LIFs intercluster doivent être configurées sur chaque nœud en configuration MetroCluster, et les clusters doivent être configurés pour le peering. Les ports disposant des LIFs intercluster sont connectés au réseau de peering de cluster fourni par le client. La réplication de la configuration SVM est effectuée sur ce réseau via le Service de réplication de configuration.



Informations associées

"Configuration cluster et SVM peering express"

"Facteurs à prendre en compte lors de la configuration du peering de clusters"

"Câblage des connexions de peering de cluster"

"Peering des clusters"

Composants de configuration IP MetroCluster requis et conventions de dénomination

Identifiez les composants matériels et logiciels requis et pris en charge pour une configuration IP MetroCluster . Examinez les conventions d'appellation utilisées par les exemples de documentation pour les composants.

Logiciels et matériel pris en charge

Le matériel et le logiciel doivent être pris en charge pour la configuration MetroCluster IP.

"NetApp Hardware Universe"

Lorsque vous utilisez des systèmes AFF, tous les modules de contrôleur de la configuration MetroCluster doivent être configurés en tant que systèmes AFF.

La redondance matérielle est requise dans une configuration MetroCluster IP

En raison de la redondance matérielle de la configuration IP MetroCluster, chaque site compte deux composants. Les lettres A et B sont attribuées arbitrairement aux sites, et les chiffres 1 et 2 sont attribués de façon arbitraire aux composantes individuelles.

Configuration requise pour le cluster ONTAP dans une configuration IP MetroCluster

Les configurations IP MetroCluster requièrent deux clusters ONTAP, un sur chaque site MetroCluster.

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

- Site A : cluster_A
- Site B : cluster_B

Configuration du commutateur IP requise dans une configuration MetroCluster IP

Les configurations IP de MetroCluster requièrent quatre commutateurs IP. Les quatre commutateurs forment deux fabrics de stockage de switch qui fournissent l'ISL entre chacun des clusters dans la configuration IP de MetroCluster.

Les commutateurs IP offrent également une communication intracluster entre les modules de contrôleur de chaque cluster.

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

- Site A : cluster_A
  - IP_switch_A_1
  - IP_Switch_A_2
- Site B : cluster_B
  - IP_Switch_B_1
  - IP_Switch_B_2

Configuration requise pour le module de contrôleur dans une configuration IP MetroCluster

Les configurations IP de MetroCluster requièrent quatre ou huit modules de contrôleur.

Les modules de contrôleur de chaque site forment une paire haute disponibilité. Chaque module de contrôleur dispose d'un partenaire de reprise sur incident sur l'autre site.

Chaque module de contrôleur doit exécuter la même version de ONTAP. Les modèles de plateforme pris en charge dépendent de la version ONTAP :

- Les nouvelles installations IP MetroCluster sur les systèmes FAS ne sont pas prises en charge par ONTAP 9.4.

  Les configurations IP MetroCluster existantes sur les systèmes FAS peuvent être mises à niveau vers ONTAP 9.4.

- Depuis ONTAP 9.5, les nouvelles installations MetroCluster IP sur les systèmes FAS sont prises en charge.
- Depuis ONTAP 9.4, les modules de contrôleur configurés pour ADP sont pris en charge.

Exemples de noms

Les noms d'exemple suivants sont utilisés dans la documentation :

- Site A : cluster_A
  - Controller_A_1
  - Contrôleur_A_2
- Site B : cluster_B
  - Contrôleur_B_1
  - Contrôleur_B_2

Configuration de la carte Gigabit Ethernet requise dans une configuration IP MetroCluster

Les configurations IP MetroCluster utilisent un adaptateur Ethernet 40/100 Gbits/s ou 10/25 Gbits/s pour les interfaces IP vers les commutateurs IP utilisés pour la structure IP MetroCluster.

Les ports intégrés sont intégrés au matériel du contrôleur (slot 0) et ne peuvent pas être remplacés. Le slot requis pour l'adaptateur n'est donc pas applicable.

Modèle de plateforme	Adaptateur Gigabit Ethernet requis	Logement requis pour l'adaptateur	Ports
AFF A900, ASA A900 et FAS9500	X91146A	Emplacement 5, emplacement 7	e5b, e7b **Remarque :** les ports e5a et e7a ne peuvent être utilisés que pour les LIF interclusters. Ils ne peuvent pas être utilisés pour une LIF de données.
AFF A700 ET FAS9000	X91146A-C.	Emplacement 5	e5a, e5b
AFF A800, AFF C800, ASA A800 et ASA C800	Ports X1146A/intégrés	Logement 1/ne s'applique pas aux ports intégrés	e0b. e1b
FAS8300, AFF A400, ASA A400, ASA C400, AFF C400	X1146A	Emplacement 1	e1a, e1b
AFF A300, FAS8200	X1116A	Emplacement 1	e1a, e1b
FAS2750, AFF A150, ASA A150, AFF A220	Ports intégrés	Sans objet	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250, AFF C250	Ports intégrés	Sans objet	e0c, e0d

AFF A320	Ports intégrés	Sans objet	e0g, e0h
AFF A70, FAS70, AFF C80	X50132A	Emplacement 2	e2a, e2b
AFF A90, AFF A1K, FAS90	X50132A	Emplacement 2, emplacement 3	e2b, e3b **Remarque :** les ports e2a et e3a doivent rester inutilisés. L'utilisation de ces ports pour les réseaux frontaux ou le peering n'est pas prise en charge.
AFF A50	X60134A	Emplacement 2	e2a, e2b
AFF A30, AFF C30, AFF C60, FAS50	X60134A	Emplacement 2	e2a, e2b
AFF A20	X60132A	Emplacement 4, emplacement 2	e2b, e4b

"En savoir plus sur l'affectation automatique des disques et les systèmes ADP dans les configurations MetroCluster IP".

Exigences relatives au pool et au disque (minimum pris en charge)

Une configuration IP MetroCluster à quatre nœuds nécessite la configuration minimale sur chaque site :

- Chaque nœud possède au moins un pool local et un pool distant au niveau du site.
- Au moins sept disques dans chaque pool.

  Dans une configuration MetroCluster à quatre nœuds avec un seul agrégat de données en miroir par nœud, la configuration minimale requiert 24 disques sur le site.

> Les noms des agrégats doivent être uniques sur l'ensemble des MetroCluster sites. Cela signifie que vous ne pouvez pas avoir deux agrégats différents portant le même nom sur le site A et le site B.

Dans une configuration minimale prise en charge, chaque pool dispose de la disposition de disque suivante :

- Trois disques racine
- Trois disques de données
- Un disque de rechange

Dans une configuration minimale prise en charge, au moins un tiroir est requis par site.

Les configurations MetroCluster prennent en charge RAID-DP, RAID4 et RAID-TEC.

Depuis ONTAP 9.4, les configurations IP de MetroCluster prennent en charge les nouvelles installations à l'aide d'un partitionnement de disque avancé et d'une affectation automatique des disques. Pour plus d'informations, reportez-vous à la section "Considérations relatives à l'affectation automatique des lecteurs et aux systèmes ADP" .

Considérations relatives à l'emplacement des disques pour les tiroirs partiellement remplis

Pour l'affectation automatique correcte des disques lorsque des tiroirs sont à moitié remplis (12 disques dans un tiroir de 24 disques), les disques doivent être situés dans les emplacements 0-5 et 18-23.

Dans une configuration avec un tiroir partiellement rempli, les disques doivent être répartis de manière égale dans les quatre quadrants du shelf.

Considérations relatives à l'emplacement des disques pour les disques internes AFF A800

Pour une mise en œuvre correcte de la fonction ADP, les emplacements des disques du système AFF A800 doivent être répartis en trimestres et les disques doivent être placés symétriquement au cours des trimestres.

Un système AFF A800 dispose de 48 baies de disque. Les baies peuvent être divisées en quatre :

- Premier trimestre :
  - Baies 0 - 5
  - Baies 24 - 29
- Deuxième trimestre :
  - Baies 6 - 11
  - Baies 30 - 35
- Troisième trimestre :
  - Baies 12 - 17
  - Baies 36 - 41
- Quatrième trimestre :
  - Baies 18 - 23
  - Baies 42 - 47

Si ce système est équipé de 16 disques durs, ils doivent être répartis symétriquement entre les quatre trimestres :

- Quatre disques au premier trimestre : 0, 1, 2, 3
- Quatre disques au deuxième trimestre : 6, 7, 8, 9
- Quatre disques au troisième trimestre : 12, 13, 14, 15
- Quatre disques au quatrième trimestre : 18, 19, 20, 21

Montez les composants matériels de configuration IP MetroCluster

Si vous n'avez pas reçu l'équipement déjà installé dans les armoires, vous devez installer les composants en rack.

Description de la tâche

Cette tâche doit être effectuée sur les deux sites MetroCluster.

Étapes

1. Planifiez le positionnement des composants MetroCluster.

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

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

   Suivez les étapes pour *Installer le matériel* sous les instructions *Installer et configurer* pour votre modèle de plate-forme dans le"Documentation des systèmes matériels ONTAP" .

4. Installez les commutateurs IP sur le rack ou l'armoire.
5. Installez les tiroirs disques, mettez-les sous tension, puis définissez les ID de tiroir.

   - Vous devez mettre chaque tiroir disque hors tension puis sous tension.
   - Il est vivement recommandé d'utiliser des ID de tiroir unique pour chaque tiroir disque SAS dans chaque groupe MetroCluster DR afin de faciliter le dépannage.

   > Ne câisez pas les tiroirs disques destinés à contenir actuellement des agrégats non mis en miroir. Vous devez patienter jusqu'à la fin de la configuration de MetroCluster et déployer les tiroirs destinés aux agrégats sans mise en miroir après l'utilisation de `metrocluster modify -enable-unmirrored-aggr-deployment true` commande.

Branchez les câbles des commutateurs IP MetroCluster

Comment utiliser les tables de ports avec plusieurs configurations IP MetroCluster

Vous devez comprendre comment utiliser les informations des tables de ports pour générer correctement vos fichiers RCF.

Avant de commencer

Vérifiez les points suivants avant d'utiliser les tableaux :

- Les tableaux suivants indiquent l'utilisation des ports pour le site A. Le même câblage est utilisé pour le site B.
- Vous ne pouvez pas configurer les commutateurs avec des ports de vitesses différentes (par exemple, un mélange de ports 100 Gbit/s et de ports 40 Gbit/s).
- Conservez une trace du groupe de ports MetroCluster (MetroCluster 1, MetroCluster 2, etc.). Vous aurez besoin de ces informations lors de l'utilisation de l'outil RcfFileGenerator comme décrit plus loin dans cette procédure de configuration.
- Vous devez câbler tous les nœuds de la même manière. Si différentes options de combinaison de ports sont disponibles pour câbler les nœuds, tous les nœuds doivent utiliser les mêmes combinaisons de ports. Par exemple, e1a sur le nœud 1 et e1a sur le nœud 2 doivent être connectés à un commutateur. De même, le second port des deux nœuds doit être connecté au second switch.
- Le "RcfFileGenerator pour MetroCluster IP" fournit également une vue d'ensemble du câblage par port pour chaque commutateur. Utilisez cette présentation du câblage pour vérifier votre câblage.

Câblage de deux configurations MetroCluster aux commutateurs

Lorsque vous connectez plusieurs configurations MetroCluster à un commutateur, connectez chaque MetroCluster conformément au tableau approprié. Par exemple, si vous connectez un FAS2750 et un AFF A700 au même commutateur, connectez le FAS2750 selon « MetroCluster 1 » du tableau 1, et l'AFF A700 selon « MetroCluster 2 » ou « MetroCluster 3 » du tableau 2. Vous ne pouvez pas connecter physiquement les systèmes FAS2750 et AFF A700 comme « MetroCluster 1 ».

Câblage des configurations MetroCluster à 8 nœuds

Pour la configuration MetroCluster qui exécute ONTAP 9.8 et les versions antérieures, certaines procédures de transition vers la mise à niveau requièrent l'ajout d'un deuxième groupe de reprise après incident à quatre nœuds à la configuration afin de créer une configuration temporaire à huit nœuds. Depuis la version ONTAP 9.9.1, les configurations MetroCluster permanentes à huit nœuds sont prises en charge.

Description de la tâche

Pour les configurations à huit nœuds, utilisez la même méthode que celle décrite ci-dessus. Au lieu d'un deuxième MetroCluster, vous câbler un autre groupe de reprise après incident à quatre nœuds.

Par exemple, votre configuration inclut les éléments suivants :

- Commutateurs Cisco 3132Q-V
- MetroCluster 1 : plateformes FAS2750
- MetroCluster 2 : plateformes AFF A700 (ces plateformes sont ajoutées comme deuxième groupe de reprise après incident à quatre nœuds)

Étapes

1. Pour le MetroCluster 1, reliez les commutateurs Cisco 3132Q-V à l'aide du tableau correspondant à la plateforme FAS2750 et aux rangées pour les interfaces MetroCluster 1.
2. Pour MetroCluster 2 (deuxième groupe DR), reliez les commutateurs Cisco 3132Q-V à l'aide du tableau pour la plateforme AFF A700 et les lignes pour les interfaces MetroCluster 2.

Affectations de ports de plate-forme pour les commutateurs Cisco 3132Q-V dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez ces directives avant d'utiliser les tableaux :

- Si vous configurez le commutateur pour la transition FC vers IP MetroCluster, le port 5, le port 6, le port 13 ou le port 14 peuvent être utilisés pour connecter les interfaces de cluster locales du nœud FC MetroCluster. Reportez-vous à la "RcfFileGenerator" et les fichiers de câblage générés pour plus de détails sur le câblage de cette configuration. Pour toutes les autres connexions, vous pouvez utiliser les affectations d'utilisation des ports répertoriées dans les tableaux.

Choisissez la table de câblage adaptée à votre configuration

Utilisez le tableau suivant pour déterminer la table de câblage que vous devez suivre.

Si votre système est…	Utilisez ce tableau de câblage…
FAS2750, AFF A220	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 1)
FAS9000, AFF A700	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 2)
AFF A800, ASA A800	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 3)

Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 1)

Vérifiez les attributions de ports de la plateforme pour connecter un système FAS2750 ou AFF A220 à un commutateur Cisco 3132Q-V :

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 2)

Vérifiez les attributions de ports de plateforme pour connecter un système FAS9000 ou AFF A700 à un commutateur Cisco 3132Q-V :

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 3)

Vérifiez les affectations des ports de la plateforme pour relier un système AFF A800 ou ASA A800 à un commutateur Cisco 3132Q-V :

Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Affectations de ports de plate-forme pour les commutateurs Cisco 3232C ou Cisco 9336C à 36 ports dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez les considérations suivantes avant d'utiliser les tableaux de configuration :

- Les tableaux de cette section concernent les commutateurs Cisco 3232C ou les commutateurs Cisco 9336C-FX2 à 36 ports qui ne connectent pas le stockage NS224.

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 12 ports, utilisez les tableaux de "Affectations de ports de plate-forme pour les commutateurs Cisco 9336C-FX2 à 12 ports" .

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 36 ports et qu'au moins une configuration MetroCluster ou un groupe DR connecte des étagères NS224 au commutateur MetroCluster, utilisez les tableaux de "Affectations de ports de plate-forme pour un commutateur Cisco 9336C-FX2 à 36 ports connectant un stockage NS224" .

- Les tableaux suivants indiquent l'utilisation des ports pour le site A. Le même câblage est utilisé pour le site B.
- Vous ne pouvez pas configurer les commutateurs avec des ports de vitesses différentes (par exemple, un mélange de ports 100 Gbit/s et de ports 40 Gbit/s).
- Si vous configurez un seul MetroCluster avec les commutateurs, utilisez le groupe de ports **MetroCluster 1**.

  Gardez une trace du groupe de ports MetroCluster (MetroCluster 1, MetroCluster 2, MetroCluster 3 ou MetroCluster 4). Vous en aurez besoin lorsque vous utilisez l'outil RcfFileGenerator comme décrit plus loin dans cette procédure de configuration.

- Le RcfFileGenerator pour MetroCluster IP fournit également une vue d'ensemble du câblage par port pour chaque commutateur.

  Utilisez cette présentation du câblage pour vérifier votre câblage.

- Le fichier RCF version 2.10 ou ultérieure est requis pour le mode d'écorché 25G pour les liens ISL MetroCluster.
- ONTAP 9.13.1 ou version ultérieure et le fichier RCF version 2.00 sont requis pour utiliser une plateforme autre que FAS8200 ou AFF A300 dans le groupe « MetroCluster 4 ».

> La version du fichier RCF est différente de celle de l'outil RCFfilegenerator utilisé pour générer le fichier. Par exemple, vous pouvez générer un fichier RCF version 2.00 à l'aide de RCFfilegenerator v1.6c.

Choisissez la table de câblage adaptée à votre configuration

Utilisez le tableau suivant pour déterminer la table de câblage que vous devez suivre.

Si votre système est…	Utilisez ce tableau de câblage…
AFF A150, ASA A150 FAS2750, AFF A220 FAS500f, AFF C250, ASA C250 AFF A250, ASA A250	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 1)
AFF A20	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 2)
AFF A30, AFF C30 FAS50 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 3a) ou 100G (groupe 3b). • Attributions des ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 3a - 25G) • Attributions des ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 3b - 100G)
FAS8200, AFF A300	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 4)

Si votre système est…	Utilisez ce tableau de câblage…
AFF A320, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 5)
AFF A50	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 6)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 7)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 8)

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 1)

Passez en revue les affectations des ports de la plateforme pour connecter les câbles des systèmes AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, système AFF C250, ASA C250, AFF A250 ou ASA A250 vers un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 2)

Vérifier les attributions de ports de plateforme pour relier un système AFF A20 à un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e2a	e4a
5/2-4		disabled	
6/1		e2a	e4a
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e2b	e4b
13/2-4		disabled	
14/1		e2b	e4b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e2b	e4b
25/2-4		disabled	
26/1		e2b	e4b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e2a	e4a
29/2-4		disabled	
30/1		e2a	e4a
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Attributions de port de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 3a)

Vérifiez les attributions de ports de la plateforme pour connecter un système AFF A30, AFF C30, AFF C60 ou FAS50 à un switch Cisco 3232C ou 9336C-FX2 à l'aide d'une carte Ethernet 25G à quatre ports.

Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5/1	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5/2-4		disabled		disabled		disabled	
6/1		e4a	e4b	e4a	e4b	e4a	e4b
6/2-4		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29/1	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
29/2-4		disabled		disabled		disabled	
30/1		e4a	e4b	e4a	e4b	e4a	e4b
30/2-4		disabled		disabled		disabled	
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Attributions des ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 3b)

Vérifiez les attributions de ports de la plateforme pour connecter un système AFF A30, AFF C30, AFF C60 ou FAS50 à un switch Cisco 3232C ou 9336C-FX2 à l'aide d'une carte Ethernet 100 Gbit/s à deux ports.

Cette configuration nécessite une carte Ethernet 100G à deux ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
30		e4a	e4b	e4a	e4b	e4a	e4b
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 4)

Vérifiez les attributions de ports de plateforme pour connecter un système FAS8200 ou AFF A300 à un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Si vous effectuez une mise à niveau à partir d'anciens fichiers RCF, la configuration du câblage peut utiliser des ports du groupe « MetroCluster 4 » (ports 25/26 et 29/30).

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 5)

Consultez les attributions de ports de plateforme pour connecter les systèmes AFF A320, FAS8300, AFF C400, ASA C400, FAS8700, système AFF A400 ou ASA A400 vers un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

L'utilisation de ports dans le groupe « MetroCluster 4 » nécessite ONTAP 9.13.1 ou version ultérieure.

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 6)

Vérifier les attributions de ports de plateforme pour relier un système AFF A50 à un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6		e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b
14		e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25	MetroCluster 4, MetroCluster interface	e2a	e2b
26		e2a	e2b
27 - 28	Unused	disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b
30		e4a	e4b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 7)

Consultez les affectations des ports de plateforme pour connecter les câbles des systèmes FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, système ASA A800, FAS9500, AFF A900 ou ASA A900 vers un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Remarque 1 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

L'utilisation de ports dans le groupe « MetroCluster 4 » nécessite ONTAP 9.13.1 ou version ultérieure.

Attributions de ports de la plateforme Cisco 3232C ou Cisco 9336C-FX2 (groupe 8)

Vérifier les attributions de ports de plateforme pour connecter un système AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K à un switch Cisco 3232C ou 9336C-FX2 :

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16									
17									
18									
19									
20									
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4									
23/1-4									
24/1-4									
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
26									
27 - 28	Unused	disabled		disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
30									
31 - 32	Unused	disabled		disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	

Affectations de ports de plate-forme pour les commutateurs Cisco 9336C-FX2 à 12 ports dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez les considérations suivantes avant d'utiliser les tableaux de configuration :

- Les tableaux de cette section concernent les commutateurs Cisco 9336C-FX2 à 12 ports.

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 36 ports qui ne connecte pas d'étagères NS224, utilisez les tableaux de "Affectations de ports de plate-forme pour les commutateurs Cisco 3232C ou Cisco 9336C-FX2 à 36 ports" .

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 36 ports et qu'au moins une configuration MetroCluster ou un groupe DR connecte des étagères NS224 au commutateur MetroCluster, utilisez les tableaux de "Affectations de ports de plate-forme pour un commutateur Cisco 9336C-FX2 à 36 ports connectant un stockage NS224" .

> Le commutateur Cisco 9336C-FX2 à 12 ports ne prend pas en charge la connexion des étagères NS224 au commutateur MetroCluster.

- Les tableaux suivants indiquent l'utilisation des ports pour le site A. Le même câblage est utilisé pour le site B.
- Vous ne pouvez pas configurer les commutateurs avec des ports de vitesses différentes (par exemple, un mélange de ports 100 Gbit/s et de ports 40 Gbit/s).
- Si vous configurez un seul MetroCluster avec les commutateurs, utilisez le groupe de ports **MetroCluster 1**.

Suivez le groupe de ports MetroCluster (MetroCluster 1, MetroCluster 2). Vous en aurez besoin pour utiliser l'outil RcfFileGenerator, comme décrit plus loin dans cette procédure de configuration.

- Le RcfFileGenerator pour MetroCluster IP fournit également une vue d'ensemble du câblage par port pour chaque commutateur.

Choisissez la table de câblage adaptée à votre configuration

Utilisez le tableau suivant pour déterminer la table de câblage que vous devez suivre.

Si votre système est…	Utilisez ce tableau de câblage…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 1)
AFF A20	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 2)
AFF A30, AFF C30 FAS50 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 3a) ou 100G (groupe 3b). • Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3a - 25G) • Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3b - 100G)
FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 4)
AFF A50	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 5)
AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 7)

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 1)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1-4	Unused	disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13-18	Ports disallowed to use	blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 2)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A20 à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3a)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A30, AFF C30, AFF C60 ou FAS50 à un commutateur Cisco 9336C-FX2 à 12 ports à l'aide d'une carte Ethernet 25G à quatre ports.

Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3b)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A30, AFF C30, AFF C60 ou FAS50 à un commutateur Cisco 9336C-FX2 à 12 ports à l'aide d'une carte Ethernet 100G à deux ports.

Cette configuration nécessite une carte Ethernet 100G à deux ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 4)

Passez en revue les affectations de ports de la plate-forme pour câbler un système FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b
2					
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b
10					
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 5)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A50 à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 6)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
3 4	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
5-6	Ports disallowed to use	blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
13-18	Ports disallowed to use	blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Remarque 2 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 7)

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K à un commutateur Cisco 9336C-FX2 à 12 ports :

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked		blocked		blocked	

Remarque 1 : vous ne pouvez configurer que les ports 19 et 20 **ou** les ports 21 et 22. Si vous utilisez d'abord les ports 19 et 20, les ports 21 et 22 sont bloqués. Si vous utilisez d'abord les ports 21 et 22, les ports 19 et 20 sont bloqués.

Affectations de ports de plate-forme pour un commutateur Cisco 9336C-FX2 à 36 ports connectant un stockage NS224 dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez les considérations suivantes avant d'utiliser les tableaux de configuration :

- Les tableaux de cette section concernent les commutateurs Cisco 9336C-FX2 à 36 ports lorsqu'au moins une configuration MetroCluster ou un groupe DR connecte des étagères NS224 au commutateur MetroCluster.

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 36 ports et que vous ne prévoyez pas de connecter un stockage NS224 au commutateur, utilisez les tableaux dans "Affectations de ports de plate-forme pour les commutateurs Cisco 3232C ou Cisco 9336C-FX2 à 36 ports".

  Si vous disposez d'un commutateur Cisco 9336C-FX2 à 12 ports, utilisez les tableaux de "Affectations de ports de plate-forme pour les commutateurs Cisco 9336C-FX2 à 12 ports" .

  > Le commutateur Cisco 9336C-FX2 à 12 ports ne prend pas en charge la connexion des étagères NS224 au commutateur MetroCluster.

- Lorsque vous câblez un commutateur Cisco 9336C-FX2 pour connecter un stockage NS224, vous ne pouvez avoir qu'un maximum de deux configurations MetroCluster ou groupes DR. Au moins une configuration MetroCluster ou un groupe DR doit connecter des étagères NS224 au commutateur MetroCluster. Si l'une de vos configurations MetroCluster ou groupes DR est un système qui ne prend pas en charge les étagères NS224, il ne peut être connecté qu'en tant que deuxième configuration MetroCluster ou groupe DR.

  Si votre deuxième groupe MetroCluster ou DR ne connecte pas les étagères NS224 au commutateur MetroCluster, suivez les instructions Tableaux de câblage pour les contrôleurs ne connectant pas les étagères NS224 connectées par commutateur .

- Le RcfFileGenerator affiche uniquement les plates-formes éligibles lorsque la première plate-forme est sélectionnée.
- La connexion d'une configuration MetroCluster à huit ou deux nœuds requiert ONTAP 9.14.1 ou version ultérieure.

Choisissez la table de câblage adaptée à votre configuration

Consultez le tableau d'affectation des ports correspondant à votre configuration. Cette section comporte deux ensembles de tables de câblage :

- Tableaux de câblage pour contrôleurs connectant des tiroirs NS224 reliés par un commutateur
- Tableaux de câblage pour les contrôleurs ne connectant pas les tiroirs NS224 reliés par un commutateur

Contrôleurs connectant des tiroirs NS224 reliés par un commutateur

Déterminez le tableau d'affectation des ports à suivre pour les contrôleurs qui connectent des tiroirs NS224 reliés par un commutateur.

Plateforme	Utilisez ce tableau de câblage…
AFF C30, AFF A30 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 1a) ou 100G (groupe 1b). • Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 1a - 25G) • Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 1b - 100G)
AFF A320 AFF C400, ASA C400 AFF A400, ASA A400	Commutateur Cisco 9336C-FX2 connectant les attributions de ports de la plateforme de stockage NS224 (groupe 2)
AFF A50	Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 3)
AFF A700 AFF C800, ASA C800, AFF A800 AFF A900, ASA A900	Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 4)
AFF A90 AFF A1K AFF A70 AFF C80	Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 5)

Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 1a)

Passez en revue les attributions de port de la plateforme pour connecter un système AFF A30, AFF C30 ou AFF C60 qui connecte des tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 à l'aide d'une carte Ethernet 25G à quatre ports.

Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled	
2/1		e4a	e4b	e4a	e4b
2/2-4		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled	
4/1		e4a	e4b	e4a	e4b
4/2-4		disabled		disabled	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 1b)

Passez en revue les attributions de port de la plateforme pour connecter un système AFF A30, AFF C30 ou AFF C60 qui connecte des tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 à l'aide d'une carte Ethernet 100 Gbit à deux ports.

Cette configuration nécessite une carte Ethernet 100G à deux ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Commutateur Cisco 9336C-FX2 connectant les attributions de ports de la plateforme de stockage NS224 (groupe 2)

Vérifiez les attributions de ports de la plateforme pour connecter un système AFF A320, AFF C400, ASA C400, AFF A400 ou ASA A400 qui connecte des tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 :

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
18							
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b				
28		NSM-2, e0a	NSM-2, e0b				
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 3)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A50 qui connecte des tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers connecting switch-attached shelves			
Switch Port	Port Use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b
18			
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b
20			
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)		
28			
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b

Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 4)

Vérifiez les attributions de ports de la plateforme pour connecter un système AFF A700, AFF C800, ASA C800, AFF A800, AFF A900 ou ASA A900 qui connecte des tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
18							
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Remarque 1 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

Affectation des ports de la plateforme de stockage NS224 via le commutateur Cisco 9336C-FX2 (groupe 5)

Vérifiez les attributions de ports de la plateforme pour connecter un système AFF A70, AFF C80, AFF A90 ou AFF A1K qui connecte des tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 :

Controllers connecting switch-attached shelves									
Switch Port	Port Use	AFF A70		AFF C80		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17	MetroCluster 1, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
18									
19	MetroCluster 2, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
20									
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Les contrôleurs ne connectent pas les tiroirs NS224 reliés par un commutateur

Déterminez le tableau d'affectation des ports à suivre pour les contrôleurs qui ne connectent pas les tiroirs NS224 reliés par un commutateur.

Plateforme	Utilisez ce tableau de câblage…
AFF A150, ASA A150 FAS2750, AFF A220	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 6)
AFF A20	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 7)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 8)

Plateforme	Utilisez ce tableau de câblage…
AFF C30, AFF A30 FAS50 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 9a) ou 100G (groupe 9b). • Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 9a) • Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 9b)
FAS8200, AFF A300	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 10)
AFF A320, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 11)
AFF A50	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 12)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 13)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 14)

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 6)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A150, ASA A150, FAS2750 ou AFF A220 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 7)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A20 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 8)

Vérifiez les attributions de ports de la plateforme pour câbler un système FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
9/2-4		disabled	
10/1		e0c	e0d
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
11/2-4		disabled	
12/1		e0c	e0d
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 9a)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A30, AFF C30, AFF C60 ou FAS50 qui ne connecte pas les tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 utilisant une carte Ethernet 25G à quatre ports :

Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 9b)

Passez en revue les attributions de ports de la plateforme pour câbler un système AFF A30, AFF C30, AFF C60 ou FAS50 qui ne connecte pas les tiroirs NSS24 reliés par commutateur à un commutateur Cisco 9336C-FX2 utilisant une carte Ethernet 100G à deux ports :

Cette configuration nécessite une carte Ethernet 100G à deux ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 10)

Vérifiez les attributions de ports de la plateforme pour connecter un système FAS8200 ou AFF A300 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 11)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A320, FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
3 4	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
5-6	Unused	disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
11 12	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17-36	Unused	disabled		disabled		disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 12)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A50 qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves			
Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Unused	disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
17-36	Unused	disabled	

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 13)

Vérifiez les attributions de ports de la plateforme pour câbler un système FAS9000, AFF A800, AFF C800, ASA C800, AFF A700, ASA A800, FAS9500, AFF A900 ou ASA A900 qui ne connecte pas les tiroirs NSS24

reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Remarque 1 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

Le commutateur Cisco 9336C-FX2 ne connecte pas les attributions de ports de la plateforme de stockage NS224 (groupe 14)

Vérifiez les attributions de ports de la plateforme pour câbler un système AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K qui ne connecte pas les tiroirs NSS24 reliés par un commutateur Cisco 9336C-FX2 :

Controllers not connecting switch-attached shelves									
Switch Port	Port Use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Unused	disabled		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17-36	Unused	disabled		disabled		disabled		disabled	

Affectations de ports de plate-forme pour les commutateurs IP BES-53248 pris en charge par Broadcom dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez les considérations suivantes avant d'utiliser les tableaux de configuration :

- Vous ne pouvez pas utiliser les switchs avec des ports ISL distants de différentes vitesses (par exemple, un port 25 Gbit/s connecté à un port ISL de 10 Gbit/s).

- Si vous configurez le switch pour la transition MetroCluster FC vers IP, les ports suivants sont utilisés selon la plateforme cible que vous choisissez :

Plate-forme cible	Port
FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, ou FAS8700	Ports 1 à 6, 10 Gbits/s.
Plateformes FAS8200 ou AFF A300	Ports 3 - 4 et 9 - 12, 10 Gbits/s.

- Les systèmes AFF A320 configurés avec des switchs Broadcom BES-53248 peuvent ne pas prendre en charge toutes les fonctionnalités.

  Toute configuration ou fonctionnalité qui nécessite la connexion du cluster local à un commutateur n'est pas prise en charge. Par exemple, les configurations et procédures suivantes ne sont pas prises en charge :

  - Configurations MetroCluster à 8 nœuds
  - Passez des configurations FC MetroCluster aux configurations IP MetroCluster
  - Mise à jour d'une configuration IP MetroCluster à quatre nœuds (ONTAP 9.8 et versions ultérieures)

Choisissez la table de câblage adaptée à votre configuration

Utilisez le tableau suivant pour déterminer la table de câblage que vous devez suivre.

Si votre système est…	Utilisez ce tableau de câblage…
AFF A150, ASA A150 FAS2750 AVEC AFF A220	Attributions de port de la plate-forme Broadcom BES-53248 (groupe 1)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Attributions de port de la plate-forme Broadcom BES-53248 (groupe 2)
AFF A20	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 3)
AFF C30, AFF A30 FAS50 AFF C60	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 4)
FAS8200, AFF A300	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 5)
AFF A320	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 6)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 7)

Attributions de port de la plate-forme Broadcom BES-53248 (groupe 1)

Vérifiez les attributions de port de la plate-forme pour connecter un système AFF A150, ASA A150, FAS2750 ou AFF A220 à un commutateur Broadcom BES-53248 :

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused	disabled	
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.
- Si les deux configurations MetroCluster utilisent la même plate-forme, NetApp recommande de sélectionner le groupe « MetroCluster 3 » pour une configuration et le groupe « MetroCluster 4 » pour l'autre. Si les plates-formes sont différentes, vous devez sélectionner « MetroCluster 3 » ou « MetroCluster 4 » pour la première configuration, et « MetroCluster 1 » ou « MetroCluster 2 » pour la seconde.

Attributions de port de la plate-forme Broadcom BES-53248 (groupe 2)

Vérifiez les affectations de port de la plate-forme pour connecter un système FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 à un commutateur Broadcom BES-53248 :

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.
- Si les deux configurations MetroCluster utilisent la même plate-forme, NetApp recommande de sélectionner le groupe « MetroCluster 3 » pour une configuration et le groupe « MetroCluster 4 » pour l'autre. Si les plates-formes sont différentes, vous devez sélectionner « MetroCluster 3 » ou « MetroCluster 4 » pour la première configuration, et « MetroCluster 1 » ou « MetroCluster 2 » pour la seconde.

Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 3)

Vérifiez les attributions de port de la plate-forme pour connecter un système AFF A20 à un commutateur Broadcom BES-53248 :

Physical Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e2a	e4a
2			
3	MetroCluster 2, Local Cluster interface	e2a	e4a
4			
5	MetroCluster 1, MetroCluster interface	e2b	e4b
6			
7	MetroCluster 2, MetroCluster interface	e2b	e4b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 3, Local Cluster interface (note 1)	e2a	e4a
18			
19	MetroCluster 3, MetroCluster interface (note 1)	e2b	e4b
20			
21	MetroCluster 4, Local Cluster interface (note 1)	e2a	e4a
22			
23	MetroCluster 4, MetroCluster interface (note 1)	e2b	e4b
24			
..	Ports not licensed (25 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.

Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 4)

Passez en revue les attributions de port de la plate-forme pour connecter un système AFF A30, AFF C30, AFF C60 ou FAS50 à un commutateur Broadcom BES-53248 à l'aide d'une carte Ethernet 25G à quatre ports.

- Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.
- Cette configuration nécessite un adaptateur QSFP-to-SFP+ dans la carte du contrôleur pour prendre en charge une vitesse de réseau de 25 Gbit/s.

Physical Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4							
5	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
6							
7	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9 - 12	Unused	disabled		disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 3, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
18							
19	MetroCluster 3, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
20							
21	MetroCluster 4, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
22							
23	MetroCluster 4, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
24							
..	Ports not licensed (25 - 54)						
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
54							
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
56							

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.

Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 5)

Vérifiez les attributions de ports de plateforme pour connecter un système FAS8200 ou AFF A300 à un commutateur Broadcom BES-53248 :

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.

Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 6)

Vérifiez les attributions de port de la plate-forme pour connecter un système AFF A320 à un commutateur Broadcom BES-53248 :

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
56			

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.
- **Remarque 2** : seul un MetroCluster à quatre nœuds utilisant des systèmes AFF A320 peut être connecté au commutateur.

  Les fonctionnalités nécessitant un cluster commuté ne sont pas prises en charge dans cette configuration. Cela inclut les procédures de transition et de mise à jour technologique de MetroCluster FC vers IP.

Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 7)

Consultez les affectations des ports de la plateforme pour connecter un système FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, ou le système FAS8700 vers un commutateur Broadcom BES-53248 :

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see Note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

- **Remarque 1** : l'utilisation de ces ports nécessite une licence supplémentaire.
- **Remarque 2** : seul un MetroCluster à quatre nœuds utilisant des systèmes AFF A320 peut être connecté au commutateur.

  Les fonctionnalités nécessitant un cluster commuté ne sont pas prises en charge dans cette configuration. Cela inclut les procédures de transition et de mise à jour technologique de MetroCluster FC vers IP.

Affectations de ports de plate-forme pour les commutateurs IP SN2100 pris en charge par NVIDIA dans une configuration IP MetroCluster

L'utilisation du port dans une configuration MetroCluster IP dépend du modèle de commutateur et du type de plate-forme.

Consultez les considérations suivantes avant d'utiliser les tableaux de configuration :

- La connexion d'une configuration MetroCluster à huit ou deux nœuds requiert ONTAP 9.14.1 ou version ultérieure et le fichier RCF version 2.00 ou version ultérieure.

  La version du fichier RCF est différente de celle de l'outil RCFfilegenerator utilisé pour générer le fichier. Par exemple, vous pouvez générer un fichier RCF version 2.00 à l'aide de RCFfilegenerator v1.6c.

- Si vous câconnectez plusieurs configurations MetroCluster, suivez le tableau correspondant. Par exemple :
  - Si vous câblez deux configurations MetroCluster à quatre nœuds de type AFF A700, connectez le premier MetroCluster indiqué sous la forme « MetroCluster 1 » et le second MetroCluster sous la forme « MetroCluster 2 » dans le tableau AFF A700.

  Les ports 13 et 14 peuvent être utilisés en mode de vitesse native prenant en charge 40 Gbits/s et 100 Gbits/s, ou en mode d'arrachage pour prendre en charge 4 × 25 Gbits/s ou 4 × 10 Gbits/s. S'ils utilisent le mode de vitesse natif, ils sont représentés par les ports 13 et 14. S'ils utilisent le mode écorché, soit 4 × 25 Gbit/s, soit 4 × 10 Gbit/s, ils sont représentés sous la forme de ports 13s0-3 et 14s0-3.

Les sections suivantes décrivent le schéma de câblage physique. Vous pouvez également vous reporter à la "RcfFileGenerator" pour des informations détaillées sur le câblage.

Choisissez la table de câblage adaptée à votre configuration

Utilisez le tableau suivant pour déterminer la table de câblage que vous devez suivre.

Si votre système est…	Utilisez ce tableau de câblage…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 1)
AFF A20	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 2)

Si votre système est…	Utilisez ce tableau de câblage…
AFF C30, AFF A30 FAS50 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 3a) ou 100G (groupe 3b). • Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 3a -25G) • Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 3b -100G)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700 FAS9000, AFF A700	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 4)
AFF A50	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 5)
AFF C800, ASA C800 AFF A800, ASA A800 FAS9500 AFF A900, ASA A900	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 7)

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 1)

Passez en revue les attributions de port de la plate-forme pour câbler un AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, système AFF A250 ou ASA A250 vers un commutateur NVIDIA SN2100 :

Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 2)

Passez en revue les affectations de port de plate-forme pour relier un système AFF A20 à un commutateur NVIDIA SN2100 :

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e2a	e4a
s1s1-3		disabled	
2s0		e2a	e4a
2s1-3		disabled	
3s0	MetroCluster 2, Local Cluster interface	e2a	e4a
3s1-3		disabled	
4s0		e2a	e4a
4s1-3		disabled	
5s0	MetroCluster 3, Local Cluster interface	e2a	e4a
5s1-3		disabled	
6s0		e2a	e4a
6s1-3		disabled	
7	MetroCluster 1, MetroCluster interface	e2b	e4b
8			
9	MetroCluster 2, MetroCluster interface	e2b	e4b
10			
11	MetroCluster 3, MetroCluster interface	e2b	e4b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 3a)

Passez en revue les attributions de port de la plate-forme pour connecter un système AFF A30, AFF C30, AFF C60 ou FAS50 à un commutateur NVIDIA SN2100 à l'aide d'une carte Ethernet 25G à quatre ports :

Cette configuration nécessite une carte Ethernet 25G à quatre ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 3b)

Passez en revue les attributions de port de la plate-forme pour connecter un système AFF A30, AFF C30, AFF C60 ou FAS50 à un commutateur NVIDIA SN2100 à l'aide d'une carte Ethernet 100G à deux ports :

Cette configuration nécessite une carte Ethernet 100G à deux ports dans le logement 4 pour connecter le cluster local et les interfaces haute disponibilité.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 4)

Consultez les affectations des ports de la plateforme pour connecter un système FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, système FAS8700, FAS9000 ou AFF A700 vers un commutateur NVIDIA SN2100 :

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
6							
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
8							
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
10							
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

Remarque 1 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 5)

Passez en revue les affectations de port de plate-forme pour connecter un système AFF A50 à un commutateur NVIDIA SN2100 :

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6			
7	MetroCluster 1, MetroCluster interface	e2a	e2b
8			
9	MetroCluster 2, MetroCluster interface	e2a	e2b
10			
11	MetroCluster 3, MetroCluster interface	e2a	e2b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 6)

Passez en revue les affectations des ports de la plateforme pour câbler un AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, système AFF A900 ou ASA A900 vers un commutateur NVIDIA SN2100 :

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Remarque 1 : utilisez les ports e4a et e4e ou e4a et e8a si vous utilisez un adaptateur X91440A (40 Gbit/s). Utilisez les ports e4a et e4b ou e4a et e8a si vous utilisez un adaptateur X91153A (100 Gbit/s).

Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 7)

Vérifiez les affectations des ports de la plate-forme pour connecter un système FAS70, AFF A70, AFF C80, FAS90, AFF A90 ou AFF A1K à un commutateur NVIDIA SN2100 :

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
8									
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
12									
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3									
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16									

Câbler les ports du module de contrôleur ONTAP dans une configuration IP MetroCluster

Vous devez câbler les ports du module de contrôleur utilisés pour le peering de cluster, la gestion et la connectivité des données.

Cette tâche doit être effectuée sur chaque module de contrôleur de la configuration MetroCluster.

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.

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.

Le peering de cluster peut être effectué sur des ports dédiés ou sur des ports data. L'utilisation de ports dédiés fournit un débit plus élevé pour le trafic de peering de cluster.

"Configuration cluster et SVM peering express"

2. Reliez les ports de gestion et de données du contrôleur aux réseaux de gestion et de données du site local.

   Suivez les instructions d'installation de votre plate-forme sur le "Documentation des systèmes matériels ONTAP".

> Les systèmes IP MetroCluster ne disposent pas de ports dédiés à haute disponibilité (HA). Selon votre plateforme, le trafic haute disponibilité est desservi par le MetroCluster, le cluster local ou l'interface cluster/MetroCluster partagée. Lorsque vous utilisez *ONTAP Hardware Systems Documentation* pour installer votre plate-forme, vous ne devez pas suivre les instructions de câblage du cluster et des ports HA.

Configuration des commutateurs IP MetroCluster

Choisissez la procédure de configuration du commutateur IP MetroCluster appropriée

Vous devez configurer les switchs IP pour assurer la connectivité IP MetroCluster back-end. La procédure à suivre dépend de votre fournisseur de commutateur.

- "Configurez les commutateurs IP Broadcom"
- "Configuration des commutateurs IP Cisco"
- "Configurez les commutateurs IP NVIDIA"

Configurer les commutateurs IP Broadcom pour l'interconnexion de cluster et la connectivité IP MetroCluster backend

Vous devez configurer les commutateurs IP Broadcom pour qu'ils servent d'interconnexion de cluster et pour la connectivité IP MetroCluster de back-end.

> Votre configuration nécessite des licences supplémentaires (6 licences de port de 100 Go) dans les scénarios suivants :

- Vous utilisez les ports 53 et 54 en tant que MetroCluster ISL de 40 Gbits/s ou 100 Gbits/s.
- Vous utilisez une plate-forme qui connecte le cluster local et les interfaces MetroCluster aux ports 49 - 52.

Réinitialisation des paramètres d'usine du commutateur IP Broadcom

Avant d'installer une nouvelle version du logiciel de commutation et des RCFs, vous devez effacer les paramètres du commutateur Broadcom et effectuer une configuration de base.

Description de la tâche

- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur à l'aide de la console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Passez à l'invite de commande surélevée (#) : `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Effacez la configuration de démarrage et supprimez la bannière

   a. Effacez la configuration de démarrage :

   `erase startup-config`

```
(IP_switch_A_1) #erase startup-config

Are you sure you want to clear the configuration? (y/n) y

(IP_switch_A_1) #
```

   Cette commande n'efface pas la bannière.

   b. Supprimer la bannière :

   `no set clibanner`

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Redémarrez le commutateur :*`(IP_switch_A_1) #reload*`

```
Are you sure you would like to reset the system? (y/n) y
```

   Si le système vous demande si vous souhaitez enregistrer la configuration non enregistrée ou modifiée avant de recharger le commutateur, sélectionnez **non**.

4. Attendre que le commutateur se recharge, puis se connecter au commutateur.

   L'utilisateur par défaut est « admin » et aucun mot de passe n'est défini. Une invite similaire à la commande suivante s'affiche :

```
(Routing)>
```

5. Passer à l'invite de commande surélevée :

`enable`

```
Routing)> enable
(Routing) #
```

6. Définissez le protocole du port de service sur `none`:

   `serviceport protocol none`

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Attribuez l'adresse IP au port de service :

   `serviceport ip` *`ip-address netmask gateway`*

   L'exemple suivant montre l'adresse IP 10.10.10.10 attribuée à un port de service avec le sous-réseau 255.255.255.0 et la passerelle 10.10.10.1 :

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Vérifiez que le port de service est correctement configuré :

   `show serviceport`

   L'exemple suivant indique que le port est activé et que les adresses correctes ont été attribuées :

```
(Routing) #show serviceport

Interface Status.............................. Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. Configurez le serveur SSH.

- Le fichier RCF désactive le protocole Telnet. Si vous ne configurez pas le serveur SSH, vous pouvez uniquement accéder au pont à l'aide de la connexion du port série.
- Vous devez configurer le serveur SSH afin d'utiliser la collecte de journaux et d'autres outils externes.

a. Générer des clés RSA.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. Générer des clés DSA (facultatif)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Si vous utilisez la version conforme FIPS de EFOS, générez les clés ECDSA. L'exemple suivant crée les clés d'une longueur de 521. Les valeurs valides sont 256, 384 ou 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Activez le serveur SSH.

Si nécessaire, quittez le contexte de configuration.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

Si des clés existent déjà, il peut vous être demandé de les remplacer.

10. Si vous le souhaitez, configurez le domaine et le serveur de noms :

    `configure`

    L'exemple suivant montre le `ip domain` et `ip name server` commandes :

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Si vous le souhaitez, configurez le fuseau horaire et la synchronisation de l'heure (SNTP).

    L'exemple suivant montre le `sntp` Commandes, en spécifiant l'adresse IP du serveur SNTP et le fuseau horaire relatif.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

    Pour EFOS version 3.10.0.3 et ultérieure, utilisez le `ntp` comme indiqué dans l'exemple suivant :

```
> (Config)# ntp ?

authenticate              Enables NTP authentication.
authentication-key        Configure NTP authentication key.
broadcast                 Enables NTP broadcast mode.
broadcastdelay            Configure NTP broadcast delay in microseconds.
server                    Configure NTP server.
source-interface          Configure the NTP source-interface.
trusted-key               Configure NTP authentication key number for
trusted time source.
vrf                       Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Configurer le nom du commutateur :

    `hostname IP_switch_A_1`

    L'invite du commutateur affiche le nouveau nom :

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. Enregistrez la configuration :

    `write memory`

    Vous recevez des invites et des valeurs de sortie similaires à l'exemple suivant :

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Téléchargement et installation du logiciel du commutateur Broadcom EFOS

Vous devez télécharger le fichier du système d'exploitation du switch et le fichier RCF sur chaque commutateur de la configuration IP de MetroCluster.

Description de la tâche

Cette tâche doit être répétée sur chaque commutateur de la configuration IP de MetroCluster.

Notez ce qui suit :

- Lors de la mise à niveau de EFOS 3.4.x.x vers EFOS 3.7.x.x ou version ultérieure, le commutateur doit exécuter EFOS 3.4.4.6 (ou version 3.4.x.x ultérieure). Si vous exécutez une version antérieure à celle-ci, mettez d'abord le commutateur à niveau vers EFOS 3.4.4.6 (ou version ultérieure 3.4.x.x), puis mettez-le à niveau vers EFOS 3.7.x.x ou version ultérieure.
- La configuration de EFOS 3.4.x.x et 3.7.x.x ou ultérieure est différente. Pour changer la version EFOS de 3.4.x.x à 3.7.x.x ou ultérieure, ou vice versa, le commutateur doit être réinitialisé aux valeurs par défaut et les fichiers RCF pour la version EFOS correspondante doivent être (ré)appliqués. Cette procédure nécessite un accès via le port série console.
- À partir de la version 3.7.x.x ou ultérieure de EFOS, une version non conforme à la norme FIPS et une version conforme à la norme FIPS sont disponibles. Différentes étapes sont appliquées lorsque vous passez d'une version non conforme à FIPS à une version conforme FIPS ou inversement. Le fait de remplacer EFOS d'une version non conforme à la norme FIPS par une version conforme à la norme FIPS ou vice versa réinitialise les paramètres par défaut du commutateur. Cette procédure nécessite un accès via le port série console.

Étapes

1. Téléchargez le micrologiciel du commutateur à partir du "Site de support Broadcom".
2. Vérifiez si votre version de EFOS est conforme à la norme FIPS ou non conforme à la norme FIPS à l'aide du `show fips status` commande. Dans les exemples suivants, `IP_switch_A_1` Utilise EFOS et conforme à la norme FIPS `IP_switch_A_2` Utilise EFOS non conforme à la norme FIPS.

Exemple 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Exemple 2

```
IP_switch_A_2 #show fips status
                      ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

3. Utilisez le tableau suivant pour déterminer la méthode à suivre :

Procédure	Version actuelle de EFOS	Nouvelle version EFOS	Pas de niveau élevé
Procédure de mise à niveau de EFOS entre deux versions (non conformes à la norme FIPS	3.4.x.x	3.4.x.x	Installer la nouvelle image EFOS à l'aide de la méthode 1) les informations de configuration et de licence sont conservées
3.4.4.6 (ou version ultérieure 3.4.x.x)	3.7.x.x ou version ultérieure non conforme FIPS	Mettre à niveau EFOS à l'aide de la méthode 1. Réinitialisez le commutateur sur les paramètres par défaut et appliquez le fichier RCF pour EFOS 3.7.x.x ou version ultérieure	3.7.x.x ou version ultérieure non conforme FIPS
3.4.4.6 (ou version ultérieure 3.4.x.x)	Rétrograder EFOS à l'aide de la méthode 1. Réinitialisez le commutateur sur les paramètres par défaut et appliquez le fichier RCF pour EFOS 3.4.x.x	3.7.x.x ou version ultérieure non conforme FIPS	

Installez la nouvelle image EFOS à l'aide de la méthode 1. Les informations de configuration et de licence sont conservées	Conforme à la norme FIPS 3.7.x.x ou ultérieure	Conforme à la norme FIPS 3.7.x.x ou ultérieure	Installez la nouvelle image EFOS à l'aide de la méthode 1. Les informations de configuration et de licence sont conservées
Procédure de mise à niveau vers/à partir d'une version conforme à la norme FIPS EFOS	Non conforme à la norme FIPS	Conforme à la norme FIPS	Installation de l'image EFOS à l'aide de la méthode 2. La configuration du commutateur et les informations de licence seront perdues.

- Méthode 1 : Procédure de mise à niveau de EFOS en téléchargeant l'image logicielle dans la partition de démarrage de sauvegarde
- Méthode 2 : Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS

Procédure de mise à niveau de EFOS en téléchargeant l'image logicielle dans la partition de démarrage de sauvegarde

Vous ne pouvez effectuer les étapes suivantes que si les deux versions EFOS ne sont pas conformes à la norme FIPS ou si les deux versions EFOS sont conformes à la norme FIPS.

N'utilisez pas ces étapes si une version est conforme à la norme FIPS et que l'autre est non conforme à la norme FIPS.

Étapes

1. Copier le logiciel du commutateur sur le commutateur : `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   Dans cet exemple, le fichier système d'exploitation efos-3.4.4.6.stk est copié du serveur SFTP à 50.50.50.50 vers la partition de sauvegarde. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename.......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Configurez le commutateur pour qu'il démarre à partir de la partition de sauvegarde lors du prochain redémarrage du commutateur :

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Vérifiez que la nouvelle image de démarrage sera active au prochain démarrage :

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Enregistrez la configuration :

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Redémarrez le commutateur :

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Attendez que le commutateur redémarre.

Dans de rares cas, le commutateur peut ne pas démarrer. Suivez le Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS pour installer la nouvelle image.

7. Si vous passez de EFOS 3.4.x.x à EFOS 3.7.x.x ou vice versa, suivez les deux procédures suivantes pour appliquer la configuration correcte (RCF) :
   a. Réinitialisation des paramètres d'usine du commutateur IP Broadcom
   b. Téléchargement et installation des fichiers RCF Broadcom
8. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS

Vous pouvez effectuer les étapes suivantes si une version de EFOS est conforme à la norme FIPS et que l'autre version de EFOS n'est pas compatible FIPS. Ces étapes peuvent être utilisées pour installer l'image EFOS 3.7.x.x non conforme à la norme FIPS ou à la norme FIPS à partir d'ONIE si le commutateur ne parvient pas à démarrer.

Étapes

1. Démarrez le commutateur en mode d'installation ONIE.

   Au cours du démarrage, sélectionnez ONIE lorsque l'écran suivant s'affiche :

```
+----------------------------------------------------------------------+
|EFOS                                                                  |
|*ONIE                                                                 |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
+----------------------------------------------------------------------+
```

   Après avoir sélectionné « ONIE », le commutateur se charge et vous présente les choix suivants :

```
+--------------------------------------------------------------------+
|*ONIE: Install OS                                                   |
| ONIE: Rescue                                                       |
| ONIE: Uninstall OS                                                 |
| ONIE: Update ONIE                                                  |
| ONIE: Embed ONIE                                                   |
| DIAG: Diagnostic Mode                                              |
| DIAG: Burn-In Mode                                                 |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
+--------------------------------------------------------------------+
```

Le commutateur démarre maintenant en mode d'installation ONIE.

2. Arrêtez la détection ONIE et configurez l'interface ethernet

   Lorsque le message suivant s'affiche, appuyez sur <ENTER> pour appeler la console ONIE :

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   La détection ONIE se poursuit et les messages sont imprimés sur la console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configurez l'interface ethernet et ajoutez la route à l'aide de `ifconfig eth0 <ipAddress> netmask <netmask> up` et `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Vérifiez que le serveur hébergeant le fichier d'installation ONIE est accessible :

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Installez le nouveau logiciel du commutateur

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Le logiciel va installer puis redémarrer le commutateur. Laissez le commutateur redémarrer normalement dans la nouvelle version de EFOS.

6. Vérifier que le nouveau logiciel de commutateur est installé

show bootvar

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Terminez l'installation

   Le commutateur redémarre sans configuration appliquée et rétablit les paramètres par défaut. Suivez les deux procédures pour configurer les paramètres de base du commutateur et appliquer le fichier RCF comme indiqué dans les deux documents suivants :

   a. Configurer les paramètres de base du commutateur. Suivez l'étape 4 et les versions ultérieures : Réinitialisation des paramètres d'usine du commutateur IP Broadcom
   b. Créez et appliquez le fichier RCF comme indiqué dans Téléchargement et installation des fichiers RCF Broadcom

Téléchargement et installation des fichiers RCF Broadcom

Vous devez générer et installer le fichier RCF des switchs sur chaque switch de configuration MetroCluster IP.

Avant de commencer

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Description de la tâche

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Il existe quatre fichiers RCF, un par pour chacun des quatre commutateurs de la configuration MetroCluster IP. Vous devez utiliser les fichiers RCF appropriés pour le modèle de commutateur que vous utilisez.

Commutateur	Fichier RCF
IP_switch_A_1	v1.32_Switch-A1.txt
IP_Switch_A_2	v1.32_Switch-A2.txt
IP_Switch_B_1	v1.32_Switch-B1.txt
IP_Switch_B_2	v1.32_Switch-B2.txt

Fichiers RCF pour EFOS version 3.4.4.6 ou ultérieure 3.4.x.x. La version et la version 3.7.0.4 de EFOS sont différentes. Vous devez vous assurer que vous avez créé les fichiers RCF appropriés pour la version EFOS que le commutateur est en cours d'exécution.

Version EFOS	Version du fichier RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Étapes

1. Générez les fichiers RCF Broadcom pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP"
   b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

Les modifications apportées aux fichiers RCF après le téléchargement ne sont pas prises en charge.

2. Copier les fichiers RCF sur les commutateurs :

   a. Copier les fichiers RCF sur le premier commutateur : `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      Dans cet exemple, le fichier RCF "BES-53248_v1.32_Switch-A1.txt" est copié du serveur SFTP à "50.50.50.50" vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /RcfFiles/
Filename..................................... BES-
53248_v1.32_Switch-A1.txt
Data Type.................................... Config Script
Destination Filename......................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"*****************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Vérifiez que le fichier RCF est enregistré comme script :

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Appliquer le script RCF :

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"*****************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Enregistrez la configuration :

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Redémarrez le commutateur :

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

a. Répétez les étapes précédentes pour chacun des trois autres commutateurs en veillant à copier le fichier RCF correspondant sur le commutateur correspondant.

3. Recharger l'interrupteur :

```
reload
```

```
IP_switch_A_1# reload
```

4. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :

> Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

Pour plus de détails sur le port ISL

Lancer la commande `show port all`.

Pour plus d'informations sur les canaux de port

Lancer la commande `show port-channel all`.

2. Désactivez les ports ISL et les canaux de port inutilisés.

   Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Configuration des commutateurs IP Cisco

Configurer les commutateurs IP Cisco pour l'interconnexion des clusters et la connectivité IP MetroCluster backend

Vous devez configurer les switchs IP Cisco pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Description de la tâche

Plusieurs procédures de cette section sont des procédures indépendantes et vous n'avez qu'à exécuter celles que vous êtes dirigé vers ou qui sont pertinentes pour votre tâche.

Réinitialisation des paramètres d'usine du commutateur IP Cisco

Avant d'installer un fichier RCF, vous devez effacer la configuration du commutateur Cisco et effectuer une configuration de base. Cette procédure est obligatoire lorsque vous souhaitez réinstaller le même fichier RCF après l'échec d'une installation précédente ou si vous souhaitez installer une nouvelle version d'un fichier RCF.

Description de la tâche

- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur à l'aide de la console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Rétablir les paramètres d'usine du commutateur :

   a. Effacez la configuration existante :

      `write erase`

b. Recharger le logiciel du contacteur :

```
reload
```

Le système redémarre et entre dans l'assistant de configuration. Au cours du démarrage, si vous recevez l'invite « abandonner la mise en service automatique et poursuivre la configuration normale ? (oui/non)", you should respond `yes pour continuer.

c. Dans l'assistant de configuration, entrez les paramètres de base du commutateur :

- Mot de passe d'administrateur
- Nom du commutateur
- Configuration de gestion hors bande
- Passerelle par défaut
- Service SSH (RSA)

Une fois l'assistant de configuration terminé, le commutateur redémarre.

d. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe pour vous connecter au commutateur.

L'exemple suivant montre les invites et les réponses système lors de la configuration du commutateur. Les supports d'angle (<<<) indique où vous saisissez les informations.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Vous entrez des informations de base dans les invites suivantes, notamment le nom du commutateur, l'adresse de gestion et la passerelle, et sélectionnez SSH avec RSA.

Cet exemple montre les informations minimales requises pour configurer la FCR. Des options supplémentaires peuvent être configurées une fois la FCR appliquée. Par exemple, vous pouvez configurer SNMPv3, NTP ou SCP/SFTP après avoir appliqué le RCF.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Le jeu d’invites final termine la configuration :

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Enregistrez la configuration :

```
IP_switch-A-1# copy running-config startup-config
```

3. Redémarrez le commutateur et attendez que le commutateur se recharge :

```
IP_switch-A-1# reload
```

4. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Téléchargement et installation du logiciel du commutateur Cisco NX-OS

Vous devez télécharger le fichier du système d'exploitation du switch et le fichier RCF sur chaque commutateur de la configuration IP de MetroCluster.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Étapes

1. Téléchargez le fichier logiciel NX-OS pris en charge.

   "Téléchargement de logiciels Cisco"

2. Copier le logiciel du commutateur sur le commutateur :

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   Dans cet exemple, le fichier nxos.7.0.3.I4.6.bin et l'image EPLD sont copiés du serveur SFTP 10.10.99.99 vers le bootflash local :

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. Vérifiez sur chaque commutateur que les fichiers de commutateur NX-OS sont présents dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installez le logiciel du commutateur :

   `install all nxos bootflash:nxos.version-number.bin`

   Le commutateur se recharge automatiquement (redémarre) après l'installation du logiciel du commutateur.

   L'exemple suivant montre l'installation du logiciel sur IP_switch_A_1 :

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos               7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Attendre que le commutateur se recharge, puis se connecter au commutateur.

   Une fois le commutateur redémarré, l'invite de connexion s'affiche :

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vérifier que le logiciel du commutateur a été installé :
   `show version`

   L'exemple suivant montre la sortie :

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Mettre à niveau l’image EPLD et redémarrer le commutateur.

```
IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  ------------------ ------------ ----------- -----------------
     1         SUP         Yes           disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module   Type  Upgrade-Result
-------- ----- --------------
     1   SUP   Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. après le redémarrage du commutateur, reconnectez-vous et vérifiez que la nouvelle version de EPLD a été chargée avec succès.

   ```
   show version module 1 epld
   ```

9. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Téléchargement et installation des fichiers Cisco IP RCF

Vous devez générer et installer le fichier RCF sur chaque switch de configuration MetroCluster IP.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Il existe quatre fichiers RCF, un par pour chacun des quatre commutateurs de la configuration MetroCluster IP. Vous devez utiliser les fichiers RCF appropriés pour le modèle de commutateur que vous utilisez.

Commutateur	Fichier RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Étapes

1. Générez les fichiers RCF Cisco pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP"
   b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

   Les modifications apportées aux fichiers RCF après le téléchargement ne sont pas prises en charge.

2. Copier les fichiers RCF sur les commutateurs :
   a. Copier les fichiers RCF sur le premier commutateur :

   ```
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
   bootflash: vrf management
   ```

   Dans cet exemple, le fichier RCF NX3232_v1.80_Switch-A1.txt est copié du serveur SFTP à 10.10.99.99 vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Répétez la sous-étape précédente pour chacun des trois autres commutateurs en étant sûr de copier le fichier RCF correspondant sur le commutateur correspondant.

3. Vérifiez sur chaque commutateur que le fichier RCF est présent dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Configurez les régions TCAM sur les switchs Cisco 3132Q-V et Cisco 3232C.

   Ignorez cette étape si vous ne disposez pas de switchs Cisco 3132Q-V ou Cisco 3232C.

   a. Sur le commutateur Cisco 3132Q-V, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. Sur le switch Cisco 3232C, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Après avoir défini les régions du TCAM, enregistrez la configuration et rechargez le commutateur :

```
copy running-config startup-config
reload
```

5. Copiez le fichier RCF correspondant de la mémoire bootflash locale vers la configuration en cours d'exécution sur chaque commutateur :

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Copiez les fichiers RCF de la configuration en cours d'exécution vers la configuration de démarrage de chaque commutateur :

   `copy running-config startup-config`

   Vous devez voir les résultats similaires à ce qui suit :

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Recharger l'interrupteur :

   `reload`

```
IP_switch_A_1# reload
```

8. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Définition de la correction d'erreurs de renvoi pour les systèmes utilisant une connectivité à 25 Gbit/s.

Si votre système est configuré avec une connectivité 25 Gbit/s, vous devez définir manuellement le paramètre fec (Forward Error correction) sur Off après avoir appliqué le fichier RCF. Le fichier RCF n'applique pas ce paramètre.

Description de la tâche

Les ports 25 Gbit/s doivent être câblés avant d'effectuer cette procédure.

"Affectation des ports de plateforme pour les switchs Cisco 3232C ou Cisco 9336C"

Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s :

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.

Étapes

1. Définissez le paramètre fec sur Off sur chaque port 25 Gbit/s connecté à un module de contrôleur, puis copiez la configuration en cours d'exécution sur la configuration de démarrage :

   a. Passer en mode configuration : `config t`

   b. Spécifiez l'interface 25 Gbit/s à configurer : `interface interface-ID`

   c. Réglez fec sur Arrêt : `fec off`

   d. Répétez les étapes précédentes pour chaque port 25 Gbit/s du commutateur.

   e. Quitter le mode de configuration : `exit`

   L'exemple suivant montre les commandes de l'interface Ethernet1/25/1 sur le commutateur IP_switch_A_1 :

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Répétez l'étape précédente sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifier les ports ISL et les canaux de port inutilisés :

```
show interface brief
```

2. Désactivez les ports ISL et les canaux de port inutilisés.

   Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configurer le cryptage MACsec sur les commutateurs Cisco 9336C dans un site IP MetroCluster

Le cryptage MACsec ne peut être appliqué qu'aux ports WAN ISL.

Configurez le cryptage MACsec sur les commutateurs Cisco 9336C

Vous devez uniquement configurer le cryptage MACsec sur les ports WAN ISL qui s'exécutent entre les sites. Vous devez configurer MACsec après avoir appliqué le fichier RCF correct.

Conditions de licence pour MACsec

MACsec nécessite une licence de sécurité. Pour une explication complète du schéma de licence Cisco NX-OS et de la manière d'obtenir et de demander des licences, consultez le "Guide des licences Cisco NX-OS"

Activez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous pouvez activer le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL WAN dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Activer MACsec et MKA sur le périphérique :

```
feature macsec
```

```
IP_switch_A_1(config)# feature macsec
```

3. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configurer une chaîne de clé MACsec et des clés

Vous pouvez créer une chaîne de clés MACsec ou des clés sur votre configuration.

Key Lifetime et hitless Key Rollover

Un trousseau MACsec peut avoir plusieurs clés pré-partagées (PSK), chacune configurée avec un ID de clé et une durée de vie facultative. La durée de vie d'une clé indique à quel moment la clé s'active et expire. En l'absence d'une configuration à vie, la durée de vie par défaut est illimitée. Lorsqu'une durée de vie est configurée, MKA passe à la prochaine clé pré-partagée configurée dans le trousseau une fois la durée de vie écoulée. Le fuseau horaire de la clé peut être local ou UTC. Le fuseau horaire par défaut est UTC. Une clé peut se déployer sur une seconde clé dans le même trousseau si vous configurez la seconde clé (dans le trousseau) et configurez une durée de vie pour la première clé. Lorsque la durée de vie de la première clé expire, elle passe automatiquement à la clé suivante de la liste. Si la même clé est configurée sur les deux côtés de la liaison en même temps, le basculement de la clé est sans arrêt (c'est-à-dire, la clé se replace sans interruption de la circulation).

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Pour masquer la chaîne d'octet de clé cryptée, remplacez la chaîne par un caractère générique dans la sortie du `show running-config` et `show startup-config` commandes :

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

> La chaîne octet est également masquée lorsque vous enregistrez la configuration dans un fichier.

   Par défaut, les clés PSK sont affichées au format crypté et peuvent être déchiffrées facilement. Cette commande ne s'applique qu'aux chaînes de clés MACsec.

3. Créer une chaîne de clés MACsec pour contenir un jeu de clés MACsec et entrer le mode de configuration de la chaîne de clés MACsec :

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

4. Créer une clé MACsec et entrer le mode de configuration de la clé MACsec :

```
key key-id
```

La plage est comprise entre 1 et 32 caractères hexadécimaux, et la taille maximale est de 64 caractères.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configurez la chaîne d'octet pour la clé :

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```

L'argument octet-chaîne peut contenir jusqu'à 64 caractères hexadécimaux. La clé octet est codée en interne, de sorte que la clé en texte clair n'apparaît pas dans la sortie du `show running-config macsec` commande.

6. Configurer une durée de vie d'envoi pour la clé (en secondes) :

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

Par défaut, l'appareil traite l'heure de début comme UTC. L'argument heure de début correspond à l'heure et à la date auxquelles la clé devient active. L'argument de durée est la durée de vie en secondes. La longueur maximale est de 2147483646 secondes (environ 68 ans).

7. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Affiche la configuration du trousseau :

   `show key chain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configurez une stratégie MACsec

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Créer une stratégie MACsec :

   `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Configurez l'un des chiffrements suivants : GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256 :

   `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configurez la priorité du serveur de clés pour rompre le lien entre les pairs lors d'un échange de clés :

   `key-server-priority number`

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configurez la stratégie de sécurité pour définir le traitement des données et des paquets de contrôle :

   `security-policy security policy`

   Choisissez une stratégie de sécurité parmi les options suivantes :

   - Doit-Secure — les paquets qui ne portent pas les en-têtes MACsec sont supprimés

- Devrait-Secure — les paquets qui ne portent pas d'en-têtes MACsec sont autorisés (il s'agit de la valeur par défaut)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configurez la fenêtre de protection de relecture de sorte que l'interface sécurisée n'accepte pas un paquet dont la taille de fenêtre configurée est inférieure à celle de la fenêtre : `window-size number`

> La taille de la fenêtre de protection de relecture représente le nombre maximum de trames hors séquence que MACsec accepte et ne sont pas supprimées. La plage va de 0 à 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configurer le temps en secondes pour forcer une nouvelle touche SAK :

   `sak-expiry-time time`

   Vous pouvez utiliser cette commande pour remplacer la clé de session par un intervalle de temps prévisible. La valeur par défaut est 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configurez l'un des décalages de confidentialité suivants dans la trame de couche 2 où le chiffrement commence :

   `conf-offsetconfidentiality offset`

   Choisissez parmi les options suivantes :

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

> Cette commande peut être nécessaire pour que les commutateurs intermédiaires utilisent des en-têtes de paquets (dmac, smac, etype) comme des balises MPLS.

9. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Afficher la configuration de la stratégie MACsec :

    `show macsec policy`

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Activez le cryptage Cisco MACsec sur les interfaces

1. Passer en mode de configuration globale :

    `configure terminal`

    ```
    IP_switch_A_1# configure terminal
    IP_switch_A_1(config)#
    ```

2. Sélectionnez l'interface que vous avez configurée avec le cryptage MACsec.

    Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

    ```
    IP_switch_A_1(config)# interface ethernet 1/15
    switch(config-if)#
    ```

3. Ajoutez le trousseau et la stratégie à configurer sur l'interface pour ajouter la configuration MACsec :

    `macsec keychain keychain-name policy policy-name`

    ```
    IP_switch_A_1(config-if)# macsec keychain 1 policy abc
    ```

4. Répétez les étapes 1 et 2 sur toutes les interfaces où le cryptage MACsec doit être configuré.
5. Copier la configuration en cours d'exécution dans la configuration de démarrage :

    `copy running-config startup-config`

    ```
    IP_switch_A_1(config)# copy running-config startup-config
    ```

Désactivez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous devrez peut-être désactiver le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL du réseau étendu dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

`configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Désactivez la configuration MACsec sur le périphérique :

   `macsec shutdown`

   ```
   IP_switch_A_1(config)# macsec shutdown
   ```

   ⓘ La sélection de l'option « non » restaure la fonction MACsec.

3. Sélectionnez l'interface que vous avez déjà configurée avec MACsec.

   Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Supprimez le trousseau et la stratégie configurés sur l'interface pour supprimer la configuration MACsec :

   `no macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
   ```

5. Répétez les étapes 3 et 4 sur toutes les interfaces où MACsec est configuré.
6. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Vérification de la configuration MACsec

Étapes

1. Répétez **tous** des procédures précédentes sur le deuxième commutateur de la configuration pour établir une session MACsec.
2. Exécutez les commandes suivantes pour vérifier que les deux commutateurs sont chiffrés :

   a. Exécuter : `show macsec mka summary`

b. Exécuter : `show macsec mka session`

c. Exécuter : `show macsec mka statistics`

Vous pouvez vérifier la configuration MACsec à l'aide des commandes suivantes :

Commande	Affiche des informations sur…
`show macsec mka session interface typeslot/port number`	La session MKA de MACsec pour une interface spécifique ou pour toutes les interfaces
`show key chain name`	La configuration de la chaîne de clés
`show macsec mka summary`	La configuration MACsec MKA
`show macsec policy policy-name`	Configuration d'une stratégie MACsec spécifique ou de toutes les politiques MACsec

Configurez les commutateurs IP NVIDIA

Configurer le commutateur NVIDIA IP SN2100 pour l'interconnexion de cluster et la connectivité IP MetroCluster backend

Vous devez configurer les switchs IP NVIDIA SN2100 pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Réinitialiser les valeurs par défaut du commutateur NVIDIA IP SN2100

Vous pouvez choisir parmi les méthodes suivantes pour réinitialiser un commutateur sur les paramètres par défaut.

- Réinitialisez le commutateur à l'aide de l'option de fichier RCF
- Téléchargez et installez le logiciel Cumulus

Réinitialiser le commutateur à l'aide de l'option de fichier RCF

Avant d'installer une nouvelle configuration RCF, vous devez rétablir les paramètres du commutateur NVIDIA.

Description de la tâche

Pour restaurer les paramètres par défaut du commutateur, exécutez le fichier RCF avec le `restoreDefaults` option. Cette option copie les fichiers d'origine sauvegardés à leur emplacement d'origine, puis redémarre le commutateur. Après le redémarrage, le switch est en ligne avec la configuration d'origine qui existait au moment d'avoir exécuté le fichier RCF pour configurer le switch.

Les détails de configuration suivants ne sont pas réinitialisés :

- Configuration utilisateur et informations d'identification
- Configuration du port réseau de gestion, eth0

Toutes les autres modifications de configuration qui se produisent pendant l'application du fichier RCF sont rétablies à la configuration d'origine.

Avant de commencer

- Vous devez configurer le commutateur conformément à Téléchargez et installez le fichier RCF NVIDIA. Si vous n'avez pas configuré cette méthode ou si des fonctionnalités supplémentaires ont été configurées avant d'exécuter le fichier RCF, vous ne pouvez pas suivre cette procédure.
- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur par une connexion de console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Vérifiez que la configuration RCF a été appliquée avec succès avec la même version ou une version de fichier RCF compatible et que les fichiers de sauvegarde sont bien en place.

Le résultat de cette commande peut afficher les fichiers de sauvegarde, les fichiers conservés, ou les deux. Si les fichiers de sauvegarde ou les fichiers conservés n'apparaissent pas dans le résultat, vous ne pouvez pas utiliser cette procédure.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Exécutez le fichier RCF avec la possibilité de restaurer les valeurs par défaut : `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Répondez « oui » à l'invite. Le commutateur revient à la configuration d'origine et redémarre.
4. Attendez que le commutateur redémarre.

   Le commutateur est réinitialisé et conserve la configuration initiale, telle que la configuration du réseau de gestion et les identifiants actuels qu'ils existaient avant d'appliquer le fichier RCF. Après le redémarrage, vous pouvez appliquer une nouvelle configuration en utilisant la même version ou une version différente du fichier RCF.

Téléchargez et installez le logiciel Cumulus

Description de la tâche

Suivez ces étapes pour réinitialiser complètement le commutateur en appliquant l'image Cumulus.

Avant de commencer

- Vous devez être connecté au commutateur par une connexion de console série.
- L'image logicielle du commutateur Cumulus est accessible via HTTP.

> Pour plus d'informations sur l'installation de Cumulus Linux, voir "Présentation de l'installation et de la configuration des switchs NVIDIA SN2100"

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.

Étapes

1. À partir de la console Cumulus, téléchargez et mettez en file d'attente l'installation du logiciel du commutateur avec la commande `onie-install -a -i` suivi du chemin du fichier vers le logiciel du commutateur :

   Dans cet exemple, le fichier du micrologiciel `cumulus-linux-4.4.3-mlx-amd64.bin` Est copié du serveur HTTP '50.50.50.50' sur le commutateur local.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
##################################################################
# 100.0%
```

```
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
```

```
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Répondez `y` à l'invite pour confirmer l'installation lors du téléchargement et de la vérification de l'image.
3. Redémarrez le commutateur pour installer le nouveau logiciel : `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> Le commutateur redémarre et entre dans l'installation du logiciel du commutateur, ce qui prend un certain temps. Une fois l'installation terminée, le commutateur redémarre et reste à l'invite de connexion.

4. Configurer les paramètres de base du commutateur
   a. Lorsque le commutateur est démarré et que vous êtes invité à ouvrir une session, connectez-vous et modifiez le mot de passe.

      > Le nom d'utilisateur est 'cumulus' et le mot de passe par défaut est 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configuration de l'interface réseau de gestion

   Les commandes que vous utilisez dépendent de la version du micrologiciel du commutateur que vous exécutez.

   L'exemple de commandes suivant configure le nom d'hôte en tant que IP_Switch_A_1, l'adresse IP en tant que 10.10.10.10, le masque de réseau en tant que 255.255.255.0 (24) et l'adresse de la passerelle en tant que 10.10.10.1.

Cumulus 4.4.x

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant Cumulus 4.4.x.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

Cumulus 5.4.x et versions ultérieures

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant Cumulus 5.4.x. ou ultérieure.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. Redémarrez le commutateur à l'aide du `sudo reboot` commande.

```
cumulus@cumulus:~$ sudo reboot
```

Lorsque le commutateur redémarre, vous pouvez appliquer une nouvelle configuration en suivant les étapes de la section Téléchargez et installez le fichier RCF NVIDIA.

Télécharger et installer les fichiers RCF NVIDIA

Vous devez générer et installer le fichier RCF des switchs sur chaque switch de configuration MetroCluster IP.

Avant de commencer

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.
- Le logiciel du commutateur est installé et le réseau de gestion est configuré.
- Vous avez suivi les étapes d'installation initiale du commutateur à l'aide de la méthode 1 ou de la méthode 2.
- Vous n'avez appliqué aucune configuration supplémentaire après l'installation initiale.

> Si vous effectuez une autre configuration après la réinitialisation du commutateur et avant d'appliquer le fichier RCF, cette procédure ne peut pas être utilisée.

Description de la tâche

Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration IP MetroCluster (nouvelle installation) ou sur le commutateur de remplacement (remplacement du commutateur).

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Étapes

1. Générer les fichiers RCF NVIDIA pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP".

b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

c. Accédez à votre répertoire personnel. Si vous êtes enregistré en tant que 'culus', le chemin du fichier est `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

d. Téléchargez le fichier RCF dans ce répertoire. L'exemple suivant montre que vous utilisez SCP pour télécharger le fichier `SN2100_v2.0.0_IP_switch_A_1.txt` du serveur '50.50.50.50' à votre répertoire personnel et enregistrez-le sous `SN2100_v2.0.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
**********************************************************************
**
Banner of the SCP server
**********************************************************************
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Exécutez le fichier RCF. Le fichier RCF requiert une option permettant d'appliquer une ou plusieurs étapes. Sauf instruction contraire du support technique, exécutez le fichier RCF sans l'option de ligne de commande. Pour vérifier l'état d'achèvement des différentes étapes du fichier RCF, utilisez l'option '-1' ou 'All' pour appliquer toutes les étapes (en attente).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

3. Si votre configuration utilise des câbles DAC, activez l'option DAC sur les ports de commutateur :

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

L'exemple suivant active l'option DAC pour le port `swp7`:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.00
    Running command: Enabling the DacOption for port swp7
    runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. Redémarrez le commutateur après avoir activé l'option DAC sur les ports de commutateur :

```
sudo reboot
```

> Lorsque vous définissez l'option DAC pour plusieurs ports de commutateur, vous ne devez redémarrer le commutateur qu'une seule fois.

Définissez la correction d'erreur de transfert pour les systèmes utilisant une connectivité de 25 Gbit/s.

Si votre système est configuré avec une connectivité de 25 Gbit/s, définissez manuellement le paramètre correction d'erreur de transfert (fec) sur Désactivé après l'application de la FCR. La FCR n'applique pas ce paramètre.

Description de la tâche

- Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s. Reportez-vous à la "Affectations des ports de plateforme pour les switchs IP SN2100 pris en charge par NVIDIA".
- Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Définissez le `fec` paramètre sur Off pour le premier port de commutateur qui utilise une connectivité 25 Gbit/s :

   ```
   sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
   ```

2. Répétez l'étape pour chaque port de commutateur 25 Gbit/s connecté à un module de contrôleur.

Définissez la vitesse du port de commutateur pour les interfaces IP MetroCluster

Description de la tâche

- Utilisez cette procédure pour régler la vitesse du port de commutation sur 100 G pour les systèmes suivants :
  - AFF A70, AFF A90, AFF A1K, AFF C80
  - AFF A30, AFF C30, AFF A50, AFF C60
  - FAS50, FAS70, FAS90
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étape

1. Utilisez le fichier RCF avec `runCmd` l'option pour définir la vitesse. Ceci applique le paramètre et enregistre la configuration.

   Les commandes suivantes définissent la vitesse des interfaces MetroCluster `swp7` et `swp8`:

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
   ```

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
   ```

   Exemple

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.20
    Running command: Setting switchport swp7 to 100G speed
    runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
    runCmd: 'nv set interface swp7 link speed 100G', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles. Vous devez désactiver chaque port ou canal de port individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :

   Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

   ```
   net show interface
   ```

2. Désactivez les ports ISL et les canaux de port inutilisés à l'aide du fichier RCF.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

L'exemple de commande suivant désactive le port « swp14 » :

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Répétez cette étape pour chaque port ou canal de port non utilisé identifié.

Installer le fichier de configuration Ethernet Switch Health Monitor pour un commutateur IP NVIDIA SN2100 MetroCluster

Pour configurer la surveillance de l'état du commutateur Ethernet sur les commutateurs Ethernet NVIDIA, suivez cette procédure.

Ces instructions s'appliquent si les commutateurs NVIDIA X190006-PE et X190006-PI ne sont pas détectés correctement, ce qui peut être confirmé en exécutant `system switch ethernet show` et vérifiez si

AUTRE est affiché pour votre modèle. Pour identifier votre modèle de commutateur NVIDIA, recherchez sa référence à l'aide de la commande `nv show platform hardware` pour NVIDIA CL 5.8 et versions antérieures ou `nv show platform` pour les versions ultérieures.

> Ces étapes sont également recommandées si vous souhaitez que la surveillance de l'intégrité et la collecte des journaux fonctionnent correctement lors de l'utilisation de NVIDIA CL 5.11.x avec les versions ONTAP suivantes. Bien que la surveillance de l'intégrité et la collecte des journaux puissent fonctionner sans ces étapes, leur respect garantit le bon fonctionnement de l'ensemble.
>
> - 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 et versions ultérieures des correctifs

Avant de commencer

- Assurez-vous que le cluster ONTAP est opérationnel.
- Activez SSH sur le commutateur pour utiliser toutes les fonctionnalités disponibles dans CSHM.
- Effacez le `/mroot/etc/cshm_nod/nod_sign/` répertoire sur tous les nœuds :

  a. Entrez le nodeshell :

  ```
  system node run -node <name>
  ```

  b. Passer au privilège avancé :

  ```
  priv set advanced
  ```

  c. Répertoriez les fichiers de configuration dans le `/etc/cshm_nod/nod_sign` répertoire. Si le répertoire existe et contient des fichiers de configuration, il répertorie les noms des fichiers.

  ```
  ls /etc/cshm_nod/nod_sign
  ```

  d. Supprimez tous les fichiers de configuration correspondant à vos modèles de commutateurs connectés.

  Si vous n'êtes pas sûr, supprimez tous les fichiers de configuration pour les modèles pris en charge répertoriés ci-dessus, puis téléchargez et installez les derniers fichiers de configuration pour ces mêmes modèles.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

  a. Vérifiez que les fichiers de configuration supprimés ne se trouvent plus dans le répertoire :

  ```
  ls /etc/cshm_nod/nod_sign
  ```

Étapes

1. Téléchargez le fichier zip de configuration du moniteur d'état du commutateur Ethernet basé sur la version ONTAP correspondante. Ce fichier est disponible à partir de la "Switchs Ethernet NVIDIA" page.
   a. Sur la page de téléchargement du logiciel NVIDIA SN2100, sélectionnez **Nvidia CSHM File**.
   b. Sur la page attention/doit lire, cochez la case pour accepter.
   c. Sur la page Contrat de licence utilisateur final, cochez la case accepter et cliquez sur **accepter et continuer**.

d. Sur la page Nvidia CSHM File - Download, sélectionnez le fichier de configuration applicable. Les fichiers suivants sont disponibles :

ONTAP 9.15.1 et versions ultérieures

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 à 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. chargez le fichier zip applicable sur votre serveur Web interne.
2. Accédez au paramètre de mode avancé à partir d'un des systèmes ONTAP du cluster.

   ```
   set -privilege advanced
   ```

3. Exécutez la commande switch Health Monitor configure.

   ```
   cluster1::> system switch ethernet configure-health-monitor
   ```

4. Vérifiez que le résultat de la commande se termine par le texte suivant pour votre version de ONTAP :

ONTAP 9.15.1 et versions ultérieures

La surveillance de l'état du commutateur Ethernet a installé le fichier de configuration.

ONTAP 9.11.1 à 9.14.1

SHM a installé le fichier de configuration.

ONTAP 9.10.1

Le package CSHM téléchargé a été traité avec succès.

En cas d'erreur, contactez le support NetApp.

1. attendez jusqu'à deux fois l'intervalle d'interrogation du moniteur d'état du commutateur Ethernet, détecté en exécutant `system switch ethernet polling-interval show`, avant de terminer l'étape suivante.
2. Exécutez la commande `system switch ethernet configure-health-monitor show` sur le système ONTAP et assurez-vous que les commutateurs du cluster sont détectés avec le champ surveillé défini sur **Vrai** et le champ du numéro de série n'affichant pas **Inconnu**.

```
cluster1::> system switch ethernet configure-health-monitor show
```

Si votre modèle affiche toujours **OTHER** après avoir appliqué le fichier de configuration, contactez le support NetApp.

Voir le "configuration-santé-surveillance du commutateur Ethernet du système" commande pour plus de détails.

Et la suite ?

"Configurer la surveillance de l'état des commutateurs".

Surveiller l'état du commutateur IP MetroCluster

En savoir plus sur la surveillance de l'état des commutateurs dans une configuration IP MetroCluster

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage.

Remarques importantes pour la configuration de CSHM dans une configuration IP MetroCluster

Cette section présente les étapes générales de configuration de SNMPv3 et de collecte de journaux sur les commutateurs Cisco, Broadcom et NVIDIA SN2100. Vous devez suivre les étapes correspondant à la version du firmware du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le "Hardware Universe" pour vérifier les versions de firmware prises en charge.

Dans une configuration MetroCluster, vous configurez la surveillance de l'état sur les commutateurs de cluster locaux uniquement.

Pour la collecte des journaux avec les commutateurs Broadcom et Cisco, un nouvel utilisateur doit être créé sur le commutateur pour chaque cluster dont la collecte des journaux est activée. Dans une configuration MetroCluster, cela signifie que MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d'un utilisateur distinct sur les commutateurs. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l'utilisateur.

Avant de configurer le CSHM, vous devez désactiver les ISL inutilisés pour éviter toute alerte ISL inutile.

Configurer SNMPv3 pour surveiller la santé des commutateurs IP MetroCluster

Dans les configurations MetroCluster IP, vous pouvez configurer SNMPv3 pour surveiller l'état des commutateurs IP.

Cette procédure montre les étapes génériques de configuration de SNMPv3 sur un commutateur. Certaines versions du micrologiciel du commutateur répertoriées peuvent ne pas être prises en charge dans une configuration IP MetroCluster.

Vous devez suivre les étapes correspondant à la version du micrologiciel du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le "Hardware Universe" pour vérifier les versions de firmware prises en charge.

- SNMPv3 n’est pris en charge que sur ONTAP 9.12.1 et versions ultérieures.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 et les versions ultérieures corrigent ces deux problèmes :
  - "Pour la surveillance de l’état ONTAP des commutateurs Cisco, le trafic SNMPv2 peut toujours être visible après le passage à SNMPv3 pour la surveillance"
  - "Alertes de ventilateur et d’alimentation de commutateur faussement positives en cas de pannes SNMP"

Description de la tâche

Les commandes suivantes sont utilisées pour configurer un nom d’utilisateur SNMPv3 sur les commutateurs **Broadcom**, **Cisco** et **NVIDIA** :

Commutateurs Broadcom

Configurez un nom d'utilisateur SNMPv3 OPÉRATEUR RÉSEAU sur les commutateurs Broadcom BES-53248.

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-
md5|auth-sha] [priv-aes128|priv-des]
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version
SNMPv3 -community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp status
```

```
(sw1)(Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1)(Config)# show snmp user snmp

     Name            Group Name      Auth Priv
                                     Meth Meth    Remote Engine ID
---------------- ------------------ ---- ------
-------------------------
<username>        network-admin      MD5  AES128
8000113d03d8c497710bee
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Après avoir attendu la période d'interrogation CSHM, vérifiez que le numéro de série est renseigné pour le commutateur Ethernet.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: <username>
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA
```

Commutateurs Cisco

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs Cisco 9336C-FX2 :

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3_USER NoAuth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3_USER AuthEncrypt  auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp user
```

```
(sw1)(Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1)(Config)# show snmp user

-----------------------------------------------------------------------
---------
                              SNMP USERS
-----------------------------------------------------------------------
---------

User              Auth            Priv(enforce)   Groups
acl_filter
----------------- --------------- --------------- ---------------
-----------
admin             md5             des(no)         network-admin
SNMPv3User        md5             aes-128(no)     network-operator

-----------------------------------------------------------------------
---------
     NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
-----------------------------------------------------------------------
---------

User              Auth                Priv
----------------- ------------------ ------------

(sw1)(Config)#
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: cshm1!
                                   Model Number: N9K-C9336C-FX2
                                 Switch Network: cluster-network
                               Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                     Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: N9K-C9336C-FX2
                               Switch Network: cluster-network
                             Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                      Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                       Source Of Switch Version: CDP/ISDP
                                 Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                  RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
```

NVIDIA - CL 5.4.0

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.4.0 :

- Pour **pas d'authentification** :

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     4318
Version 1 and 2c Community String  Configured
Version 3 Usernames                Not Configured
---------------------------------  ----------------
cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf        2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf   2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
 # Auto-generated config file: do not edit. #
 agentaddress udp:@mgmt:161
 agentxperms 777 777 snmp snmp
 agentxsocket /var/agentx/master
 createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
 ifmib_max_num_ifaces 500
 iquerysecname _snmptrapusernameX
 master agentx
 monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```
 pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
 pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! default


net add/del commands since the last "net commit"

User        Timestamp                   Command
----------  --------------------------
------------------------------------------------------------------------
-----
SNMPv3User  2020-08-11 00:13:51.826987  net add snmp-server username
SNMPv3User auth-md5 <password> encrypt-aes <password>

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     24253
Version 1 and 2c Community String  Configured
Version 3 Usernames                Configured     <---- Configured
here
---------------------------------  ----------------
cumulus@sw1:~$
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv2c
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                      Reason For Not Monitoring: None
                       Source Of Switch Version: LLDP
                                 Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

NVIDIA - CL 5.11.0

Configurez un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.11.0 :

- Pour **pas d'authentification** :

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server
                      applied
--------------------  ----------------------------------------
[username]            SNMPv3_USER
[username]            limiteduser1
[username]            testuserauth
[username]            testuserauthaes
[username]            testusernoauth
trap-link-up
  check-frequency     60
trap-link-down
  check-frequency     60
[listening-address]   all
[readonly-community]  $nvsec$94d69b56e921aec1790844eb53e772bf
state                 enabled
cumulus@sw1:~$
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
          Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Configurer la collecte de journaux sur un commutateur IP MetroCluster

Dans une configuration IP MetroCluster, vous pouvez configurer la collecte de journaux pour collecter les journaux de commutation à des fins de débogage.

> Sur les commutateurs Broadcom et Cisco, un nouvel utilisateur est requis pour chaque cluster avec collecte de journaux. Par exemple, MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d'un utilisateur distinct sur les commutateurs. L'utilisation de plusieurs clés SSH pour un même utilisateur n'est pas prise en charge.

Description de la tâche

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage. Cette procédure vous guide tout au long du processus de configuration de la collecte, de demande de journaux **support** détaillés et d'activation d'une collecte horaire de données **périodiques** collectées par AutoSupport.

REMARQUE : si vous activez le mode FIPS, vous devez effectuer les opérations suivantes :

1. Régénérer les clés SSH sur le commutateur en suivant les instructions du fournisseur.
2. Régénérer les clés SSH dans ONTAP à l'aide de `debug system regenerate-systemshell-key-pair`
3. Réexécutez la routine de configuration de la collecte des journaux à l'aide de la `system switch ethernet log setup-password` commande

Avant de commencer

- L'utilisateur doit avoir accès aux commandes du commutateur `show` . S'ils ne sont pas disponibles, créez un nouvel utilisateur et accordez les autorisations nécessaires à l'utilisateur.
- La surveillance de l'état du commutateur doit être activée pour le commutateur. Vérifiez cela en vous assurant que `Is Monitored:` le champ est défini sur **true** dans la sortie du `system switch ethernet show` commande.
- Pour la collecte de journaux avec les commutateurs Broadcom et Cisco :
  - L'utilisateur local doit disposer de privilèges d'administrateur réseau.
  - Un nouvel utilisateur doit être créé sur le commutateur pour chaque configuration de cluster avec la collecte des journaux activée. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l'utilisateur.
- Pour la prise en charge de la collecte de journaux avec les commutateurs NVIDIA, *user* pour la collecte de journaux doit être autorisé à exécuter la `cl-support` commande sans avoir à fournir de mot de passe. Pour autoriser cette utilisation, lancer la commande :

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus
```

Étapes

ONTAP 9.15.1 et versions ultérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

   REMARQUE : Si vous répondez **y** à l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessaires comme indiqué dans Avant de commencer .

   ```
   system switch ethernet log setup-password
   ```

   ```
   cluster1::*> system switch ethernet log setup-password
   Enter the switch name: <return>
   The switch name entered is not recognized.
   Choose from the following list:
   cs1
   cs2

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs1
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs2

   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>
   ```

   Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Activer la collecte périodique des journaux :

   ```
   system switch ethernet log modify -device <switch-name> -periodic
   -enabled true
   ```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs1: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs2: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       true        scheduled
never-run
cs2                                       true        scheduled
never-run
2 entries were displayed.
```

2. Demander la collecte du journal de support :

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1

cs1: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> system switch ethernet log collect-support-log -device
cs2

cs2: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> *system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       false       halted
initiated
cs2                                       true        scheduled
initiated
2 entries were displayed.
```

3. Pour afficher tous les détails de la collecte des journaux, y compris l'activation, le message d'état, l'horodatage précédent et le nom de fichier de la collecte périodique, l'état de la demande, le message d'état, ainsi que l'horodatage précédent et le nom de fichier de la collection de support, utilisez les éléments suivants :

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

                    Switch Name: cs1
           Periodic Log Enabled: true
            Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
    Last Periodic Log Timestamp: 3/11/2024 11:02:59
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:14:20
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

                    Switch Name: cs2
           Periodic Log Enabled: false
            Periodic Log Status: Periodic collection has been
halted.
    Last Periodic Log Timestamp: 3/11/2024 11:05:18
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:18:54
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

ONTAP 9.14.1 et versions antérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

   REMARQUE : si vous répondez à `y` l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessairesAvant de commencer, comme indiqué dans .

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Pour demander la collecte des journaux d'assistance et activer la collecte périodique, exécutez la commande suivante. Ceci lance les deux types de collecte de journaux : les journaux détaillés `Support` et une collecte de données toutes les heures `Periodic`.

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Attendez 10 minutes, puis vérifiez que la collecte des journaux se termine :

```
system switch ethernet log show
```

Si des États d'erreur sont signalés par la fonction de collecte de journaux (visible dans la sortie de `system switch ethernet log show`), voir "Dépannage de la collecte des journaux" pour plus de détails.

Gérer la surveillance des commutateurs Ethernet dans une configuration IP MetroCluster

Dans la plupart des cas, les commutateurs Ethernet sont automatiquement détectés par ONTAP et surveillés par CSHM. Le fichier de configuration de référence (RCF) appliqué au commutateur, entre autres, active le protocole CDP (Cisco Discovery Protocol) et/ou le protocole LLDP (Link Layer Discovery Protocol). Cependant, vous devrez peut-être ajouter manuellement un commutateur qui n'est pas détecté ou supprimer un commutateur qui n'est plus utilisé. Vous pouvez également arrêter la surveillance active tout en maintenant le commutateur dans la configuration, par exemple pendant la maintenance.

Créez une entrée de commutateur afin que ONTAP puisse la surveiller

Description de la tâche

Utilisez `system switch ethernet create` la commande pour configurer et activer manuellement la surveillance d'un commutateur Ethernet spécifié. Ceci est utile si ONTAP n'ajoute pas automatiquement le commutateur, ou si vous avez précédemment supprimé le commutateur et souhaitez le rajouter.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type
cluster-network
```

Un exemple type est l'ajout d'un commutateur nommé [DeviceName], avec l'adresse IP 1.2.3.4, et les informations d'identification SNMPv2c définies sur **cshm1!**. Utilisez `-type storage-network` plutôt que `-type cluster-network` si vous configurez un commutateur de stockage.

Désactiver la surveillance sans supprimer le commutateur

Si vous souhaitez mettre en pause ou arrêter la surveillance d'un certain commutateur, mais le conserver pour une surveillance future, modifiez son `is-monitoring-enabled-admim` paramètre au lieu de le supprimer.

Par exemple :

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Cela vous permet de préserver les détails et la configuration du commutateur sans générer de nouvelles alertes ou de nouvelles découvertes.

Retirez un commutateur dont vous n'avez plus besoin

Utiliser `system switch ethernet delete` pour supprimer un commutateur qui a été déconnecté ou n'est plus nécessaire :

```
system switch ethernet delete -device DeviceName
```

Par défaut, cette commande réussit uniquement si ONTAP ne détecte pas actuellement le commutateur via CDP ou LLDP. Pour supprimer un commutateur découvert, utilisez le `-force` paramètre :

```
system switch ethernet delete -device DeviceName -force
```

Lorsque `-force` est utilisé, le commutateur peut être ajouté automatiquement si ONTAP le détecte à nouveau.

Vérifier la surveillance du commutateur Ethernet dans une configuration IP MetroCluster

Le moniteur d'état du commutateur Ethernet (CSHM) tente automatiquement de surveiller les commutateurs qu'il découvre ; cependant, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

Confirmez la surveillance des commutateurs Ethernet connectés

Description de la tâche

Pour vérifier que les commutateurs Ethernet connectés sont surveillés, exécutez :

```
system switch ethernet show
```

Si la colonne affiche **OTHER** ou si `Model` le `IS Monitored` champ affiche **FALSE**, ONTAP ne peut pas surveiller le commutateur. Une valeur de **AUTRE** indique généralement que ONTAP ne prend pas en charge ce commutateur pour la surveillance de l'intégrité.

Le `IS Monitored` champ est défini sur **FALSE** pour la raison spécifiée dans le `Reason` champ.

> Si un commutateur n'est pas répertorié dans la sortie de commande, ONTAP ne l'a probablement pas découvert. Vérifiez que le commutateur est correctement câblé. Si nécessaire, vous pouvez ajouter le commutateur manuellement. Voir "Gérer la surveillance des commutateurs Ethernet" pour plus de détails.

Vérifiez que les versions du firmware et des fichiers RCF sont à jour

Assurez-vous que le commutateur exécute le micrologiciel le plus récent pris en charge et qu'un fichier RCF compatible a été appliqué. Plus d'informations sont disponibles sur le "Page des téléchargements du support NetApp".

Par défaut, le moniteur d'intégrité utilise SNMPv2c avec la chaîne de communauté **cshm1!** pour la surveillance, mais SNMPv3 peut également être configuré.

Si vous devez modifier la chaîne de communauté SNMPv2c par défaut, assurez-vous que la chaîne de communauté SNMPv2c souhaitée a été configurée sur le commutateur.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c
-community-or-username newCommunity!
```

> Pour plus d'informations sur la configuration de SNMPv3 pour utilisation, reportez-vous à la section"Facultatif : configurer SNMPv3".

Confirmez la connexion au réseau de gestion

Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

Une connexion de port de gestion correcte est requise pour que ONTAP puisse effectuer des requêtes SNMP et collecter des journaux.

Informations associées

- "Résolution des alertes"

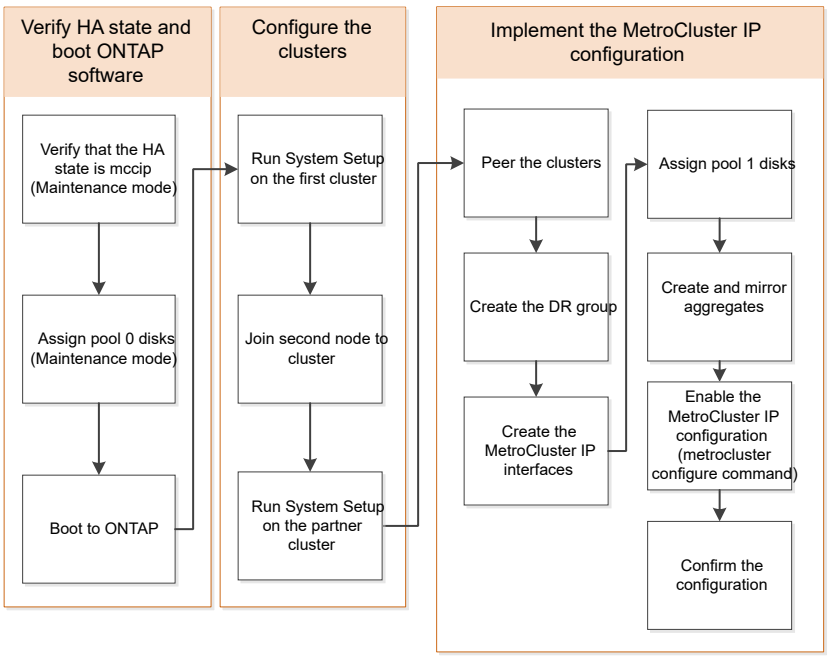
Configurez le logiciel MetroCluster dans ONTAP

Configurez le logiciel MetroCluster à l'aide de l'interface de ligne de commandes

Configurer les nœuds et les clusters ONTAP dans la configuration IP MetroCluster

Vous devez installer chaque nœud dans la configuration MetroCluster de ONTAP, y compris les configurations au niveau des nœuds et la configuration des nœuds en deux sites. Vous devez également implémenter la relation MetroCluster entre les deux sites.

Si un module de contrôleur tombe en panne pendant la configuration, reportez-vous à la section "Scénarios de panne du module de contrôleur lors de l'installation de MetroCluster".



Configurer des configurations IP MetroCluster à huit nœuds

Une configuration MetroCluster à huit nœuds se compose de deux groupes de reprise après incident. Pour configurer le premier groupe de reprise après sinistre, suivez les étapes décrites dans cette section. Après avoir configuré le premier groupe de reprise après sinistre, suivez les étapes suivantes : "étendre une configuration IP MetroCluster à quatre nœuds à une configuration à huit nœuds" .

Rassemblez les informations requises pour votre configuration IP MetroCluster

Vous devez rassembler les adresses IP requises pour les modules de contrôleur avant de commencer le processus de configuration.

Vous pouvez utiliser ces liens pour télécharger des fichiers CSV et remplir les tableaux avec les informations spécifiques à votre site.

"Fiche d'installation IP de MetroCluster, site_A"

"Fiche d'installation IP de MetroCluster, site_B"

Comparez les configurations de cluster standard ONTAP et MetroCluster

La configuration des nœuds de chaque cluster dans une configuration MetroCluster est similaire à celle des nœuds d'un cluster standard.

La configuration MetroCluster est basée sur deux clusters standard. Physiquement, la configuration doit être symétrique. Chaque nœud présente la même configuration matérielle et tous les composants MetroCluster doivent être câblés et configurés. Cependant, la configuration logicielle de base des nœuds dans une configuration MetroCluster est identique à celle des nœuds d'un cluster standard.

Étape de configuration	Configuration standard en cluster	Configuration MetroCluster
Configurez la gestion, le cluster et la LIF de données sur chaque nœud.	La même chose dans les deux types de clusters	
Configurer l'agrégat root.	La même chose dans les deux types de clusters	
Configurez le cluster sur un nœud.	La même chose dans les deux types de clusters	
Joignez l'autre nœud au cluster.	La même chose dans les deux types de clusters	
Créez un agrégat racine en miroir.	Facultatif	Obligatoire
Peer-to-peer des clusters	Facultatif	Obligatoire
Activez la configuration MetroCluster.	Ne s'applique pas	Obligatoire

Vérifiez l'état de configuration HA de votre contrôleur et des composants de votre châssis dans une configuration IP MetroCluster

Dans une configuration IP MetroCluster, vous devez vérifier que l'état ha-config du contrôleur et des composants du châssis est défini sur `mccip` pour qu'ils démarrent correctement. Bien que cette valeur doive être préconfigurée sur les systèmes reçus de l'usine, vous devez toujours vérifier le réglage avant de continuer.

Si l'état haute disponibilité du module de contrôleur et du châssis est incorrect, vous ne pouvez pas configurer la MetroCluster sans avoir réinitialisé le nœud. Vous devez corriger le paramètre à l'aide de cette procédure, puis initialiser le système à l'aide de l'une des procédures suivantes :

- Dans une configuration IP MetroCluster, suivez les étapes de la section "Restaurez les paramètres par défaut du système sur un module de contrôleur".
- Dans une configuration MetroCluster FC, suivez les étapes de la section "Restaurez les paramètres par défaut du système et configurez le type de HBA sur un module de contrôleur".

Avant de commencer

Vérifiez que le système est en mode Maintenance.

Étapes

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

   `ha-config show`

   L'état correct de haute disponibilité dépend de votre configuration MetroCluster.

Type de configuration MetroCluster	État HAUTE DISPONIBILITÉ pour tous les composants…
Configuration FC MetroCluster à huit ou quatre nœuds	mcc
Configuration FC MetroCluster à deux nœuds	mcc-2n
Configuration IP MetroCluster à huit ou quatre nœuds	ccip

2. Si l'état système affiché du contrôleur est incorrect, définissez l'état de haute disponibilité correct pour votre configuration sur le module de contrôleur :

Type de configuration MetroCluster	Commande
Configuration FC MetroCluster à huit ou quatre nœuds	`ha-config modify controller mcc`
Configuration FC MetroCluster à deux nœuds	`ha-config modify controller mcc-2n`
Configuration IP MetroCluster à huit ou quatre nœuds	`ha-config modify controller mccip`

3. Si l'état système affiché du châssis n'est pas correct, définissez l'état de haute disponibilité correct pour votre configuration sur le châssis :

Type de configuration MetroCluster	Commande
Configuration FC MetroCluster à huit ou quatre nœuds	`ha-config modify chassis mcc`
Configuration FC MetroCluster à deux nœuds	`ha-config modify chassis mcc-2n`
Configuration IP MetroCluster à huit ou quatre nœuds	`ha-config modify chassis mccip`

4. Démarrez le nœud sur ONTAP :

   `boot_ontap`

5. Répétez cette procédure pour vérifier l'état de haute disponibilité sur chaque nœud de la configuration MetroCluster.

Restaurer les paramètres par défaut du système sur un module de contrôleur avant de configurer une configuration IP MetroCluster

Réinitialisez et restaurez les valeurs par défaut sur les modules de contrôleur.

1. Dans l'invite DU CHARGEUR, valeurs par défaut des variables environnementales : `set-defaults`
2. Démarrez le nœud sur le menu de démarrage : `boot_ontap menu`

   Une fois que vous avez exécuté cette commande, attendez que le menu de démarrage s'affiche.

3. Effacez la configuration des nœuds :

   - Si vous utilisez des systèmes configurés pour ADP, sélectionnez option `9a` dans le menu de démarrage, puis répondez `no` lorsque vous y êtes invité.

     Ce processus est perturbateur.

     L'écran suivant affiche l'invite du menu de démarrage :

```
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)? 9a
...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

◦ Si votre système n'est pas configuré pour ADP, tapez `wipeconfig` À l'invite du menu de démarrage, puis appuyez sur entrée.

L'écran suivant affiche l'invite du menu de démarrage :

```
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.
    Selection (1-9)?  wipeconfig
This option deletes 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?: yes
Rebooting to finish wipeconfig request.
```

Attribuer manuellement des lecteurs au pool 0 dans une configuration IP MetroCluster

Si vous n'avez pas reçu les systèmes préconfigurés en usine, vous devrez peut-être affecter manuellement les lecteurs du pool 0. Selon le modèle de plate-forme et si le système utilise ADP, vous devez affecter manuellement les lecteurs au pool 0 pour chaque nœud de la configuration IP MetroCluster. La procédure que vous utilisez dépend de la version de ONTAP que vous utilisez.

Affectation manuelle de lecteurs pour le pool 0 (ONTAP 9.4 et versions ultérieures)

Si le système n'a pas été préconfiguré en usine et ne répond pas aux exigences relatives à l'affectation automatique des disques, vous devez affecter manuellement les disques du pool 0.

Description de la tâche

Cette procédure s'applique aux configurations exécutant ONTAP 9.4 ou version ultérieure.

Pour déterminer si votre système nécessite une affectation manuelle du disque, vous devez passer en revue "Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures".

Effectuez les étapes suivantes en mode Maintenance. La procédure doit être effectuée sur chaque nœud de la configuration.

Les exemples de cette section se basent sur les hypothèses suivantes :

- Les disques des nœuds Node_A_1 et Node_A_2 sont propriétaires :
  - Site_A-shelf_1 (local)
  - Site_B-tiroir_2 (distant)
- Les propriétaires des disques des nœuds_B_1 et Node_B_2 sont les suivants :

- Site_B-shelf_1 (locale)
- Site_A-shelf_2 (à distance)

Étapes

1. Afficher le menu de démarrage :

   ```
   boot_ontap menu
   ```

2. Sélectionnez l'option 9a et répondez `no` lorsque vous y êtes invité.

   L'écran suivant affiche l'invite du menu de démarrage :

   ```
   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)? 9a

   ...

   ########## WARNING: AGGREGATES WILL BE DESTROYED ##########
   This is a disruptive operation that applies to all the disks
   that are attached and visible to this node.

   Before proceeding further, make sure that:

   The aggregates visible from this node do not contain
   data that needs to be preserved.
   This option (9a) has been executed or will be executed
   on the HA partner node (and DR/DR-AUX partner nodes if
   applicable), prior to reinitializing any system in the
   HA-pair or MetroCluster configuration.
   The HA partner node (and DR/DR-AUX partner nodes if
   applicable) is currently waiting at the boot menu.
   Do you want to abort this operation (yes/no)? no
   ```

3. Lorsque le nœud redémarre, appuyez sur Ctrl-C lorsque vous êtes invité à afficher le menu de démarrage, puis sélectionnez l'option **Maintenance mode boot**.

4. En mode Maintenance, attribuez manuellement des disques aux agrégats locaux sur le nœud :

   `disk assign disk-id -p 0 -s local-node-sysid`

   Les disques doivent être affectés de manière symétrique, de sorte que chaque nœud dispose d'un nombre égal de disques. La procédure suivante concerne une configuration avec deux tiroirs de stockage sur chaque site.

   a. Lors de la configuration de node_A_1, affectez manuellement les disques des emplacements 0 à 11 dans la pool0 du nœud A1 à partir de site_A-shelf_1.
   b. Lors de la configuration de node_A_2, affectez manuellement les lecteurs de l'emplacement 12 à 23 dans la pool0 du nœud A2 à partir de site_A-shelf_1.
   c. Lors de la configuration de node_B_1, affectez manuellement les disques des emplacements 0 à 11 dans la pool0 du nœud B1 du site_B-shelf_1.
   d. Lors de la configuration de node_B_2, affectez manuellement les lecteurs de l'emplacement 12 à 23 dans la pool0 du nœud B2 à partir de site_B-shelf_1.

5. Quitter le mode Maintenance :

   `halt`

6. Afficher le menu de démarrage :

   `boot_ontap menu`

7. Répétez cette procédure sur les autres nœuds de la configuration MetroCluster IP.
8. Sélectionnez l'option **4** dans le menu d'amorçage sur les deux nœuds et laissez le système démarrer.
9. Passez à la section "Configuration de ONTAP".

Attribution manuelle de disques pour le pool 0 (ONTAP 9.3)

Si vous avez au moins deux tiroirs disques pour chaque nœud, la fonctionnalité d'affectation automatique d'ONTAP vous permet d'attribuer automatiquement les disques locaux (pool 0).

Description de la tâche

Lorsque le nœud est en mode Maintenance, vous devez d'abord attribuer un seul disque sur les tiroirs appropriés afin de regrouper 0. ONTAP attribue ensuite automatiquement le reste des disques du tiroir au même pool. Cette tâche n'est pas requise sur les systèmes reçus de l'usine, qui disposent du pool 0 pour contenir l'agrégat racine préconfiguré.

Cette procédure s'applique aux configurations exécutant ONTAP 9.3.

Cette procédure n'est pas requise si vous avez reçu votre configuration MetroCluster en usine. Les nœuds situés en usine sont configurés avec 0 disques pool et des agrégats racine.

Cette procédure ne peut être utilisée que si vous disposez d'au moins deux tiroirs disques pour chaque nœud, ce qui permet l'affectation automatique des disques au niveau du tiroir. Si vous ne pouvez pas utiliser l'affectation automatique au niveau du tiroir, vous devez affecter manuellement vos disques locaux de sorte que chaque nœud dispose d'un pool local de disques (pool 0).

Ces étapes doivent être effectuées en mode Maintenance.

Les exemples de cette section supposent les tiroirs disques suivants :

- Node_A_1 possède des disques sur :
  - Site_A-shelf_1 (local)
  - Site_B-tiroir_2 (distant)
- Node_A_2 est connecté à :
  - Site_A-shelf_3 (local)
  - Site_B-shelf_4 (à distance)
- Node_B_1 est connecté à :
  - Site_B-shelf_1 (locale)
  - Site_A-shelf_2 (à distance)
- Node_B_2 est connecté à :
  - Site_B-shelf_3 (locale)
  - Site_A-shelf_4 (à distance)

Étapes

1. Assigner manuellement un seul disque pour l'agrégat racine sur chaque nœud :

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   L'assignation manuelle de ces disques permet à la fonctionnalité d'autoassignation des ONTAP d'assigner les autres disques de chaque shelf.

   a. Sur le nœud_A_1, affectez manuellement un disque du site local_A-shelf_1 au pool 0.
   b. Sur node_A_2, affectez manuellement un disque du site local_A-shelf_3 au pool 0.
   c. Sur le nœud_B_1, affectez manuellement un disque du site local_B-shelf_1 au pool 0.
   d. Sur le nœud_B_2, affectez manuellement un disque du site local_B-shelf_3 au pool 0.
2. Démarrez chaque nœud sur le site A, en utilisant l'option 4 du menu de démarrage :

   Vous devez effectuer cette étape sur un nœud avant de passer au nœud suivant.

   a. Quitter le mode Maintenance :

      `halt`

   b. Afficher le menu de démarrage :

      `boot_ontap menu`

   c. Sélectionnez l'option 4 dans le menu de démarrage et continuez.
3. Démarrez chaque nœud sur le site B, en utilisant l'option 4 du menu de démarrage :

   Vous devez effectuer cette étape sur un nœud avant de passer au nœud suivant.

   a. Quitter le mode Maintenance :

      `halt`

   b. Afficher le menu de démarrage :

```
boot_ontap menu
```

c. Sélectionnez l'option 4 dans le menu de démarrage et continuez.

Configurer des nœuds ONTAP dans une configuration IP MetroCluster

Après le démarrage de chaque nœud, vous êtes invité à effectuer une configuration de nœud et de cluster de base. Une fois le cluster configuré, vous revenez à l'interface de ligne de commandes de ONTAP pour créer des agrégats et créer la configuration MetroCluster.

Avant de commencer

- Vous devez avoir câblé la configuration MetroCluster.

Si vous devez démarrer en réseau les nouveaux contrôleurs, reportez-vous à la section "NetBoot les nouveaux modules de contrôleur".

Description de la tâche

Cette tâche doit être effectuée sur les deux clusters en configuration MetroCluster.

Étapes

1. Mettez chaque nœud sous tension sur le site local si vous ne l'avez pas déjà fait et laissez-le démarrer complètement.

   Si le système est en mode maintenance, vous devez lancer la commande halt pour quitter le mode Maintenance, puis lancer le `boot_ontap` commande de démarrage du système et d'obtention de la configuration du cluster.

2. Sur le premier nœud de chaque cluster, suivez les invites pour configurer le cluster.

   a. Activer l'outil AutoSupport en suivant les instructions fournies par le système.

      La sortie doit être similaire à ce qui suit :

```
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
.
.
.
```

b. Configurez l'interface de gestion des nœuds en répondant aux invites.

   Les invites sont similaires à ce qui suit :

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
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 172.17.8.229
has been created.
```

c. Créez le cluster en répondant aux invites.

   Les invites sont similaires à ce qui suit :

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
create


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Ajoutez des licences, configurez un SVM d'administration du cluster, puis entrez les informations DNS en répondant aux invites.

Les invites sont similaires à ce qui suit :

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Activez le basculement du stockage et configurez le nœud en répondant aux invites.

Les invites sont similaires à ce qui suit :

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Terminez la configuration du nœud, mais ne créez pas d'agrégats de données.

Vous pouvez utiliser ONTAP System Manager et pointer votre navigateur Web vers l'adresse IP de gestion du cluster (https://172.17.12.153).)

"Gestion des clusters à l'aide de System Manager (ONTAP 9.7 et versions antérieures)"

"ONTAP System Manager (version 9.7 et ultérieure)"

g. Configurez le processeur de service :

"Configuration du réseau SP/BMC"

"Utilisez un processeur de service avec System Manager - ONTAP 9.7 et versions antérieures"

3. Démarrez le contrôleur suivant et connectez-le au cluster, en suivant les invites.
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 configurer le mode HA sur chaque nœud, puis redémarrer les nœuds :

```
storage failover modify -mode ha -node localhost
```

> L'état de configuration attendu pour la haute disponibilité et le basculement du stockage est le suivant :
>
> - Le mode HA est configuré mais le basculement du stockage n'est pas activé.
> - La fonctionnalité de basculement HAUTE DISPONIBILITÉ est désactivée.
> - Les interfaces HAUTE DISPONIBILITÉ sont hors ligne.
> - Le mode HA, le basculement du stockage et les interfaces sont configurés ultérieurement dans ce processus.

5. Vérifiez que quatre ports sont configurés en tant qu'interconnexions de cluster :

```
network port show
```

Les interfaces IP MetroCluster ne sont pas configurées pour le moment et n'apparaissent pas dans la sortie de la commande.

L'exemple suivant montre deux ports de cluster sur le nœud_A_1 :

```
cluster_A::*> network port show -role cluster


Node: node_A_1


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
```

```
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Répétez cette procédure sur le cluster partenaire.

Que faire ensuite

Revenez à l'interface de ligne de commandes ONTAP et terminez la configuration MetroCluster en effectuant les tâches suivantes.

Configurer les clusters ONTAP dans une configuration IP MetroCluster

Vous devez peer-to-peer les clusters, mettre en miroir les agrégats racine, créer un agrégat de données en miroir, puis lancer la commande pour mettre en œuvre les opérations MetroCluster.

Description de la tâche

Avant de courir `metrocluster configure`, Le mode HA et la mise en miroir DR ne sont pas activés et un message d'erreur peut s'afficher concernant ce comportement attendu. Vous activez le mode HA et la mise en miroir de reprise après incident plus tard lors de l'exécution de la commande `metrocluster configure` pour implémenter la configuration.

Désactivation de l'affectation automatique des lecteurs (en cas d'affectation manuelle dans ONTAP 9.4)

Dans ONTAP 9.4, si votre configuration MetroCluster IP comporte moins de quatre tiroirs de stockage externes par site, vous devez désactiver l'affectation automatique des disques sur tous les nœuds et attribuer manuellement des disques.

Description de la tâche

Cette tâche n'est pas requise dans ONTAP 9.5 et versions ultérieures.

Cette tâche ne s'applique pas à un système AFF A800 équipé d'un tiroir interne et sans tiroirs externes.

"Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures"

Étapes

1. Désactiver l'affectation automatique des disques :

   ```
   storage disk option modify -node <node_name> -autoassign off
   ```

2. Vous devez lancer cette commande sur tous les nœuds de la configuration IP MetroCluster.

Vérification de l'affectation des disques du pool 0

Vous devez vérifier que les lecteurs distants sont visibles par les nœuds et ont été correctement affectés.

Description de la tâche

L'assignation automatique dépend du modèle de plateforme de stockage et de l'organisation des tiroirs disques.

"Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures"

Étapes

1. Vérifiez que les disques du pool 0 sont affectés automatiquement :

   ```
   disk show
   ```

   L'exemple suivant montre la sortie « cluster_A » pour un système AFF A800 sans tiroir externe.

   Un quart (8 disques) ont été automatiquement affectés à « node_A_1 » et un trimestre a été automatiquement affecté à « node_A_2 ». Les disques restants seront des disques distants (pool 1) pour « node_B_1 » et « node_B_2 ».

   ```
   cluster_A::*> disk show
                    Usable      Disk      Container           Container
   Disk             Size        Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   ```

```
node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

L’exemple suivant montre la sortie « cluster_B » :

```
cluster_B::> disk show
                 Usable     Disk              Container   Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
```

```
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_B_2
node_B_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_B_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_B_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_B_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_B_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_B_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_B_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_B_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_B_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_B_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_B_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_B_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_B_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_B_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_B_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_B_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.

cluster_B::>
```

Peering des clusters

Les clusters de la configuration MetroCluster doivent être dans une relation de pairs, de sorte qu'ils puissent communiquer entre eux et exécuter la mise en miroir des données essentielle à la reprise sur incident de MetroCluster.

Informations associées

"Configuration cluster et SVM peering express"

"Considérations relatives à l'utilisation de ports dédiés"

"Points à prendre en compte lors du partage de ports de données"

Configuration des LIFs intercluster pour le peering de cluster

Vous devez créer des LIFs intercluster sur les ports utilisés pour la communication entre les clusters partenaires MetroCluster. Vous pouvez utiliser des ports ou ports dédiés qui ont également le trafic de données.

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 « intercluster 01 » sur le système « SVM 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.

Dans ONTAP 9.6 et versions ultérieures, exécutez :

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Dans ONTAP 9.5 et les versions antérieures, exécutez :

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création des 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 versions ultérieures, exécutez :

```
network interface show -service-policy default-intercluster
```

Dans ONTAP 9.5 et les versions antérieures, exécutez :

```
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 versions ultérieures, exécutez :

```
network interface show -service-policy default-intercluster -failover
```

Dans ONTAP 9.5 et les versions antérieures, exécutez :

```
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 « SVMe0e » 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
```

Informations associées

"Considérations relatives à l'utilisation de ports dédiés"

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 versions ultérieures, exécutez :

   ```
   network interface create -vserver <system_svm> -lif <lif_name> -service
   -policy default-intercluster -home-node <node_name> -home-port <port_name>
   -address <port_ip_address> -netmask <netmask>
   ```

   Dans ONTAP 9.5 et les versions antérieures, exécutez :

   ```
   network interface create -vserver <system_svm> -lif <lif_name> -role
   intercluster -home-node <node_name> -home-port <port_name> -address
   <port_ip_address> -netmask <netmask>
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création des 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 versions ultérieures, exécutez :

```
network interface show -service-policy default-intercluster
```

Dans ONTAP 9.5 et les versions antérieures, exécutez :

```
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 versions ultérieures, exécutez :

```
network interface show -service-policy default-intercluster -failover
```

Dans ONTAP 9.5 et les versions antérieures, exécutez :

```
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
```

Informations associées

"Points à prendre en compte lors du partage de ports de données"

Création d'une relation entre clusters

Vous pouvez utiliser la commande cluster peer create pour créer une relation homologue entre un cluster local et un cluster distant. Une fois la relation homologue créée, vous pouvez exécuter cluster peer create sur le cluster distant afin de l'authentifier auprès du cluster local.

Description de la tâche

- Vous devez avoir créé des LIF intercluster sur chaque nœud des clusters qui sont en cours de peering.
- Les clusters doivent exécuter ONTAP 9.3 ou version ultérieure.

Étapes

1. Sur le cluster destination, créez une relation entre pairs et le cluster source :

   ```
   cluster peer create -generate-passphrase -offer-expiration <MM/DD/YYYY
   HH:MM:SS|1…7days|1…168hours> -peer-addrs <peer_lif_ip_addresses> -ipspace
   <ipspace>
   ```

Si vous spécifiez les deux `-generate-passphrase` et `-peer-addrs`, Uniquement le cluster dont les LIFs intercluster sont spécifiés dans `-peer-addrs` peut utiliser le mot de passe généré.

Vous pouvez ignorer `-ipspace` Option si vous n'utilisez pas un IPspace personnalisé. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée une relation de cluster peer-to-peer sur un cluster distant non spécifié :

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Sur le cluster source, authentifier le cluster source sur le cluster destination :

   `cluster peer create -peer-addrs <peer_lif_ip_addresses> -ipspace <ipspace>`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant authentifie le cluster local sur le cluster distant aux adresses IP « 192.140.112.101 » et « 192.140.112.102 » de LIF intercluster :

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   Entrez la phrase de passe de la relation homologue lorsque vous y êtes invité.

3. Vérifiez que la relation entre clusters a été créée :

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                      Peer Cluster Name: cluster02
                          Cluster UUID: b07036f2-7d1c-11f0-bedb-
d039ea48b059
           Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
      Availability of the Remote Cluster: Available
                    Remote Cluster Name: cluster02
                    Active IP Addresses: 192.140.112.101,
192.140.112.102
                  Cluster Serial Number: 1-80-123456
                   Remote Cluster Nodes: cluster02-01, cluster02-02,
                  Remote Cluster Health: true
                Unreachable Local Nodes: -
             Operation Timeout (seconds): 60
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                 Timeout for RPC Connect: 10
               Timeout for Update Pings: 5
                       Last Update Time: 10/9/2025 10:15:29
            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
```

4. Vérifier la connectivité et l'état des nœuds de la relation peer-to-peer :

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

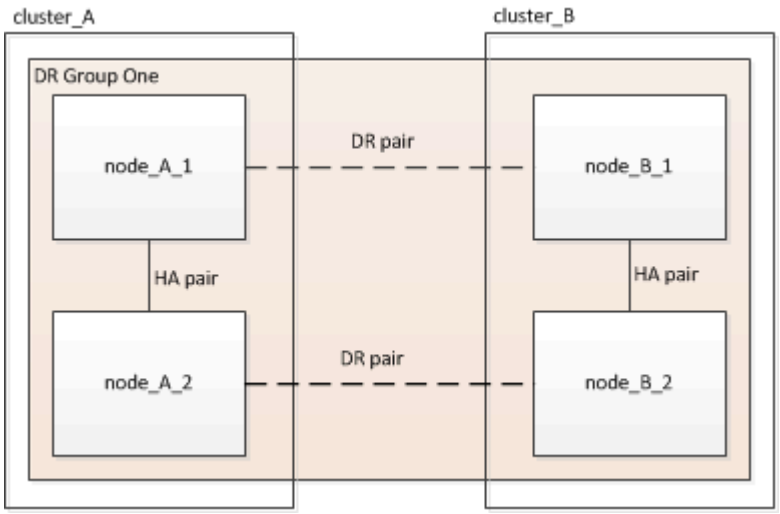
Création du groupe DR

Vous devez créer les relations de groupe de reprise après incident entre les clusters.

Description de la tâche

Cette procédure est effectuée sur l'un des clusters de la configuration MetroCluster afin de créer les relations de DR entre les nœuds des deux clusters.

Les relations de DR ne peuvent pas être modifiées une fois les groupes de DR créés.



Étapes

1. Vérifiez que les nœuds sont prêts à créer le groupe de reprise sur incident en entrant la commande

suivante sur chaque nœud :

```
metrocluster configuration-settings show-status
```

Le résultat de la commande doit afficher que les nœuds sont prêts :

```
cluster_A::> metrocluster configuration-settings show-status
Cluster                   Node          Configuration Settings Status
------------------------- -------------
-------------------------------
cluster_A                 node_A_1      ready for DR group create
                          node_A_2      ready for DR group create
2 entries were displayed.
```

```
cluster_B::> metrocluster configuration-settings show-status
Cluster                   Node          Configuration Settings Status
------------------------- -------------
-------------------------------
cluster_B                 node_B_1      ready for DR group create
                          node_B_2      ready for DR group create
2 entries were displayed.
```

2. Créez le groupe DR :

```
metrocluster configuration-settings dr-group create -partner-cluster
<partner_cluster_name> -local-node <local_node_name> -remote-node
<remote_node_name>
```

Cette commande n'est émise qu'une seule fois. Il n'est pas nécessaire de le répéter sur le cluster partenaire. Dans la commande, vous spécifiez le nom du cluster distant, ainsi que le nom d'un nœud local et d'un nœud sur le cluster partenaire.

Les deux nœuds que vous spécifiez sont configurés en tant que partenaires DR et les deux autres nœuds (qui ne sont pas spécifiés dans la commande) sont configurés en tant que seconde paire DR dans le groupe DR. Ces relations ne peuvent pas être modifiées une fois que vous avez saisi cette commande.

La commande suivante crée ces paires de reprise sur incident :

- Node_A_1 et node_B_1
- Node_A_2 et node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Configuration et connexion des interfaces IP MetroCluster

Vous devez configurer les interfaces IP MetroCluster utilisées pour la réplication du stockage de chaque nœud et du cache non volatile. Vous déterminez ensuite les connexions en utilisant les interfaces IP de MetroCluster. Cela crée des connexions iSCSI pour la réplication du stockage.

> L'adresse IP MetroCluster et les ports de commutateur connectés ne sont pas mis en ligne avant la création des interfaces IP MetroCluster.

Description de la tâche

- Vous devez créer deux interfaces pour chaque nœud. Les interfaces doivent être associées aux VLAN définis dans le fichier RCF MetroCluster.
- Vous devez créer tous les ports de l'interface IP MetroCluster « A » sur le même VLAN et tous les ports de l'interface IP MetroCluster « B » dans l'autre VLAN. Reportez-vous à la section "Considérations relatives à la configuration MetroCluster IP".
- 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".

  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.

  Si elle est prise en charge, vous pouvez également spécifier un VLAN différent (non par défaut) supérieur à 100 (entre 101 et 4095) en utilisant le `-vlan-id` paramètre de la `metrocluster configuration-settings interface create` commande.

  Les plates-formes suivantes ne prennent pas en charge le `-vlan-id` paramètre :

  - FAS8200 ET AFF A300
  - AFF A320
  - FAS9000 et AFF A700
  - AFF C800, ASA C800, AFF A800 et ASA A800

    Toutes les autres plates-formes prennent en charge le `-vlan-id` paramètre.

    Les affectations de VLAN par défaut et valides dépendent du fait que la plate-forme prend en charge le `-vlan-id` paramètre :

Les plateformes qui prennent en charge <code>-vlan-</code>

VLAN par défaut :

- Lorsque le `-vlan-id` paramètre n'est pas spécifié, les interfaces sont créées avec le VLAN 10 pour les ports "A" et le VLAN 20 pour les ports "B".
- Le VLAN spécifié doit correspondre au VLAN sélectionné dans la FCR.

Plages VLAN valides :

- VLAN 10 et 20 par défaut
- VLAN 101 et supérieur (entre 101 et 4095)

Les plateformes qui ne prennent pas en charge <code>-vlan-</code>

VLAN par défaut :

- Sans objet L'interface ne nécessite pas la spécification d'un VLAN sur l'interface MetroCluster. Le port du commutateur définit le VLAN utilisé.

Plages VLAN valides :

- Tous les VLAN non explicitement exclus lors de la génération de la FCR. Le RCF vous avertit si le VLAN n'est pas valide.

- Les ports physiques utilisés par les interfaces IP MetroCluster dépendent du modèle de plateforme. Reportez-vous "Branchez les câbles des commutateurs IP MetroCluster" à pour connaître l'utilisation des ports pour votre système.
- Les adresses IP et sous-réseaux suivants sont utilisés dans les exemples :

Nœud	Interface	Adresse IP	Sous-réseau
Nœud_A_1	Interface IP MetroCluster 1	10.1.1.1	10.1.1/24
Interface IP MetroCluster 2	10.1.2.1	10.1.2/24	Nœud_A_2
Interface IP MetroCluster 1	10.1.1.2	10.1.1/24	Interface IP MetroCluster 2
10.1.2.2	10.1.2/24	Nœud_B_1	Interface IP MetroCluster 1
10.1.1.3	10.1.1/24	Interface IP MetroCluster 2	10.1.2.3
10.1.2/24	Nœud_B_2	Interface IP MetroCluster 1	10.1.1.4

10.1.1/24	Interface IP MetroCluster 2	10.1.2.4	10.1.2/24

- Cette procédure utilise les exemples suivants :

  Ports pour un système AFF A700 ou FAS9000 (e5a et e5b).

  Ports d'un système AFF A220 pour montrer comment utiliser le `-vlan-id` paramètre sur une plateforme prise en charge.

  Configurez les interfaces sur les ports appropriés pour votre modèle de plate-forme.

Étapes

1. Vérifiez que l'affectation automatique des disques est activée pour chaque nœud :

   `storage disk option show`

   L'assignation automatique des disques attribue 0 pool et 1 pool disques par tiroir.

   La colonne affectation automatique indique si l'affectation automatique des disques est activée.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

2. Vérifiez que vous pouvez créer les interfaces IP MetroCluster sur les nœuds :

   `metrocluster configuration-settings show-status`

   Tous les nœuds doivent être prêts :

```
Cluster       Node         Configuration Settings Status
----------    -----------  --------------------------------
cluster_A
              node_A_1     ready for interface create
              node_A_2     ready for interface create
cluster_B
              node_B_1     ready for interface create
              node_B_2     ready for interface create
4 entries were displayed.
```

3. Créer les interfaces sur node_A_1.

   a. Configurer l'interface sur le port "e5a" sur "node_A_1" :

N'utilisez pas d'adresses IP 169.254.17.x ou 169.254.18.x lorsque vous créez des interfaces IP MetroCluster pour éviter les conflits avec les adresses IP d'interface générées automatiquement par le système dans la même plage.

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5a" sur "node_A_1" avec l'adresse IP "10.1.1.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Sur les modèles de plateforme prenant en charge les VLAN pour l'interface IP MetroCluster, vous pouvez inclure le `-vlan-id` Paramètre si vous ne souhaitez pas utiliser les ID de VLAN par défaut. L'exemple suivant montre la commande pour un système AFF A220 avec un ID VLAN de 120 :

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configurer l'interface sur le port "e5b" sur "node_A_1" :

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5b" sur "node_A_1" avec l'adresse IP "10.1.2.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Vous pouvez vérifier que ces interfaces sont présentes à l'aide du `metrocluster configuration-settings interface show` commande.

4. Créer les interfaces sur node_A_2.

   a. Configurer l'interface sur le port « e5a » sur « node_A_2 » :

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      L'exemple suivant montre la création de l'interface sur le port "e5a" sur "node_A_2" avec l'adresse IP "10.1.1.2":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
      10.1.1.2 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

   b. Configurer l'interface sur le port « e5b » sur « node_A_2 » :

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
      -netmask <netmask>
      ```

      L'exemple suivant montre la création de l'interface sur le port "e5b" sur "node_A_2" avec l'adresse IP "10.1.2.2":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
      10.1.2.2 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

      Sur les modèles de plateforme prenant en charge les VLAN pour l'interface IP MetroCluster, vous pouvez inclure le `-vlan-id` Paramètre si vous ne souhaitez pas utiliser les ID de VLAN par défaut. L'exemple suivant montre la commande pour un système AFF A220 avec un ID VLAN de 220 :

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
      10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

5. Créer les interfaces sur « node_B_1 ».

   a. Configurer l'interface sur le port « e5a » sur « node_B_1 » :

      ```
      metrocluster configuration-settings interface create -cluster-name
      ```

```
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5a" sur "node_B_1" avec l'adresse IP "10.1.1.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5a -address
10.1.1.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

b. Configurer l'interface sur le port « e5b » sur « node_B_1 » :

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5b" sur "node_B_1" avec l'adresse IP "10.1.2.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Créer les interfaces sur « node_B_2 ».

a. Configurez l'interface sur le port e5a du nœud_B_2 :

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5a" sur "node_B_2" avec l'adresse IP "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configurer l'interface sur le port « e5b » sur « node_B_2 » :

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

L'exemple suivant montre la création de l'interface sur le port "e5b" sur "node_B_2" avec l'adresse IP "10.1.2.4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Vérifiez que les interfaces ont été configurées :

   `metrocluster configuration-settings interface show`

   L'exemple suivant montre que l'état de configuration de chaque interface est terminé.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                               Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- --------- ----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Vérifiez que les nœuds sont prêts à connecter les interfaces MetroCluster :

   `metrocluster configuration-settings show-status`

L'exemple suivant montre tous les nœuds avec l'état « prêt pour la connexion » :

```
Cluster       Node         Configuration Settings Status
----------    -----------  --------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Établir les connexions : `metrocluster configuration-settings connection connect`

   Si vous exécutez une version antérieure à ONTAP 9.10.1, les adresses IP ne peuvent pas être modifiées après l'exécution de cette commande.

   L'exemple suivant montre que cluster_A est connecté avec succès :

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Vérifier que les connexions ont été établies :

    `metrocluster configuration-settings show-status`

    L'état des paramètres de configuration de tous les nœuds doit être terminé :

```
Cluster       Node         Configuration Settings Status
----------    -----------  --------------------------------
cluster_A
              node_A_1     completed
              node_A_2     completed
cluster_B
              node_B_1     completed
              node_B_2     completed
4 entries were displayed.
```

11. Vérifiez que les connexions iSCSI ont été établies :

    a. Changement au niveau de privilège avancé :

       `set -privilege advanced`

       Vous devez répondre avec `y` lorsque vous êtes invité à passer en mode avancé, l'invite du mode

avancé s'affiche (*>).

b. Afficher les connexions :

```
storage iscsi-initiator show
```

Sur les systèmes exécutant ONTAP 9.5, il existe huit initiateurs IP MetroCluster sur chaque cluster qui doivent apparaître dans la sortie.

Sur les systèmes exécutant ONTAP 9.4 et versions antérieures, chaque cluster doit avoir quatre initiateurs IP MetroCluster qui doivent s'afficher dans la sortie.

L'exemple suivant montre les huit initiateurs IP MetroCluster sur un cluster exécutant ONTAP 9.5 :

```
cluster_A::*> storage iscsi-initiator show
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
--------------------------------- --------

cluster_A-01
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
               mccip-aux-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
               mccip-aux-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
               mccip-aux-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
               mccip-pri-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-pri-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-b-initiator2
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
```

```
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-aux-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-b-initiator2
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
     dr_partner
               mccip-pri-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
               mccip-pri-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
               mccip-pri-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
               mccip-pri-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

a. Retour au niveau de privilège admin :

```
set -privilege admin
```

12. Vérifier que les nœuds sont prêts pour une implémentation finale de la configuration MetroCluster :

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_A
              node_A_1          ready to configure -     -
              node_A_2          ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_B
              node_B_1           ready to configure -     -
              node_B_2           ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Vérification ou exécution manuelle de l'affectation des disques du pool 1

En fonction de la configuration du stockage, vous devez vérifier l'affectation des lecteurs du pool 1 ou attribuer manuellement les lecteurs au pool 1 pour chaque nœud de la configuration IP MetroCluster. La procédure que vous utilisez dépend de la version de ONTAP que vous utilisez.

Type de configuration	Procédure
Les systèmes répondent aux exigences d'affectation automatique des disques ou, s'ils exécutent ONTAP 9.3, ont été reçus en usine.	Vérification de l'affectation des disques du pool 1
La configuration inclut trois tiroirs ou, si elle contient plus de quatre tiroirs, présente un nombre irrégulier de quatre tiroirs (par exemple, sept tiroirs) et exécute ONTAP 9.5.	Affectation manuelle de lecteurs pour le pool 1 (ONTAP 9.4 ou version ultérieure)
La configuration n'inclut pas quatre tiroirs de stockage par site et exécute ONTAP 9.4	Affectation manuelle de lecteurs pour le pool 1 (ONTAP 9.4 ou version ultérieure)
Les systèmes n'ont pas été reçus en usine et exécutent ONTAP 9.3les systèmes reçus en usine sont préconfigurés avec les disques affectés.	Assignation manuelle de disques pour le pool 1 (ONTAP 9.3)

Vérification de l'affectation des disques du pool 1

Vous devez vérifier que les disques distants sont visibles pour les nœuds et qu'ils ont été correctement affectés.

Avant de commencer

Vous devez patienter au moins dix minutes que l'affectation automatique du disque se termine après la création des interfaces IP MetroCluster et des connexions avec le `metrocluster configuration-settings connection connect` commande.

La sortie de la commande affiche les noms des disques sous la forme : nom-nœud:0m.i1.0L1

"Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures"

Étapes

1. Vérifiez que les disques du pool 1 sont affectés automatiquement :

   ```
   disk show
   ```

   Le résultat suivant montre les valeurs de sortie d'un système AFF A800 sans tiroir externe.

   L'affectation automatique des disques a affecté un quart (8 disques) à « node_A_1 » et un quart à « node_A_2 ». Les disques restants seront des disques distants (pool 1) pour « node_B_1 » et « node_B_2 ».

   ```
   cluster_B::> disk show -host-adapter 0m -owner node_B_2
                        Usable     Disk              Container   Container
   Disk                 Size       Shelf Bay Type    Type        Name
   Owner
   ----------------     ---------- ----- --- ------- ----------- ---------
   --------
   node_B_2:0m.i0.2L4   894.0GB    0     29  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L3   894.0GB    0     28  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L9   894.0GB    0     24  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
   node_B_2
   8 entries were displayed.

   cluster_B::> disk show -host-adapter 0m -owner node_B_1
                        Usable     Disk              Container   Container
   Disk                 Size       Shelf Bay Type    Type        Name
   Owner
   ----------------     ---------- ----- --- ------- ----------- ---------
   --------
   node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
   node_B_1
   node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
   node_B_1
   node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
   node_B_1
   ```

```
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
```

```
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
```

```
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
```

```
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Affectation manuelle de lecteurs pour le pool 1 (ONTAP 9.4 ou version ultérieure)

Si le système n'a pas été préconfiguré en usine et ne répond pas aux exigences relatives à l'affectation automatique des lecteurs, vous devez affecter manuellement les lecteurs du pool distant 1.

Description de la tâche

Cette procédure s'applique aux configurations exécutant ONTAP 9.4 ou version ultérieure.

Vous trouverez des informations permettant de déterminer si votre système nécessite une affectation manuelle des disques dans le "Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures".

Lorsque la configuration inclut uniquement deux tiroirs externes par site, les pools 1 disques pour chaque site doivent être partagés depuis le même tiroir, comme illustré ci-dessous :

- Le nœud_A_1 est affecté aux disques dans les baies 0-11 du site_B-shelf_2 (à distance)
- Le node_A_2 est affecté aux disques dans les baies 12-23 sur site_B-shelf_2 (à distance)

Étapes

1. À partir de chaque nœud de la configuration IP MetroCluster, attribuez des disques distants au pool 1.

   a. Afficher la liste des disques non assignés :

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Affecter la propriété des lecteurs distants (0m) au pool 1 du premier nœud (par exemple, node_A_1) :

```
disk assign -disk <disk-id> -pool 1 -owner <owner_node_name>
```

`disk-id` vous devez identifier un lecteur sur un shelf distant de `owner_node_name`.

c. Vérifiez que les disques ont été affectés au pool 1 :

```
disk show -host-adapter 0m -container-type unassigned
```

> La connexion iSCSI utilisée pour accéder aux lecteurs distants apparaît comme périphérique 0m.

Le résultat suivant indique que les disques du tiroir 23 ont été affectés, car ils n'apparaissent plus dans la liste des disques non assignés :

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Répétez ces étapes pour affecter les lecteurs du pool 1 au second nœud du site A (par exemple, « node_A_2 »).

b. Répétez ces étapes sur le site B.

Assignation manuelle de disques pour le pool 1 (ONTAP 9.3)

Si vous avez au moins deux tiroirs disques pour chaque nœud, vous utilisez la fonctionnalité d'affectation automatique d'ONTAP pour attribuer automatiquement des disques distants (pool1).

Avant de commencer

Vous devez d'abord affecter un disque du tiroir au pool 1. ONTAP attribue ensuite automatiquement le reste des disques du tiroir au même pool.

Description de la tâche

Cette procédure s'applique aux configurations exécutant ONTAP 9.3.

Cette procédure ne peut être utilisée que si vous disposez d'au moins deux tiroirs disques pour chaque nœud, ce qui permet l'assignation automatique de disques au niveau des tiroirs.

Si vous ne pouvez pas utiliser l'affectation automatique au niveau du tiroir, vous devez attribuer manuellement les disques distants de sorte que chaque nœud dispose d'un pool de disques distant (pool 1).

La fonctionnalité d'affectation automatique de disques ONTAP attribue les disques selon le tiroir. Par exemple :

- Tous les disques du site_B-shelf_2 sont affectés automatiquement dans la pool1 du nœud_A_1
- Tous les disques du site_B-shelf_4 sont affectés automatiquement dans la pool1 du nœud_A_2
- Tous les disques du site_A-shelf_2 sont affectés automatiquement dans la pool1 du nœud_B_1
- Tous les disques du site_A-shelf_4 sont automatiquement affectés à la pool1 du nœud_B_2

Vous devez définir l'auto-assignation en spécifiant un seul disque sur chaque shelf.

Étapes

1. À partir de chaque nœud de la configuration IP MetroCluster, affectez un disque distant au pool 1.

   a. Afficher la liste des disques non assignés :

      `disk show -host-adapter 0m -container-type unassigned`

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

   b. Sélectionner un disque distant (0m) et attribuer la propriété du disque au pool 1 du premier nœud (par exemple, « node_A_1 ») :

      `disk assign -disk <disk_id> -pool 1 -owner <owner_node_name>`

      Le `disk-id` doit identifier un disque sur un shelf distant de `owner_node_name`.

      La fonction d'affectation automatique des disques ONTAP affecte tous les disques du tiroir distant qui contient le disque spécifié.

   c. Après avoir attendu au moins 60 secondes que l'affectation automatique du disque ait lieu, vérifiez que les disques distants du shelf ont été affectés automatiquement au pool 1 :

      `disk show -host-adapter 0m -container-type unassigned`

      > La connexion iSCSI utilisée pour accéder aux disques distants s'affiche en tant que périphérique 0m.

      Le résultat suivant indique que les disques du tiroir 23 ont été attribués et qu'ils ne sont plus visibles :

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Répétez ces étapes pour affecter les disques du pool 1 au second nœud du site A (par exemple, « node_A_2 »).

b. Répétez ces étapes sur le site B.

Activation de l'affectation automatique des disques dans ONTAP 9.4

Description de la tâche

Dans ONTAP 9.4, si vous avez désactivé l'affectation automatique des disques comme indiqué précédemment dans cette procédure, vous devez la réactiver sur tous les nœuds.

"Considérations relatives à l'affectation automatique des disques et aux systèmes ADP dans ONTAP 9.4 et versions ultérieures"

Étapes

1. Activer l'affectation automatique des disques :

   ```
   storage disk option modify -node <node_name> -autoassign on
   ```

   Vous devez exécuter cette commande sur tous les nœuds de la configuration IP MetroCluster.

Mise en miroir des agrégats racine

Pour assurer la protection des données, vous devez mettre en miroir les agrégats racine.

Description de la tâche

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 racine 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.

Informations associées

"Gestion du stockage logique"

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"

- Les noms des agrégats doivent être uniques sur l'ensemble des MetroCluster sites. Cela signifie que vous ne pouvez pas avoir deux agrégats différents portant le même nom sur le site A et le site B.

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
   - Si les disques à RPM différents sont autorisés pour plus d'informations sur ces options, consultez la page man de l'agrégat de stockage create.

     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>
```

Mise en œuvre de la configuration MetroCluster

Vous devez exécuter le `metrocluster configure` Commande pour démarrer la protection des données en configuration MetroCluster.

Description de la tâche

- Chaque cluster doit contenir au moins deux agrégats de données en miroir non racines.

  Vous pouvez le vérifier à l'aide du `storage aggregate show` commande.

  > Si vous souhaitez utiliser un seul agrégat de données en miroir, reportez-vous à la section Étape 1 pour obtenir des instructions.

- L'état ha-config des contrôleurs et du châssis doit être « mccip ».

Vous émettez le `metrocluster configure` Commandez une fois sur n'importe quel nœud pour activer la configuration MetroCluster. Vous n'avez pas besoin d'exécuter la commande sur chacun des sites ou nœuds, et ce n'est pas quel nœud ou site vous choisissez d'exécuter la commande.

Le `metrocluster configure` 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.

> Vous devez **pas** configurer Onboard Key Manager (OKM) ou la gestion externe des clés avant d'exécuter la commande `metrocluster configure`.

Étapes

1. configurer le MetroCluster au format suivant :

Si votre configuration MetroCluster possède…	Alors, procédez comme ça…
Plusieurs agrégats de données	Depuis n'importe quelle invite de nœud, configurer MetroCluster : `metrocluster configure <node_name>`

Un seul agrégat de données en miroir	a. Depuis l'invite de n'importe quel 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 que vous voyez l'invite du mode avancé (*>).
	
	b. Configurez le MetroCluster avec le `-allow -with-one-aggregate true` paramètre :
	
	`metrocluster configure -allow-with -one-aggregate true <node_name>`
	
	c. Retour au niveau de privilège admin :
	
	`set -privilege admin`

Il est recommandé d'avoir plusieurs agrégats de données. Si le premier groupe de reprise après incident ne dispose que d'un seul agrégat et que vous souhaitez ajouter un groupe de reprise après incident avec un seul agrégat, vous devez déplacer le volume de métadonnées depuis cet agrégat. Pour plus d'informations sur cette procédure, voir "Déplacement d'un volume de métadonnées dans les configurations MetroCluster".

La commande suivante permet d'activer la configuration MetroCluster sur tous les nœuds du groupe DR qui contient « Controller_A_1 » :

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

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

      Configuration: IP fabric

      Cluster                   Entry Name          State
      ------------------------- ------------------- -----------
       Local: cluster_A         Configuration state configured
                                Mode                normal
      Remote: cluster_B         Configuration state configured
                                Mode                normal
      ```

   b. 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
```

4. Pour éviter tout problème avec la mise en miroir de la mémoire non volatile, redémarrez chacun des quatre nœuds :

   `node reboot -node <node_name> -inhibit-takeover true`

5. Émettez le `metrocluster show` contrôlez les deux clusters pour vérifier à nouveau la configuration.

Configuration du second groupe de reprise sur incident dans une configuration à huit nœuds

Répétez les tâches précédentes pour configurer les nœuds dans le second groupe DR.

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

- Vérifiez que vous savez quels lecteurs 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 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. Activer le déploiement d'agrégats non mis en miroir :

   `metrocluster modify -enable-unmirrored-aggr-deployment true`

2. Vérifiez que l'autoassignation des disques est désactivée :

   ```
   disk option show
   ```

3. Installez et câisez les tiroirs disques qui contiennent les agrégats non mis en miroir.

   Vous pouvez utiliser les procédures décrites dans la documentation installation et configuration de la plateforme et des tiroirs disques.

   "Documentation des systèmes matériels ONTAP"

4. Attribuer manuellement tous les disques du nouveau shelf au nœud approprié :

   ```
   disk assign -disk <disk_id> -owner <owner_node_name>
   ```

5. 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, vous devez utiliser le paramètre -node ou spécifier les disques qui appartiennent à 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 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 pouvant être inclus dans un groupe RAID
   - Indique si les disques à régime différent sont autorisés

     Pour plus d'informations sur ces options, consultez la page man relative à la création d'agrégat de stockage.

     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
```

6. Vérifier le groupe RAID et les disques de votre nouvel agrégat :

   `storage aggregate show-status -aggregate <aggregate_name>`

7. Désactiver le déploiement d'agrégats non mis en miroir :

   `metrocluster modify -enable-unmirrored-aggr-deployment false`

8. Vérifiez que l'autoassignation des disques est activée :

   `disk option show`

Informations associées

"Gestion des disques et des agrégats"

Vérification de la configuration MetroCluster

Vous pouvez vérifier que les composants et les relations de la configuration MetroCluster fonctionnent correctement.

Description de la tâche

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.

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 des résultats plus détaillés à partir de la commande MetroCluster check run la plus récente :

   `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
```

```
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.

```
cluster_A::> metrocluster check cluster show

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.
```

Informations associées

"Gestion des disques et des agrégats"

"Gestion du réseau et des LIF"

Finalisation de la configuration ONTAP

Après la configuration, l'activation et la vérification de la configuration MetroCluster, vous pouvez terminer la configuration du cluster en ajoutant des SVM, des interfaces réseau et d'autres fonctionnalités ONTAP supplémentaires, si nécessaire.

Configurer le chiffrement de bout en bout dans une configuration MetroCluster IP

À partir d' ONTAP 9.15.1, vous pouvez configurer le chiffrement de bout en bout sur les systèmes pris en charge pour chiffrer le trafic back-end, tel que les données de réplication NVlog et de stockage, entre les sites d'une configuration IP MetroCluster .

Description de la tâche

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

- Avant de pouvoir configurer le chiffrement de bout en bout, vous devez "Configurez la gestion externe des clés".
- Vérifiez les systèmes pris en charge et la version minimale de ONTAP requise pour configurer le chiffrement de bout en bout dans une configuration MetroCluster IP :

Version minimale de ONTAP	Systèmes pris en charge
ONTAP 9.17.1	• AFF A800, AFF C800 • AFF A20, AFF A30, AFF C30, AFF A50, AFF C60 • AFF A70, AFF A90, AFF A1K, AFF C80 • FAS50, FAS70, FAS90
ONTAP 9.15.1	• AFF A400 • AFF C400 • FAS8300 • FAS8700

Chiffrez vos données de bout en bout

Procédez comme suit pour activer le chiffrement de bout en bout.

Étapes

1. Vérifier l'état de santé de la configuration MetroCluster.

   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` l'opération se termine, exécutez :

   ```
   metrocluster check show
   ```

   Après environ cinq minutes, les résultats suivants s'affichent :

```
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.
```

a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id <id>
```

b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Vérifier que la gestion externe des clés est configurée sur les deux clusters :

```
security key-manager external show-status
```

3. Chiffrement de bout en bout pour chaque groupe de reprise d'activité :

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Exemple

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Répétez cette étape pour chaque groupe DR de la configuration.

4. Vérifiez que le chiffrement de bout en bout est activé :

```
metrocluster node show -fields is-encryption-enabled
```

Exemple

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

Désactivez le chiffrement de bout en bout

Procédez comme suit pour désactiver le chiffrement de bout en bout.

Étapes

1. Vérifier l'état de santé de la configuration MetroCluster.

   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` l'opération se termine, exécutez :

   ```
   metrocluster check show
   ```

   Après environ cinq minutes, les résultats suivants s'affichent :

```
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.
```

a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id <id>
```

b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Vérifier que la gestion externe des clés est configurée sur les deux clusters :

```
security key-manager external show-status
```

3. Désactivez le chiffrement de bout en bout sur chaque groupe de reprise après incident :

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Exemple

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Répétez cette étape pour chaque groupe DR de la configuration.

4. Vérifiez que le chiffrement de bout en bout est désactivé :

```
metrocluster node show -fields is-encryption-enabled
```

Exemple

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Configurer MetroCluster Tiebreaker ou ONTAP Mediator pour une configuration IP MetroCluster

Vous pouvez télécharger et installer sur un troisième site le logiciel MetroCluster Tiebreaker ou, à partir de ONTAP 9.7, le médiateur ONTAP.

Avant de commencer

Vous devez disposer d'un hôte Linux disponible qui dispose d'une connectivité réseau aux deux clusters de la configuration MetroCluster. Les exigences spécifiques sont décrites dans la documentation du logiciel MetroCluster Tiebreaker ou du programme ONTAP Mediator.

Si vous vous connectez à une instance Tiebreaker ou ONTAP Mediator existante, vous avez besoin du nom d'utilisateur, du mot de passe et de l'adresse IP du Tiebreaker ou du Mediator.

Si vous devez installer une nouvelle instance du médiateur ONTAP, suivez les instructions pour installer et configurer le logiciel.

"Configurer ONTAP Mediator pour un basculement automatique non planifié"

Si vous devez installer une nouvelle instance du logiciel disjoncteur d'attache, suivez le "instructions d'installation et de configuration du logiciel".

Description de la tâche

Vous ne pouvez pas utiliser à la fois le logiciel MetroCluster Tiebreaker et le Mediator ONTAP avec la même configuration MetroCluster.

"Considérations relatives à l'utilisation du médiateur ONTAP ou d'un logiciel MetroCluster Tiebreaker"

Étape

1. Configurer ONTAP Mediator ou le logiciel Tiebreaker :
   - Si vous utilisez une instance existante d'ONTAP Mediator, ajoutez ONTAP Mediator à ONTAP :

     ```
     metrocluster configuration-settings mediator add -mediator-address ip-
     ```

```
address-of-mediator-host
```

- Si vous utilisez le logiciel disjoncteur d'attache, reportez-vous au "Documentation Tiebreaker".

Sauvegarder les fichiers de configuration du cluster dans une configuration IP MetroCluster

Vous pouvez fournir une protection supplémentaire pour les fichiers de sauvegarde de la configuration du cluster en spécifiant une URL distante (HTTP ou FTP) dans laquelle les fichiers de sauvegarde de configuration seront chargés en plus des emplacements par défaut dans le cluster local.

Étape

1. Définissez l'URL de la destination distante pour les fichiers de sauvegarde de configuration :

```
system configuration backup settings modify URL-of-destination
```

Le "Gestion du cluster via l'interface de ligne de commandes" Contient des informations supplémentaires sous la section *gestion des sauvegardes de configuration*.

Configurez le logiciel MetroCluster à l'aide de System Manager

Configurer un site IP MetroCluster avec ONTAP System Manager

Depuis la version ONTAP 9.8, vous pouvez utiliser System Manager pour configurer un site IP MetroCluster.

Un site MetroCluster se compose de deux clusters. En règle générale, les clusters se trouvent dans des emplacements géographiques différents.

Avant de commencer

- Votre système doit déjà être installé et câblé conformément à celui fourni avec le "Instructions d'installation et de configuration" système.
- Les interfaces réseau de clusters doivent être configurées sur chaque nœud de chaque cluster pour des communications intra-cluster.

Attribuez une adresse IP de gestion des nœuds

Système Windows

Vous devez connecter votre ordinateur Windows au même sous-réseau que les contrôleurs. Cette opération attribue automatiquement une adresse IP de gestion des nœuds à votre système.

Étapes

1. À partir du système Windows, ouvrez le lecteur **réseau** pour découvrir les nœuds.
2. Double-cliquez sur le nœud pour lancer l'assistant de configuration du cluster.

Autres systèmes

Vous devez configurer l'adresse IP node-management pour l'un des nœuds du cluster. Vous pouvez utiliser cette adresse IP node-management pour lancer l'assistant de configuration des clusters.

Pour plus d'informations sur l'attribution d'une adresse IP de gestion de nœuds, reportez-vous à la section"Création du cluster sur le premier node".

Initialiser et configurer le cluster

Vous initialisez le cluster en définissant un mot de passe administratif pour le cluster et en configurant les réseaux de gestion du cluster et de gestion des nœuds. Vous pouvez également configurer des services tels qu'un serveur de noms de domaine (DNS) pour résoudre les noms d'hôte et un serveur NTP pour synchroniser l'heure.

Étapes

1. Sur un navigateur Web, entrez l’adresse IP de gestion des nœuds que vous avez configurée : "https://node-management-IP"

   System Manager détecte automatiquement les nœuds restants dans le cluster.

2. Dans la fenêtre **Initialize Storage System**, effectuez les opérations suivantes :
   a. Saisissez les données de configuration du réseau de gestion du cluster.
   b. Entrez les adresses IP de gestion des nœuds pour tous les nœuds.
   c. Fournir les détails DNS.
   d. Dans la section **autre**, cochez la case **utiliser le service de temps (NTP)** pour ajouter les serveurs de temps.

Lorsque vous cliquez sur **Submit**, attendez que le cluster soit créé et configuré. Ensuite, un processus de validation a lieu.

Et la suite ?

Une fois que les deux clusters ont été configurés, initialisés et configurés, effectuez la "Configurer le peering IP MetroCluster" procédure.

Configurez ONTAP sur une nouvelle vidéo de cluster

Configurer le peering IP MetroCluster avec ONTAP System Manager

Depuis ONTAP 9.8, vous pouvez gérer les opérations de configuration IP de MetroCluster avec System Manager. Une fois que deux clusters sont configurés, vous configurez le peering entre eux.

Avant de commencer

Configurez deux clusters. Voir la "Configurez un site IP MetroCluster"procédure.

Différentes étapes sont réalisées par différents administrateurs système sur les sites géographiques de chaque cluster. Pour expliquer ce processus, les clusters sont appelés « grappe de sites A » et « grappe de sites B ».

Effectuez le processus de peering à partir du site A.

Ce processus est exécuté par un administrateur système sur le site A.

Étapes

1. Connectez-vous au site A cluster.
2. Dans System Manager, sélectionnez **Dashboard** dans la colonne de navigation de gauche pour afficher la vue d'ensemble du cluster.

   Le tableau de bord affiche les détails de ce cluster (site A). Dans la section **MetroCluster**, site Un cluster est affiché sur la gauche.

3. Cliquez sur **attacher le cluster partenaire**.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site A de communiquer avec les nœuds du cluster site B.

5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **joindre un cluster partenaire**, sélectionnez **Je n'ai pas de phrase de passe**. Ceci vous permet de générer une phrase de passe.
7. Copiez le mot de passe généré et partagez-le avec l'administrateur système du site B.
8. Sélectionnez **Fermer**.

Effectuez le processus de peering à partir du site B.

Ce processus est effectué par un administrateur système sur le site B.

Étapes

1. Connectez-vous au cluster site B.
2. Dans System Manager, sélectionnez **Dashboard** pour afficher la vue d'ensemble du cluster.

   Le tableau de bord affiche les détails de ce cluster (site B). Dans la section MetroCluster, le cluster du site B est indiqué sur la gauche.

3. Cliquez sur **Attach Partner Cluster** pour démarrer le processus de peering.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site B de communiquer avec les nœuds du cluster site A.
5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **joindre un cluster partenaire**, sélectionnez **J'ai une phrase de passe**. Vous pouvez ainsi saisir la phrase de passe que vous avez reçue de l'administrateur système du site A.
7. Sélectionnez **Peer** pour terminer le processus de peering.

Et la suite ?

Une fois le processus de peering terminé, vous configurez les clusters. Voir "Configurez un site IP MetroCluster".

Configurer un site IP MetroCluster avec ONTAP System Manager

Depuis ONTAP 9.8, vous pouvez gérer les opérations de configuration IP de MetroCluster avec System Manager. Cela implique la configuration de deux clusters, le peering de cluster et la configuration des clusters.

Avant de commencer

Effectuez les procédures suivantes :

- "Configurez un site IP MetroCluster"
- "Configurer le peering IP MetroCluster"

Configurer la connexion entre les clusters

Étapes

1. Connectez-vous à System Manager sur l'un des sites et sélectionnez **Dashboard**.

   Dans la section **MetroCluster**, le graphique montre les deux clusters que vous avez configurés et associés pour les sites MetroCluster. Le cluster depuis lequel vous travaillez (cluster local) s'affiche sur la gauche.

2. Cliquez sur **configurer MetroCluster**. Dans cette fenêtre, effectuez les opérations suivantes :
   a. Les nœuds de chaque cluster de la configuration MetroCluster sont affichés. Utilisez les listes déroulantes pour sélectionner les nœuds du cluster local qui seront associés à la reprise sur incident avec les nœuds du cluster distant.
   b. Cochez la case si vous souhaitez configurer ONTAP Mediator. Voir "Configurer ONTAP Mediator".
   c. Si les deux clusters disposent d'une licence pour activer le chiffrement, la section **Encryption** s'affiche.

      Pour activer le chiffrement, entrez une phrase de passe.

   d. Cochez la case si vous souhaitez configurer MetroCluster avec un réseau de couche 3 partagé.

      Les nœuds partenaires haute disponibilité et les commutateurs réseau qui se connectent aux nœuds doivent avoir une configuration correspondante.

3. Cliquez sur **Enregistrer** pour configurer les sites MetroCluster.

   Dans la section **MetroCluster** du **Tableau de bord**, le graphique montre une coche sur la liaison entre les deux grappes, indiquant une connexion saine.

Configurer ONTAP Mediator pour un basculement automatique non planifié

Exigences d'installation d'ONTAP Mediator pour les configurations IP MetroCluster

Votre environnement doit répondre à certaines exigences.

Les exigences suivantes s'appliquent à un seul groupe de reprise d'activité (DR Group). En savoir plus sur "Groupes de reprise sur incident".

- Si vous prévoyez de mettre à jour votre version Linux, faites-le avant d'installer la version la plus récente d'ONTAP Mediator.
- Les logiciels ONTAP Mediator et MetroCluster Tiebreaker ne doivent pas être utilisés tous les deux avec la même configuration MetroCluster.
- ONTAP Mediator doit être installé sur un hôte Linux à un emplacement distinct des sites MetroCluster.

  La connectivité entre le médiateur ONTAP et chaque site doit être composée de deux domaines de panne distincts.

- Le basculement non planifié automatique est pris en charge dans ONTAP 9.7 et versions ultérieures.
- À partir d' ONTAP 9.18.1 et ONTAP Mediator 1.11, une seule instance ONTAP Mediator peut gérer jusqu'à dix configurations MetroCluster simultanément. Dans les versions précédentes, ONTAP Mediator pouvait prendre en charge jusqu'à cinq configurations MetroCluster simultanément.
- À partir d' ONTAP 9.18.1, IPv6 est pris en charge pour ONTAP Mediator 1.11 ou ultérieur dans une configuration IP MetroCluster .

Configuration réseau requise pour l'utilisation d'ONTAP Mediator dans une configuration MetroCluster

Pour installer ONTAP Mediator dans une configuration MetroCluster, vous devez vous assurer que la configuration répond à plusieurs exigences réseau.

- Latence

  Latence maximale inférieure à 75 ms (RTT).

  La gigue ne doit pas dépasser 5 ms.

- MTU

  La taille de MTU doit être d'au moins 1400.

- Perte de paquets

  Pour le trafic ICMP (Internet Control message Protocol) et TCP, la perte de paquets doit être inférieure à 0.01 %.

- La bande passante

  Le lien entre ONTAP Mediator et un groupe DR doit avoir au moins 20 Mbps de bande passante.

- Connectivité indépendante

  Une connectivité indépendante entre chaque site et le médiateur ONTAP est requise. Une défaillance sur un site ne doit pas interrompre la connectivité IP entre les deux autres sites non affectés.

Exigences de l'hôte pour ONTAP Mediator dans une configuration MetroCluster

Vous devez vous assurer que la configuration répond à plusieurs exigences d'hôte.

- Le médiateur ONTAP doit être installé sur un site externe qui est physiquement séparé des deux clusters ONTAP.
- Le médiateur ONTAP ne nécessite pas plus que la configuration minimale requise par le système d'exploitation hôte pour le processeur et la mémoire (RAM).
- Outre les exigences minimales du système d'exploitation hôte, 30 Go d'espace disque utilisable supplémentaires doivent être disponibles.
  - Chaque groupe de reprise après incident nécessite jusqu'à 200 Mo d'espace disque.

Exigences relatives au pare-feu pour le médiateur ONTAP

ONTAP Mediator utilise un certain nombre de ports pour communiquer avec des services spécifiques.

Si vous utilisez un pare-feu tiers :

- L'accès HTTPS doit être activé.
- Il doit être configuré de manière à autoriser l'accès sur les ports 31784 et 3260.

  Lors de l'utilisation du pare-feu Red Hat ou CentOS par défaut, le pare-feu est automatiquement configuré lors de l'installation de Mediator.

Le tableau suivant répertorie les ports que vous devez autoriser dans votre pare-feu :

- Le port iSCSI n'est requis que dans une configuration IP MetroCluster.
- Le port 22/tcp n'est pas nécessaire pour un fonctionnement normal, mais vous pouvez l'activer temporairement pour la maintenance et le désactiver une fois la session de maintenance terminée.

Port/services	Source	Direction	Destination	Objectif
22/tcp	Hôte de gestion	Entrant	Médiateur de ONTAP	Gestion du médiateur SSH/ONTAP
31784/tcp	LIF de gestion de cluster et de gestion de nœud	Entrant	Serveur web du médiateur ONTAP	API REST (HTTPS)
3260/tcp	LIF de gestion des nœuds	Entrant	Cibles iSCSI du médiateur ONTAP	Connexion de données iSCSI pour les boîtes aux lettres

Directives pour la mise à niveau d'ONTAP Mediator dans une configuration MetroCluster

Si vous mettez à niveau ONTAP Mediator, vous devez respecter les exigences de version Linux et suivre les instructions pour la mise à niveau.

- ONTAP Mediator peut être mis à niveau d'une version immédiatement antérieure à la version actuelle.
- Toutes les versions de Mediator sont prises en charge sur les configurations IP de MetroCluster exécutant ONTAP 9.7 ou version ultérieure.

"Installer ou mettre à niveau ONTAP Mediator"

Après la mise à niveau

Une fois la mise à niveau du Mediator et du système d'exploitation terminée, vous devez émettre le `storage iscsi-initiator show` Commande pour confirmer que les connexions du médiateur sont en cours.

Configurer le médiateur ONTAP pour une configuration IP MetroCluster

Vous devez configurer le médiateur ONTAP sur le nœud ONTAP pour l'utiliser dans une configuration IP MetroCluster .

Avant de commencer

- ONTAP Mediator doit avoir été installé avec succès sur un emplacement réseau accessible par les deux sites MetroCluster.

  "Installer ou mettre à niveau ONTAP Mediator"

- Vous devez disposer de l'adresse IP de l'hôte exécutant ONTAP Mediator.
- Vous devez disposer du nom d'utilisateur et du mot de passe pour ONTAP Mediator.
- Tous les nœuds de la configuration IP de MetroCluster doivent être en ligne.

Depuis ONTAP 9.12.1, vous pouvez activer la fonctionnalité de basculement forcé automatique MetroCluster dans une configuration IP MetroCluster. Cette fonction est une extension du basculement non planifié assisté par un médiateur. Avant d'activer cette fonction, consultez le "Risques et limitations liés à l'utilisation du basculement automatique forcé de MetroCluster".

Description de la tâche

- Cette tâche permet le basculement automatique non planifié par défaut.
- Cette tâche peut être effectuée sur l'interface ONTAP de n'importe quel nœud de la configuration IP de MetroCluster.
- À partir d' ONTAP 9.18.1 et ONTAP Mediator 1.11, une seule instance ONTAP Mediator peut gérer jusqu'à dix configurations MetroCluster simultanément. Dans les versions précédentes, ONTAP Mediator pouvait prendre en charge jusqu'à cinq configurations MetroCluster simultanément.

Étapes

1. Ajouter ONTAP Mediator à ONTAP. Les étapes dépendent du type d'adresse que vous souhaitez utiliser : IPv4 ou IPv6.

   - Vous devez exécuter ONTAP 9.18.1 ou une version ultérieure et ONTAP Mediator 1.11 ou une version ultérieure pour utiliser IPv6.
   - Si vous activez IPv6 sur un cluster, vous ne pouvez pas le désactiver ultérieurement.

   Utiliser IPv4

   a. Exécutez la commande suivante pour ajouter le médiateur ONTAP :

   ```
   metrocluster configuration-settings mediator add -mediator-address
   <mediator_host_ip_address>
   ```

   Il vous est demandé de saisir le nom d'utilisateur et le mot de passe du compte utilisateur administrateur du médiateur.

   Utilisez IPv6

   a. Exécutez la commande suivante sur les deux clusters :

   ```
   network options ipv6 modify -enabled true
   ```

   b. Configurez l'adresse IP de gestion des nœuds avec des adresses IPv6 sur les quatre nœuds.

   c. Ajouter le médiateur ONTAP :

   ```
   metrocluster configuration-settings mediator add -mediator-address
   <mediator_host_ipv6_ip_address>
   ```

   Il vous est demandé de saisir le nom d'utilisateur et le mot de passe du compte utilisateur administrateur du médiateur.

2. Vérifiez que la fonction de basculement automatique est activée :

```
metrocluster show
```

3. Vérifiez que le médiateur est en cours d'exécution.

   a. Afficher les disques virtuels du médiateur :

   ```
   storage disk show -container-type mediator
   ```

   ```
    cluster_A::> storage disk show -container-type mediator
                           Usable           Disk    Container
   Container
    Disk                   Size Shelf Bay Type    Type        Name
   Owner
    ---------------- ---------- ----- --- ------- ----------- ---------
   --------
    NET-1.5                   -     -   - VMDISK  mediator    -
   node_A_2
    NET-1.6                   -     -   - VMDISK  mediator    -
   node_B_1
    NET-1.7                   -     -   - VMDISK  mediator    -
   node_B_2
    NET-1.8                   -     -   - VMDISK  mediator    -
   node_A_1
   ```

   b. Définissez le mode de privilège sur Avancé :

   ```
   set advanced
   ```

   ```
    cluster_A::> set advanced
   ```

   c. Afficher les initiateurs appelés médiateur :

   ```
   storage iscsi-initiator show -label mediator
   ```

```
 cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
--------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

d. Vérification de l'état du domaine de défaillance du basculement automatique non planifié (AUSO) :

`metrocluster show`

> L'exemple de sortie suivant s'applique à ONTAP 9.13.1 et versions ultérieures. Pour ONTAP 9.12.1 et les versions antérieures, l'état du domaine de défaillance AUSO doit être `auso-on-cluster-disaster`.

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

4. Vous pouvez également configurer le basculement automatique forcé de MetroCluster.

   Vous ne pouvez utiliser la commande suivante que dans un niveau de privilège avancé.

> Avant d'utiliser cette commande, consultez le "Risques et limitations liés à l'utilisation du basculement automatique forcé de MetroCluster".

`metrocluster modify -allow-auto-forced-switchover true`

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

Supprimer le médiateur ONTAP d'une configuration IP MetroCluster

Vous pouvez déconfigurer ONTAP Mediator à partir de la configuration IP MetroCluster.

Avant de commencer

Vous devez avoir installé et configuré avec succès ONTAP Mediator sur un emplacement réseau accessible par les deux sites MetroCluster.

Étapes

1. Annulez la configuration d'ONTAP Mediator à l'aide de la commande suivante :

   `metrocluster configuration-settings mediator remove`

   Vous êtes invité à entrer le nom d'utilisateur et le mot de passe du compte d'utilisateur admin du Mediator ONTAP.

   > Si le médiateur ONTAP est en panne, le `metrocluster configuration-settings mediator remove` La commande vous invite toujours à saisir le nom d'utilisateur et le mot de passe du compte d'utilisateur administrateur ONTAP Mediator et supprime ONTAP Mediator de la configuration MetroCluster.

   a. Vérifier s'il y a des disques cassés en utilisant la commande suivante :

      `disk show -broken`

      Exemple

```
There are no entries matching your query.
```

2. Confirmez que ONTAP Mediator a été supprimé de la configuration MetroCluster en exécutant les commandes suivantes sur les deux clusters :

   a. `metrocluster configuration-settings mediator show`

      Exemple

```
This table is currently empty.
```

   b. `storage iscsi-initiator show -label mediator`

      Exemple

```
There are no entries matching your query.
```

Connecter une configuration IP MetroCluster à une autre instance ONTAP Mediator

Si vous souhaitez connecter les nœuds MetroCluster à une autre instance de médiateur ONTAP, vous devez déconfigurer puis reconfigurer la connexion du médiateur dans le logiciel ONTAP.

Avant de commencer

Vous avez besoin du nom d'utilisateur, du mot de passe et de l'adresse IP de la nouvelle instance du médiateur ONTAP.

Description de la tâche

Ces commandes peuvent être émises depuis n'importe quel nœud de la configuration MetroCluster.

Étapes

1. Supprimez le médiateur ONTAP actuel de la configuration MetroCluster :

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Établissez la nouvelle connexion du médiateur ONTAP à la configuration MetroCluster :

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

Comment le médiateur ONTAP prend en charge le basculement automatique non planifié dans les configurations IP MetroCluster

ONTAP Mediator fournit des LUN de boîte aux lettres pour stocker les informations d'état des nœuds IP MetroCluster. Ces LUN sont colocalisés avec ONTAP Mediator, qui s'exécute sur un hôte Linux physiquement distinct des sites MetroCluster. Les nœuds IP MetroCluster peuvent utiliser les informations de la boîte aux lettres pour surveiller l'état de leurs partenaires de reprise après incident et mettre en œuvre un basculement non planifié assisté par Mediator (MAUSO) en cas d'incident.

La fonction MAUSO n'est pas prise en charge dans les configurations FC MetroCluster.

Lorsqu'un nœud détecte une défaillance de site nécessitant un basculement, il prend des mesures pour confirmer que le basculement est approprié et effectue le basculement. Par défaut, un MAUSO est lancé pour les scénarios suivants :

- La mise en miroir SyncMirror et la mise en miroir reprise après incident du cache non volatile de chaque nœud sont opérationnelles, et les caches et les miroirs sont synchronisés au moment de la panne.
- Aucun des nœuds du site survivant n'est en état de basculement.
- En cas d'incident sur site. Un incident de site est une défaillance de *tous* nœuds sur le même site.

Un MAUSO est *non* initié dans les scénarios d'arrêt suivants :

- Vous initiez un arrêt. Par exemple, lorsque vous :
  - Arrêtez les nœuds

◦ Redémarrez les nœuds

Découvrez les fonctionnalités MAUSO disponibles avec chaque version de ONTAP 9.

À commencer par…	Description
ONTAP 9.13.1	• Un MAUSO est lancé si un scénario par défaut se produit et une panne de ventilateur ou de matériel entraîne un arrêt de l'environnement. Une température élevée ou basse, une unité d'alimentation, une batterie NVRAM ou une défaillance de pulsation du processeur de service sont des exemples de pannes matérielles. • La valeur par défaut du domaine de défaillance est définie sur « auso-on-dr-group » dans une configuration IP MetroCluster. Pour ONTAP 9.12.1 et les versions antérieures, la valeur par défaut est « auso-on-cluster-Disaster ». Dans une configuration IP MetroCluster à huit nœuds, « auso-on-dr-group » déclenche une commande MAUSO en cas de panne du cluster ou d'une paire HA dans un groupe DR. Dans le cas d'une paire haute disponibilité, les deux nœuds doivent tomber en panne en même temps. Vous pouvez également remplacer le paramètre de domaine de défaillance par le domaine « auso-on-cluster-désastre » à l'aide du `metrocluster modify -auto -switchover-failure-domain auso-on-cluster-disaster` Commande permettant de déclencher une commande MAUSO uniquement en cas de défaillance d'une paire de nœuds HA dans les deux groupes DR. • Vous pouvez modifier le comportement pour forcer une MAUSO même si la NVRAM n'est pas synchronisée au moment de la panne.
ONTAP 9.12.1	Vous pouvez activer la fonction de basculement automatique forcé MetroCluster dans une configuration MetroCluster IP à l'aide de `metrocluster modify -allow-auto -forced-switchover true` commande. Le basculement en cas de détection d'une défaillance de site se produit automatiquement lorsque vous activez la fonctionnalité de basculement forcé automatique MetroCluster. Cette fonction peut être utilisée en complément de la fonctionnalité de basculement automatique MetroCluster IP. **Risques et limitations liés à l'utilisation du basculement automatique forcé de MetroCluster** Lorsque vous autorisez une configuration MetroCluster IP à fonctionner en mode de basculement forcé automatique, le problème connu suivant peut entraîner une perte de données : • La mémoire non volatile des contrôleurs de stockage n'est pas mise en miroir sur le partenaire de reprise après incident distant du site partenaire. **Attention** : vous pouvez rencontrer des scénarios qui ne sont pas mentionnés. NetApp n'est pas responsable de la corruption des données, de la perte de données ou des autres dommages susceptibles d'apparaître liés à l'activation de la fonction de basculement automatique forcé de MetroCluster. N'utilisez pas la fonctionnalité de basculement automatique forcé de MetroCluster si les risques et les limitations ne sont pas acceptables.

Gérer le médiateur ONTAP avec System Manager dans les configurations IP MetroCluster

À l'aide du Gestionnaire système, vous pouvez effectuer des tâches pour gérer ONTAP Mediator.

À propos de ces tâches

À partir de ONTAP 9.8, vous pouvez utiliser System Manager comme interface simplifiée pour gérer une configuration IP MetroCluster à quatre nœuds, qui peut inclure un médiateur ONTAP installé à un troisième emplacement.

Depuis ONTAP 9.14.1, vous pouvez utiliser System Manager pour effectuer ces opérations sur un site IP MetroCluster à huit nœuds. Bien que vous ne puissiez pas configurer ou développer un système à huit nœuds avec System Manager, si vous avez déjà configuré un système IP MetroCluster à huit nœuds, vous pouvez effectuer ces opérations.

Effectuez les tâches suivantes pour gérer ONTAP Mediator.

Pour effectuer cette tâche…	Prenez ces mesures…
Configurer ONTAP Mediator	Les deux clusters des sites MetroCluster doivent être up et associés. **Étapes** 1. Dans System Manager sous ONTAP 9.8, sélectionnez **Cluster > Paramètres**. 2. Dans la section **Mediator**, cliquez sur le ⚙. 3. Dans la fenêtre **Configure Mediator**, cliquez sur **Add+**. 4. Saisissez les détails de configuration pour ONTAP Mediator. Vous pouvez saisir les détails suivants lors de la configuration d'ONTAP Mediator avec System Manager. ◦ L'adresse IP d'ONTAP Mediator. ◦ Nom d'utilisateur. ◦ Le mot de passe.

Activer ou désactiver la commutation automatique assistée par Mediator (MAUSO)	**Étapes** 1. Dans System Manager, cliquez sur **Dashboard**. 2. Faites défiler jusqu'à la section MetroCluster. 3. Cliquez sur ⋮ en regard du nom du site MetroCluster. 4. Sélectionnez **Activer** ou **Désactiver**. 5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Activer** ou **Désactiver**. ⓘ Vous pouvez activer ou désactiver ONTAP Mediator lorsqu'il est accessible et que les deux sites sont en mode « Normal ». ONTAP Mediator reste accessible lorsque MAUSO est activé ou désactivé si le système MetroCluster est sain.
Supprimer ONTAP Mediator de la configuration MetroCluster	**Étapes** 1. Dans System Manager, cliquez sur **Dashboard**. 2. Faites défiler jusqu'à la section MetroCluster. 3. Cliquez sur ⋮ en regard du nom du site MetroCluster. 4. Sélectionnez **Supprimer le médiateur**. 5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Supprimer**.
Vérifiez l'état de santé d'ONTAP Mediator	Effectuez les étapes spécifiques à System Manager dans "Vérifiez l'état de santé d'une configuration MetroCluster".
Effectuer un basculement et un rétablissement	Effectuez les étapes de la section "Utilisez System Manager pour effectuer le basculement et le rétablissement (configurations MetroCluster IP uniquement)".

Testez le basculement du nœud ONTAP pour votre configuration IP MetroCluster

Vous pouvez tester les scénarios d'échec pour vérifier le bon fonctionnement de la configuration MetroCluster.

Vérification du basculement négocié

Vous pouvez tester le basculement négocié (planifié) pour confirmer la disponibilité ininterrompue des données.

Description de la tâche

Ce test valide que la disponibilité des données n'est pas affectée (à l'exception des protocoles SMB et Fibre Channel) par le basculement du cluster vers le deuxième centre de données.

Ce test devrait prendre environ 30 minutes.

Cette procédure présente les résultats attendus suivants :

- Le `metrocluster switchover` la commande affiche une invite d'avertissement.

  Si vous répondez `yes` à l'invite, le site dont la commande est émise bascule sur le site partenaire.

Pour les configurations MetroCluster IP :

- Pour ONTAP 9.4 et versions antérieures :
  - Les agrégats en miroir seront dégradés après le basculement négocié.
- Pour ONTAP 9.5 et versions ultérieures :
  - Les agrégats en miroir resteront dans un état normal en cas d'accès au stockage distant.
  - En cas de perte de l'accès au stockage distant, les agrégats en miroir sont dégradés après le basculement négocié.
- Pour ONTAP 9.8 et versions ultérieures :
  - En cas de perte de l'accès au stockage distant, les agrégats non mis en miroir qui se trouvent sur le site de reprise après incident deviennent indisponibles. Cela peut entraîner une panne du contrôleur.

Étapes

1. Vérifier que tous les nœuds sont en mode configuré et normal :

   `metrocluster node show`

   ```
   cluster_A::>  metrocluster node show

   Cluster                           Configuration State    Mode
   ------------------------------ ----------------------
   -------------------------
    Local: cluster_A                configured             normal
   Remote: cluster_B                configured             normal
   ```

2. Commencer l'opération de basculement :

   `metrocluster switchover`

   ```
   cluster_A::> metrocluster switchover
   Warning: negotiated switchover is about to start. It will stop all the
   data Vservers on cluster "cluster_B" and
   automatically re-start them on cluster "cluster_A". It will finally
   gracefully shutdown cluster "cluster_B".
   ```

3. Vérifier que le cluster local est en mode configuré et basculement :

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. Vérifier que l'opération de basculement a réussi :

   `metrocluster operation show`

```
cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Utilisez le `vserver show` et `network interface show` Les commandes qui permettent de vérifier que les SVM et les LIF de DR sont bien en ligne.

Vérification de la correction et du rétablissement manuel

Vous pouvez tester les opérations de rétablissement et de rétablissement manuel pour vérifier que la disponibilité des données n'est pas affectée (sauf dans le cas des configurations FC SMB et Solaris) en repassant le cluster au data Center d'origine après un basculement négocié.

Description de la tâche

Ce test devrait prendre environ 30 minutes.

Cette procédure devrait permettre de revenir aux nœuds de départ des services.

Les étapes de correction ne sont pas nécessaires sur les systèmes exécutant ONTAP 9.5 ou version ultérieure, sur lesquels la correction est automatiquement exécutée après un basculement négocié. Sur les systèmes exécutant ONTAP 9.6 et versions ultérieures, la correction est également effectuée automatiquement après un basculement non planifié.

Étapes

1. Si le système exécute ONTAP 9.4 ou une version antérieure, procédez à l'ajustement de l'agrégat de données :

   `metrocluster heal aggregates`

   L'exemple suivant montre la réussite de la commande :

```
cluster_A::> metrocluster heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. Si le système exécute ONTAP 9.4 ou une version antérieure, procédez à une correction de l'agrégat racine :

   `metrocluster heal root-aggregates`

   Cette étape est requise dans les configurations suivantes :

   - Configurations FC MetroCluster.
   - Les configurations IP de MetroCluster exécutant ONTAP 9.4 ou une version antérieure. L'exemple suivant montre la réussite de la commande :

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. Vérifiez que la correction est terminée :

   `metrocluster node show`

   L'exemple suivant montre la réussite de la commande :

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   heal roots
completed
      cluster_B
              node_B_2         unreachable    -         switched over
42 entries were displayed.
```

   Si l'opération de correction automatique échoue pour une raison quelconque, vous devez émettre le `metrocluster heal` Commandes manuelles comme effectuées dans les versions ONTAP antérieures à ONTAP 9.5. Vous pouvez utiliser le `metrocluster operation show` et `metrocluster operation history show -instance` commandes permettant de contrôler l'état de la correction et de déterminer la cause d'une défaillance.

4. Vérifier que tous les agrégats sont mis en miroir :

   `storage aggregate show`

   L'exemple suivant montre que tous les agrégats ont un statut RAID en miroir :

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

5. Vérifier l'état de la restauration en cas de rétablissement :

   `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   heal roots
completed
      cluster_B
            node_B_2            configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

6. Effectuez le rétablissement :

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

7. Confirmer l'état des nœuds :

```
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_2         configured     enabled   normal

2 entries were displayed.
```

8. Confirmer l'état de l'opération MetroCluster :

```
metrocluster operation show
```

Le résultat doit indiquer un état réussi.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Vérification du fonctionnement après une interruption de la ligne d'alimentation

Vous pouvez tester la réponse de la configuration MetroCluster à la défaillance d'une PDU.

Description de la tâche

Il est recommandé de connecter un composant à des blocs d'alimentation distincts. Si les deux blocs d'alimentation sont connectés à la même unité de distribution électrique et qu'une interruption électrique se produit, le site peut être en panne ou si un tiroir complet risque de ne plus être disponible. La défaillance d'une ligne d'alimentation est testée pour vérifier qu'il n'y a pas de défaut de câblage susceptible d'entraîner une interruption du service.

Ce test devrait prendre environ 15 minutes.

Ce test nécessite la mise hors tension de toutes les PDU de gauche, puis toutes les PDU de droite sur tous les racks contenant les composants MetroCluster.

Cette procédure présente les résultats attendus suivants :

- Les erreurs doivent être générées lorsque les PDU sont déconnectées.
- Aucun basculement ni perte de service ne doit se produire.

Étapes

1. Coupez l'alimentation des PDU situées sur le côté gauche du rack contenant les composants MetroCluster.
2. Surveiller le résultat sur la console :

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

   ```
   cluster_A::> system environment sensors show -state fault

   Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
   Crit-Hi
   ---- -------------------- ------ ----------- -------- -------- -------
   -------
   node_A_1
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   node_A_2
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   4 entries were displayed.

   cluster_A::> storage shelf show -errors
       Shelf Name: 1.1
        Shelf UID: 50:0a:09:80:03:6c:44:d5
    Serial Number: SHFHU1443000059

   Error Type          Description
   ------------------  ---------------------------
   Power               Critical condition is detected in storage shelf
   power supply unit "1". The unit might fail.Reconnect PSU1
   ```

3. Remettez l’alimentation en marche sur les unités de distribution d’alimentation de gauche.
4. Assurez-vous que ONTAP efface la condition d’erreur.
5. Répétez les étapes précédentes avec les PDU de droite.

Vérification de l’opération après la perte d’un tiroir de stockage

Vous pouvez tester la panne d’un tiroir de stockage pour vérifier qu’il n’y a pas de point de défaillance unique.

Description de la tâche

Cette procédure présente les résultats attendus suivants :

- Un message d’erreur doit être signalé par le logiciel de surveillance.
- Aucun basculement ni perte de service ne doit se produire.
- La resynchronisation du miroir démarre automatiquement après la restauration de la défaillance matérielle.

Étapes

1. Vérifier l’état du basculement du stockage :

   ```
   storage failover show
   ```

   ```
   cluster_A::> storage failover show

   Node           Partner        Possible State Description
   -------------- -------------- --------
   ------------------------------------
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Vérifier le statut de l’agrégat :

   ```
   storage aggregate show
   ```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Vérifier que tous les SVM et volumes de données sont en ligne et transfère les données :

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identifiez un tiroir dans le pool 1 pour le nœud « Node_A_2 » hors tension afin de simuler une panne matérielle soudaine :

`storage aggregate show -r -node node-name !*root`

Le tiroir que vous sélectionnez doit contenir des lecteurs faisant partie d'un agrégat de données en miroir.

Dans l'exemple suivant, l'ID de tiroir « 31 » est sélectionné pour échouer.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                      0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                      1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.3                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                      1   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     1.31.5                          1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                     0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Mettez physiquement hors tension la tablette que vous avez sélectionnée.
6. Vérifier à nouveau l'état de l'agrégat :

```
storage aggregate show

storage aggregate show -r -node node_A_2 !*root
```

L'agrégat avec disques du shelf hors tension doit avoir un état RAID « dégradé », et les disques du plex affecté doivent avoir un état en panne, comme illustré ci-dessous :

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,
```

```
mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.6                          0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                          0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                          0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                      -   -          -  827.7GB
-  (failed)
     parity   FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Vérifier que les données sont servies et que tous les volumes sont toujours en ligne :

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Mettez le shelf sous tension physique.

   La resynchronisation démarre automatiquement.

9. Vérifier que la resynchronisation a démarré :

   `storage aggregate show`

   L'agrégat affecté doit avoir l'état de « resynchronisation », comme l'illustre l'exemple suivant :

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. Surveiller l'agrégat pour vérifier que la resynchronisation est terminée :

    `storage aggregate show`

    L'agrégat affecté doit avoir un statut RAID « normal », comme illustré dans l'exemple suivant :

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Supprimer les configurations MetroCluster

Si vous devez supprimer la configuration MetroCluster, contactez le support technique.

Contactez le support technique NetApp et consultez le guide approprié pour votre configuration à partir de "Comment supprimer des nœuds d'une configuration MetroCluster - Guide de résolution."

Vous ne pouvez pas inverser la déconfiguration de MetroCluster. Ce processus ne doit être effectué qu'en collaboration avec le support technique. Après avoir supprimé la configuration MetroCluster, tous les paramètres de connectivité et d'interconnexion de disque doivent être ajustés pour qu'ils soient pris en charge.

Exigences et considérations pour les opérations ONTAP avec les configurations IP MetroCluster

Lorsque vous utilisez ONTAP dans une configuration MetroCluster, vous devez tenir compte de certaines considérations en matière de licence, de peering vers des clusters en dehors de la configuration MetroCluster, d'exécution des opérations de volume, des opérations NVFAIL et d'autres opérations ONTAP.

La configuration ONTAP des deux clusters, y compris la mise en réseau, doit être identique car la fonctionnalité MetroCluster repose sur la capacité d'un cluster à transmettre des données en toute transparence à son partenaire en cas de basculement.

Considérations relatives aux licences

- Les deux sites doivent bénéficier d'une licence pour les mêmes fonctionnalités du site.
- Tous les nœuds doivent être sous licence pour les mêmes fonctionnalités verrouillées par des nœuds.

Considération de SnapMirror

- La reprise après incident de SnapMirror sur les SVM n'est prise en charge que sur les configurations MetroCluster qui exécutent les versions de ONTAP 9.5 ou ultérieures.

Opérations MetroCluster dans ONTAP System Manager

Selon la version de votre ONTAP, certaines opérations propres à MetroCluster peuvent être effectuées à l'aide de ONTAP System Manager.

Pour en savoir plus, consultez le "Gérez des sites MetroCluster avec System Manager" documentation :

Prise en charge de FlexCache dans une configuration MetroCluster

Les volumes FlexCache sont pris en charge sur les configurations MetroCluster depuis ONTAP 9.7. Il est important de connaître les exigences relatives à la dépelage manuel après les opérations de basculement ou de rétablissement.

SVM abroge après le basculement lorsque l'origine et le cache FlexCache se trouvent sur le même site MetroCluster

Après un basculement négocié ou non planifié, toute relation de peering de SVM FlexCache au sein du cluster doit être configurée manuellement.

Par exemple, les SVM vs1 (cache) et vs2 (origine) se trouvent sur site_A. Ces SVM sont peering.

Après le basculement, les SVM vs1-mc et vs2-mc sont activés sur le site partenaire (site_B). Elles doivent être abrogés manuellement pour que FlexCache fonctionne à l'aide de la commande vserver peer broder.

SVM abroge après le basculement ou le rétablissement lorsqu'une destination FlexCache se trouve sur un troisième cluster et en mode déconnecté

Pour les relations FlexCache sur un cluster en dehors de la configuration MetroCluster, le peering doit toujours être reconfiguré manuellement après un basculement si les clusters concernés sont en mode déconnecté lors du basculement.

Par exemple :

- L'une des extrémités du FlexCache (cache_1 sur vs1) réside sur MetroCluster site_A possède une extrémité du FlexCache
- L'autre extrémité du FlexCache (origine_1 sur vs2) se trouve sur site_C (pas dans la configuration MetroCluster)

Lorsque le basculement est déclenché et si site_A et site_C ne sont pas connectés, vous devez peamer manuellement les SVM sur site_B (le cluster de basculement) et site_C à l'aide de la commande vserver peer depeer après le basculement.

Lorsque le rétablissement s'effectue, vous devez à nouveau abroger les SVM du site_A (le cluster d'origine) et du site_C.

Informations associées

"Gestion des volumes FlexCache via l'interface de ligne de commandes"

Prise en charge de FabricPool dans les configurations MetroCluster

Depuis ONTAP 9.7, les configurations MetroCluster prennent en charge les niveaux de stockage FabricPool.

Pour des informations générales sur l'utilisation de FabricPool, voir "Gestion des disques et des niveaux (agrégat)".

Considérations à prendre en compte lors de l'utilisation de FabricPool

- Les clusters doivent disposer de licences FabricPool correspondant aux limites de capacité.
- Les clusters doivent disposer d'IPspaces avec des noms correspondant.

  Il peut s'agir de l'IPspace par défaut, ou un espace IP qu'un administrateur a créé. Cet IPspace sera utilisé pour les configurations de magasin d'objets FabricPool.

- Pour l'IPspace sélectionné, chaque cluster doit avoir une LIF intercluster définie qui peut atteindre le magasin d'objets externe.
- La migration des SVM n'est pas prise en charge avec FabricPool lorsque la source ou la destination est un cluster MetroCluster.

  "En savoir plus sur la mobilité des données des SVM".

Configuration d'un agrégat à utiliser dans une FabricPool en miroir

Avant de configurer l'agrégat, vous devez configurer des magasins d'objets comme décrit dans la section « Configuration des magasins d'objets pour FabricPool dans une configuration MetroCluster » du "Gestion des disques et des agrégats".

Étapes

Pour configurer un agrégat afin de l'utiliser dans une FabricPool :

1. Création de l'agrégat ou sélection d'un agrégat existant.
2. Mettre en miroir l'agrégat en tant qu'agrégat en miroir standard au sein de la configuration MetroCluster.
3. Créer le miroir FabricPool avec l'agrégat, comme décrit à la "Gestion des disques et des agrégats"
   a. Attacher un magasin d'objets primaire.

      Ce magasin d'objets est physiquement plus proche du cluster.

   b. Ajouter un magasin d'objets symétriques.

      Ce magasin d'objets est physiquement plus éloigné du cluster que le magasin d'objets primaire.

Prise en charge de FlexGroup dans les configurations MetroCluster

Depuis la version ONTAP 9.6, les configurations MetroCluster prennent en charge les volumes FlexGroup.

Planifications de travaux dans une configuration MetroCluster

Dans ONTAP 9.3 et les versions ultérieures, la planification des tâches créées par l'utilisateur est automatiquement répliquée entre les clusters dans une configuration MetroCluster. Si vous créez, modifiez ou supprimez un programme de travaux sur un cluster, le même programme est automatiquement créé sur le cluster partenaire à l'aide du service de réplication de configuration (CRS).

Les planifications créées par le système ne sont pas répliquées et vous devez effectuer manuellement la même opération sur le cluster partenaire afin que les planifications de tâches sur les deux clusters soient identiques.

Peering de cluster depuis le site de MetroCluster vers un troisième cluster

Étant donné que la configuration de peering n'est pas répliquée, si vous peer l'un des clusters de la configuration MetroCluster sur un troisième cluster en dehors de cette configuration, vous devez également configurer le peering sur le cluster partenaire MetroCluster. Cela permet de maintenir le peering en cas de basculement.

Le cluster non MetroCluster doit exécuter ONTAP 8.3 ou une version ultérieure. Si ce n'est pas le cas, le peering est perdu en cas de basculement, même si le peering a été configuré sur les deux partenaires de MetroCluster.

Réplication de la configuration du client LDAP dans une configuration MetroCluster

Une configuration client LDAP créée sur un SVM (Storage Virtual machine) sur un cluster local est répliquée vers son SVM de données partenaire sur le cluster distant. Par exemple, si la configuration client LDAP est créée sur le SVM d'administration au sein du cluster local, il est répliqué sur tous les SVM de données d'administration au sein du cluster distant. Cette fonctionnalité de MetroCluster est intentionnelle, ce qui signifie que la configuration du client LDAP est active sur tous les SVM partenaires du cluster distant.

Instructions de création de LIF et de mise en réseau pour les configurations MetroCluster

Il est important de savoir comment les LIF sont créées et répliquées dans une configuration MetroCluster. Vous devez également connaître l'exigence de cohérence afin de pouvoir prendre les bonnes décisions lors de la configuration de votre réseau.

Informations associées

"Gestion du réseau et des LIF"

"Exigences de configuration de sous-réseau et de réplication d'objets IPspace"

"Conditions requises pour la création de LIF dans une configuration MetroCluster"

"Exigences et problèmes de réplication et de placement de LIF"

Exigences de configuration de sous-réseau et de réplication d'objets IPspace

Il est important de connaître les exigences relatives à la réplication d'objets IPspace vers le cluster partenaire et à la configuration des sous-réseaux et IPv6 dans une configuration MetroCluster.

Réplication IPspace

Lors de la réplication d'objets IPspace vers le cluster partenaire, vous devez prendre en compte les instructions suivantes :

- Les noms IPspace des deux sites doivent correspondre.
- Les objets IPspace doivent être répliqués manuellement sur le cluster partenaire.

  Toute machine virtuelle de stockage (SVM) créée et attribuée à un IPspace avant la réplication de l'IPspace ne sera pas répliquée au cluster partenaire.

Configuration de sous-réseau

Lors de la configuration des sous-réseaux dans une configuration MetroCluster, vous devez tenir compte des consignes suivantes :

- Les deux clusters de la configuration MetroCluster doivent avoir un sous-réseau dans le même IPspace avec le même nom de sous-réseau, sous-réseau, domaine de diffusion et passerelle.
- La plage IP des deux clusters doit être différente.

  Dans l'exemple suivant, les plages IP sont différentes :

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------       -------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      --------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.21-192.168.2.30
```

Configuration IPv6

Si IPv6 est configuré sur un site, IPv6 doit également être configuré sur l'autre site.

Informations associées

"Conditions requises pour la création de LIF dans une configuration MetroCluster"

"Exigences et problèmes de réplication et de placement de LIF"

Conditions requises pour la création de LIF dans une configuration MetroCluster

Lors de la configuration du réseau dans une configuration MetroCluster, il est important de connaître les conditions requises pour la création des LIFs.

Lors de la création de LIF, vous devez tenir compte des consignes suivantes :

- Fibre Channel : vous devez utiliser des VSAN étirés ou des fabrics étirés
- IP/iSCSI : vous devez utiliser un réseau étendu de couche 2
- Diffusions ARP : vous devez activer les diffusions ARP entre les deux clusters
- Dupliquer les LIF : vous ne devez pas créer plusieurs LIF avec la même adresse IP (LIFs dupliquées) dans un IPspace
- Configurations NFS et SAN : vous devez utiliser différents SVM pour les agrégats sans miroir et en miroir
- Avant de créer une LIF, vous devez créer un objet de sous-réseau. Un objet de sous-réseau permet à ONTAP de déterminer les cibles de basculement sur le cluster de destination, car il possède un broadcast domain associé.

Vérifier la création de LIF

Vous pouvez confirmer le succès de la création d'une LIF dans une configuration MetroCluster en exécutant la commande MetroCluster check lif show. Si vous rencontrez des problèmes lors de la création du LIF, vous pouvez utiliser la commande MetroCluster check lif repair-placement pour résoudre le problème.

Informations associées

"Exigences de configuration de sous-réseau et de réplication d'objets IPspace"

"Exigences et problèmes de réplication et de placement de LIF"

Exigences et problèmes de réplication et de placement de LIF

Il est important de connaître les exigences de réplication de la LIF dans une configuration MetroCluster. Vous devez également savoir comment placer une LIF répliquée sur un cluster partenaire, et vous devez connaître les problèmes qui se produisent en cas de défaillance de la réplication LIF ou du placement de LIF.

Réplication des LIFs vers le cluster partenaire

Lorsque vous créez une LIF sur un cluster dans une configuration MetroCluster, celle-ci est répliquée sur le cluster partenaire. Les LIF ne sont pas placées sous un nom unique. Pour assurer la disponibilité des LIF après une opération de basculement, le processus de placement de la LIF vérifie que les ports peuvent héberger les LIF en fonction des vérifications d'attributs de port et de accessibilité.

Le système doit remplir les conditions suivantes pour placer les LIF répliquées sur le cluster partenaire :

Condition	Type de LIF : FC	Type de LIF : IP/iSCSI
Identification du nœud	ONTAP tente de placer la LIF répliquée sur le partenaire de reprise après incident du nœud sur lequel elle a été créée. Si le partenaire DR n'est pas disponible, le partenaire auxiliaire DR est utilisé pour le placement.	ONTAP tente de placer la LIF répliquée sur le partenaire de reprise après incident du nœud sur lequel elle a été créée. Si le partenaire DR n'est pas disponible, le partenaire auxiliaire DR est utilisé pour le placement.
Identification des ports	ONTAP identifie les ports FC target connectés sur le cluster DR.	Les ports du cluster DR qui se trouvent dans le même IPspace que la LIF source sont sélectionnés pour une vérification de la capacité.si aucun port n'est présent dans le cluster DR dans le même IPspace, la LIF ne peut pas être placée. Tous les ports du cluster DR qui hébergent déjà une LIF dans le même IPspace et le même sous-réseau sont automatiquement marqués comme accessibles ; et peuvent être utilisés pour le placement. Ces ports ne sont pas inclus dans le contrôle de la capacité d'accessibilité.

Vérification de l'accessibilité	L'accessibilité est déterminée en vérifiant la connectivité du WWN de la structure source sur les ports du cluster DR.si la même structure n'est pas présente sur le site de reprise après incident, la LIF est placée sur un port aléatoire sur le partenaire de reprise après incident.	La réaccessibilité est déterminée par la réponse à un protocole ARP (Address Resolution Protocol) diffusé de chaque port précédemment identifié sur le cluster DR à l'adresse IP source de la LIF à placer.pour que les contrôles de réaccessibilité réussissent, les diffusions ARP doivent être autorisées entre les deux clusters. Chaque port qui reçoit une réponse de la LIF source sera marqué comme possible pour le placement.
Sélection de port	ONTAP catégorise les ports d'après des attributs tels que le type d'adaptateur et la vitesse, puis sélectionne les ports avec des attributs correspondants.si aucun port ne correspond à des attributs, la LIF est placée sur un port connecté au hasard dans le partenaire de DR.	Depuis les ports marqués comme accessibles pendant la vérification de la capacité d'accessibilité, ONTAP préfère les ports qui sont situés dans le broadcast domain associé au sous-réseau de la LIF.si aucun port réseau n'est disponible sur le cluster DR qui sont dans le broadcast domain associé au sous-réseau de la LIF, Ensuite, ONTAP sélectionne les ports qui ont réachcapacité vers le LIF source. Si aucun port n'est capable de reachpuisse la LIF source, un port est sélectionné dans le broadcast domain associé au sous-réseau de la LIF source, et s'il n'existe aucun tel broadcast domain, un port aléatoire est sélectionné. ONTAP catégorise les ports en fonction d'attributs tels que le type d'adaptateur, le type d'interface et la vitesse, puis sélectionne les ports avec des attributs correspondants.
Placement de LIF	Dans les ports accessibles, ONTAP sélectionne le port le moins chargé pour le placement.	Dans les ports sélectionnés, ONTAP sélectionne le port le moins chargé pour le placement.

Placement des LIF répliquées lorsque le nœud partenaire de DR est en panne

Lorsqu'une LIF iSCSI ou FC est créée sur un nœud dont le partenaire de reprise après incident est repris, elle est placée sur le nœud partenaire auxiliaire de reprise après incident. Après une opération de rétablissement ultérieure, les LIF ne sont pas automatiquement déplacées vers le partenaire de reprise après incident. Cela peut entraîner une concentration des LIF sur un seul nœud du cluster partenaire. Lors d'une opération de basculement MetroCluster, les tentatives suivantes de mappage de LUN appartenant à la machine virtuelle de stockage (SVM) échouent.

Vous devez exécuter le `metrocluster check lif show` Commande après une opération de basculement ou de rétablissement pour vérifier que le placement de LIF est correct. Si des erreurs existent, vous pouvez exécuter le `metrocluster check lif repair-placement` commande pour résoudre les problèmes.

Erreurs de placement de LIF

Erreurs de placement de LIF affichées par le `metrocluster check lif show` la commande est conservée après une opération de basculement. Si le `network interface modify`, `network interface rename`, ou `network interface delete` La commande est émise pour une LIF avec une erreur de placement, l'erreur est supprimée et n'apparaît pas dans la sortie du `metrocluster check lif show` commande.

Échec de réplication de LIF

Vous pouvez également vérifier si la réplication LIF a réussi à l'aide de `metrocluster check lif show` commande. Un message EMS est affiché en cas d'échec de la réplication de la LIF.

Vous pouvez corriger un échec de réplication en exécutant le `metrocluster check lif repair-placement` Commande de tout LIF qui ne parvient pas à trouver le port correct. Vous devez résoudre toutes les défaillances liées à la réplication de la LIF dès que possible afin de vérifier la disponibilité de cette LIF lors d'une opération de basculement de la MetroCluster.

> Même si le SVM source est en panne, le placement de la LIF peut se poursuivre normalement si une LIF appartient à un autre SVM dans un port avec le même IPspace et le même réseau dans le SVM de destination.

Informations associées

"Exigences de configuration de sous-réseau et de réplication d'objets IPspace"

"Conditions requises pour la création de LIF dans une configuration MetroCluster"

Création du volume sur un agrégat root

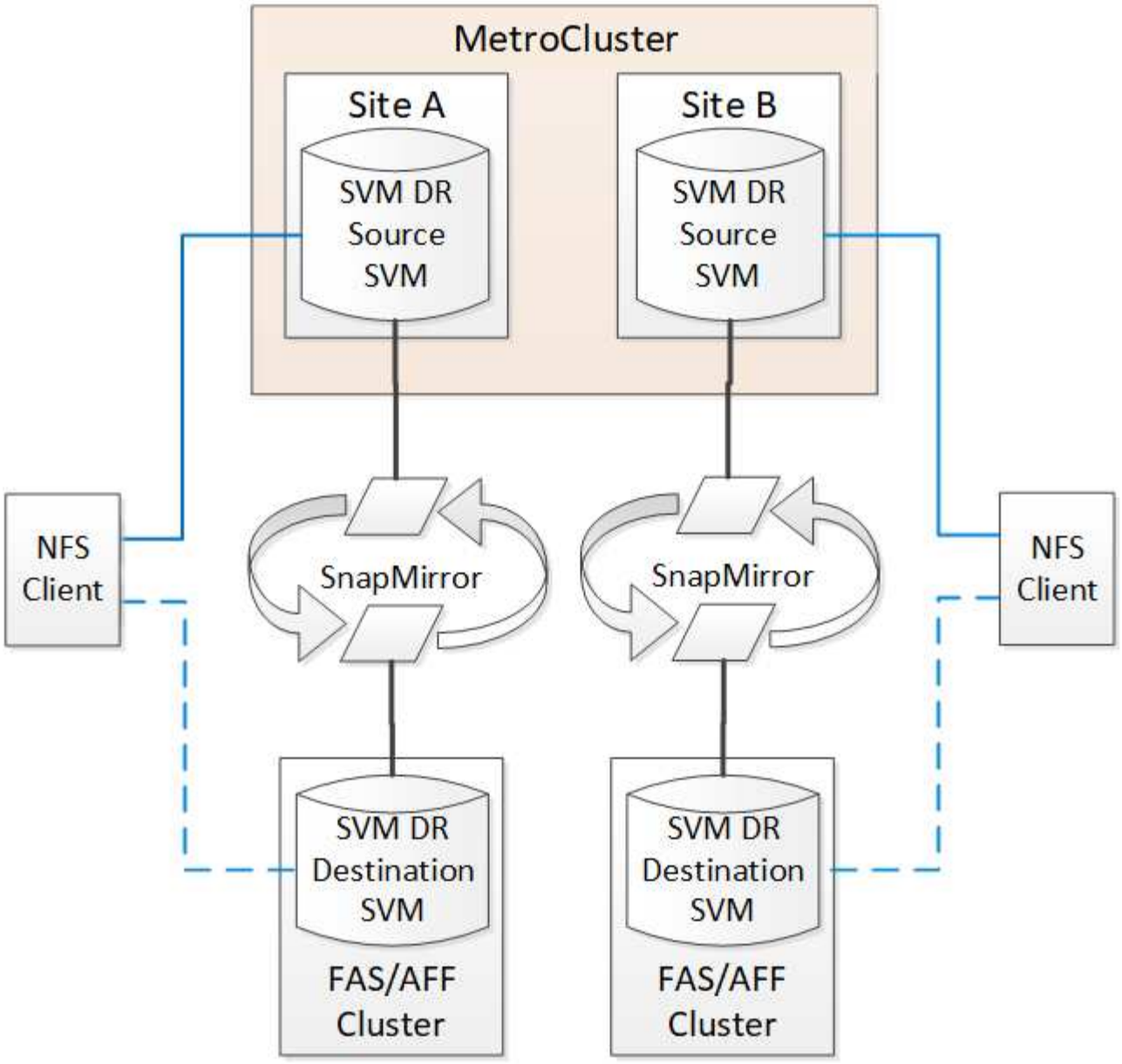
Le système n'autorise pas la création de nouveaux volumes sur l'agrégat racine (un agrégat avec une politique de haute disponibilité de CFO) d'un nœud d'une configuration MetroCluster.

Du fait de cette restriction, les agrégats root ne peuvent pas être ajoutés à un SVM via le `vserver add-aggregates` commande.

Reprise après incident de SVM dans une configuration MetroCluster

Depuis ONTAP 9.5, des serveurs virtuels de stockage actifs dans une configuration MetroCluster peuvent être utilisés en tant que sources au sein de la fonctionnalité de reprise après incident de SVM SnapMirror. Le SVM destination doit être sur le troisième cluster en dehors de la configuration MetroCluster.

Depuis ONTAP 9.11.1, les deux sites d'une configuration MetroCluster peuvent être à la source d'une relation SVM DR avec un cluster FAS ou AFF de destination, comme illustré dans l'image suivante.



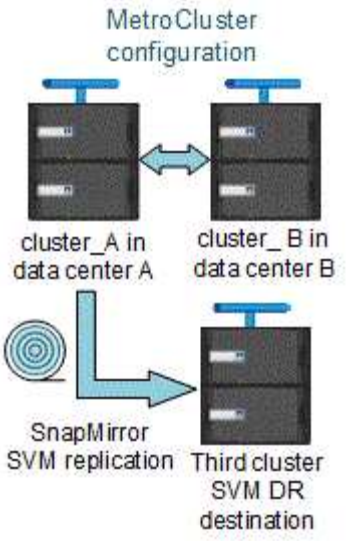
La reprise sur incident SnapMirror doit être consciente des exigences et limitations suivantes, liées à l'utilisation de SVM :

- Seul un SVM actif au sein d'une configuration MetroCluster peut être à l'origine d'une relation de reprise d'activité de SVM.

  Une source peut être un SVM source synchrone avant le basculement ou un SVM de destination synchrone après le basculement.

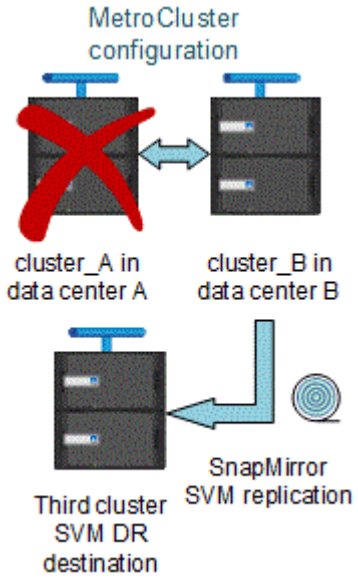
- Lorsqu'une configuration MetroCluster est dans un état stable, le SVM MetroCluster destination ne peut pas être à l'origine d'une relation de reprise d'activité SVM, car les volumes ne sont pas en ligne.

  L'image suivante montre le comportement de reprise après incident du SVM dans un état stable :



- Lorsque le SVM source synchrone est la source d'une relation de SVM DR, les informations de la relation de SVM DR source sont répliquées vers le partenaire MetroCluster.

  Les mises à jour de reprise après incident du SVM peuvent ainsi se poursuivre après un basculement, comme illustré dans l'image suivante :



- Lors des processus de basculement et de rétablissement, la réplication vers la destination SVM DR peut échouer.

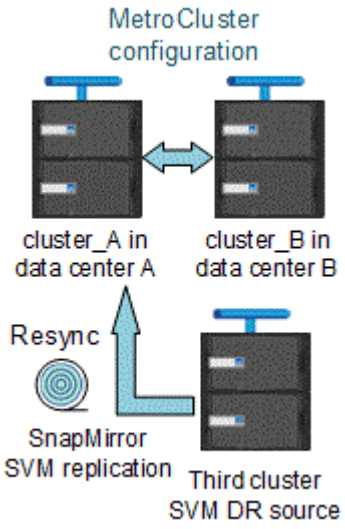
  Toutefois, une fois le processus de basculement ou de rétablissement terminé, les mises à jour planifiées de reprise sur incident du SVM suivantes seront appliquées.

Voir « réplication de la configuration SVM » dans "Protection des données" Pour plus d'informations sur la configuration d'une relation de SVM DR.

Resynchronisation des SVM au niveau d'un site de reprise d'activité

Pendant la resynchronisation, la source de reprise d'activité des machines virtuelles de stockage (SVM) sur la configuration MetroCluster est restaurée à partir du SVM de destination sur le site non MetroCluster.

Pendant la resynchronisation, le SVM source (cluster_A) agit temporairement comme un SVM de destination, comme illustré dans l'image suivante :



En cas de basculement non planifié lors de la resynchronisation

Les mélangeurs non planifiés qui se produisent pendant la resynchronisation stoppent le transfert de resynchronisation. En cas de basculement non planifié, les conditions suivantes sont vraies :

- Le SVM de destination sur le site MetroCluster (qui était un SVM source avant resynchronisation) reste comme un SVM de destination. Le SVM au cluster partenaire continuera de conserver son sous-type et reste inactif.
- La relation SnapMirror doit être recrécréée manuellement avec la SVM de destination du système Sync.
- La relation SnapMirror n'apparaît pas dans le résultat SnapMirror après un basculement sur le site survivant sauf si une opération SnapMirror create est exécutée.

Rétablissement après un basculement non planifié lors de la resynchronisation

Pour réussir le processus de rétablissement, la relation de resynchronisation doit être interrompue et supprimée. Le rétablissement n'est pas autorisé en cas de SVM de destination SnapMirror DR dans la configuration MetroCluster ou si le cluster dispose d'un SVM de sous-type « `dp-destination' ».

Le résultat de la commande plex show de l'agrégat de stockage est indéterminé après un basculement de MetroCluster

Lorsque vous exécutez la commande Storage agmoyen plex show après un basculement de MetroCluster, l'état du plex0 de l'agrégat racine commuté est indéterminé et s'affiche comme ayant échoué. Pendant ce temps, la racine de commutation n'est pas mise à jour. L'état réel de ce plex ne peut être déterminé qu'après la phase de guérison MetroCluster.

Modification des volumes pour définir l'indicateur NVFAIL en cas de basculement

Vous pouvez modifier un volume de sorte que l'indicateur NVFAIL soit défini sur le volume en cas de basculement MetroCluster. L'indicateur NVFAIL empêche le volume d'être clôturé de toute modification. Cela est nécessaire pour les volumes qui doivent être traités comme si des écritures validées sur le volume étaient perdues après le basculement.

Dans les versions ONTAP antérieures à 9.0, l'indicateur NVFAIL est utilisé pour chaque basculement. Dans ONTAP 9.0 et versions ultérieures, le basculement non planifié (USO) est utilisé.

Étape

1. Activez la configuration MetroCluster pour déclencher NVFAIL lors du basculement en réglant le `vol -dr -force-nvfail` paramètre sur on :

```
vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
```

Comment utiliser Active IQ Unified Manager et ONTAP System Manager pour obtenir des informations supplémentaires sur la configuration et le contrôle

Utilisez Active IQ Unified Manager et ONTAP System Manager pour une configuration et une surveillance supplémentaires dans une configuration IP MetroCluster

Active IQ Unified Manager et ONTAP System Manager peuvent être utilisés pour la gestion des clusters à partir d'une interface graphique et pour le contrôle de la configuration.

Chaque nœud est préinstallé par ONTAP System Manager. Pour charger System Manager, entrez l'adresse LIF de gestion du cluster en tant qu'URL dans un navigateur Web qui dispose d'une connexion au nœud.

Vous pouvez également utiliser Active IQ Unified Manager pour surveiller la configuration de MetroCluster.

Informations associées

"Documentation Active IQ Unified Manager"

Synchroniser l'heure système à l'aide de NTP dans une configuration IP MetroCluster

Chaque cluster a besoin de son propre serveur NTP (Network Time Protocol) pour synchroniser l'heure entre les nœuds et leurs clients.

Description de la tâche

- Vous ne pouvez pas modifier les paramètres du fuseau horaire d'un nœud défaillant ou du nœud partenaire après un basculement.
- Chaque cluster de configuration MetroCluster IP doit disposer de son propre serveur NTP ou de ses propres serveurs utilisés par les nœuds et les commutateurs IP sur ce site MetroCluster.
- Si vous utilisez le Tiebreaker MetroCluster ou le Mediator ONTAP, il doit également disposer de son propre serveur NTP.
- Cette procédure montre comment configurer le protocole NTP après avoir déjà configuré les clusters IP MetroCluster. Si vous avez utilisé System Manager pour configurer les clusters, vous devez déjà avoir configuré les serveurs NTP dans le cadre du programme de configuration du cluster. Voir "Configurez un site IP MetroCluster" pour plus de détails.

Selon votre version de ONTAP, vous pouvez configurer le NTP à partir de l'onglet **Cluster** ou **Insights** de l'interface utilisateur du Gestionnaire système.

Cluster

Dans le Gestionnaire système, vous pouvez configurer le protocole NTP à partir de l'onglet **Cluster** en utilisant deux options différentes, selon votre version de ONTAP :

ONTAP 9.8 ou version ultérieure :

Procédez comme suit pour synchroniser le NTP à partir de l'onglet **Cluster** de ONTAP 9.8 ou version ultérieure.

Étapes

1. Accédez à **Cluster > Présentation**
2. Sélectionnez ensuite l' 

option et sélectionnez **Modifier**.
3. Dans la fenêtre **Modifier les détails du cluster**, sélectionnez l'option **+Ajouter** sous serveurs NTP.
4. Ajoutez le nom, l'emplacement et spécifiez l'adresse IP du serveur de temps.
5. Sélectionnez ensuite **Enregistrer**.
6. Répétez les étapes pour tous les autres serveurs de temps.

ONTAP 9.11.1 ou version ultérieure :

Procédez comme suit pour synchroniser le NTP à partir de la fenêtre **Insights** de l'onglet **Cluster** de ONTAP 9.11.1 ou version ultérieure.

Étapes

1. Accédez à **Cluster > Présentation**
2. Faites défiler jusqu'à la fenêtre **Insights** de la page, localisez **trop peu de serveurs NTP sont configurés**, puis sélectionnez **Fix it**.
3. Spécifiez l'adresse IP du serveur de temps, puis sélectionnez **Enregistrer**.
4. Répétez l'étape précédente pour tout autre serveur de temps.

Visibilité

Dans ONTAP 9.11.1 ou version ultérieure, vous pouvez également configurer le NTP à l'aide de l'onglet **Insights** du Gestionnaire système :

Étapes

1. Accédez à l'onglet **Insights** de l'interface utilisateur de System Manager.
2. Faites défiler jusqu'à **trop peu de serveurs NTP sont configurés** et sélectionnez **Fix it**.
3. Spécifiez l'adresse IP du serveur de temps, puis sélectionnez **Enregistrer**.
4. Répétez l'étape précédente pour tout autre serveur de temps.

Où trouver des informations supplémentaires sur MetroCluster IP

Pour en savoir plus sur la configuration MetroCluster,

MetroCluster et informations diverses

Informations	Objet
"Architecture et conception de la solution IP MetroCluster, TR-4689"	• Présentation technique de la configuration et du fonctionnement IP de MetroCluster. • Bonnes pratiques pour une configuration IP 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 MetroCluster"	• Présentation de la configuration MetroCluster • Basculement, rétablissement et rétablissement
"Reprise sur incident"	• Reprise après incident • Basculement forcé • La restauration après une panne de plusieurs contrôleurs ou de stockage

"Maintenance 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 et extension de MetroCluster"	• Mise à niveau ou actualisation d'une configuration MetroCluster • Extension d'une configuration MetroCluster par l'ajout de nœuds supplémentaires
"Transition MetroCluster"	• Passer d'une configuration MetroCluster FC à une configuration MetroCluster IP
"Mise à niveau, transition et extension de MetroCluster"	• Contrôle de la configuration de MetroCluster avec le logiciel MetroCluster Tiebreaker
"Documentation des systèmes matériels ONTAP" **Remarque :** les procédures de maintenance standard des tiroirs de stockage peuvent être utilisées avec les configurations IP de MetroCluster.	• 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

Informations sur les marques commerciales