



Installez une configuration MetroCluster extensible

ONTAP MetroCluster

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap-metrocluster/install-stretch/index.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Installez une configuration MetroCluster extensible	1
Présentation	1
La préparation de l'installation de MetroCluster	1
Différences entre les configurations ONTAP MetroCluster	1
Peering de clusters	3
Considérations relatives à l'utilisation d'agrégats non mis en miroir	5
Utilisation du pare-feu sur les sites MetroCluster	6
Choix de la procédure d'installation adaptée à votre configuration	7
Reliez une configuration Stretch MetroCluster à deux nœuds avec connexion SAS	7
Câblage d'une configuration Stretch MetroCluster à deux nœuds avec connexion SAS	7
Composants d'une configuration Stretch MetroCluster à deux nœuds avec disques SAS	7
Composants matériels MetroCluster requis et instructions de nommage pour les configurations Stretch SAS-Attached à deux nœuds	8
Installez et câbez les composants MetroCluster pour les configurations étendues reliées à SAS à deux nœuds	10
Câconstitue une configuration MetroCluster extensible à deux nœuds (Bridge-Attached)	13
Câblage d'une configuration MetroCluster extensible à deux nœuds Bridge-Attached	13
Composants d'une configuration Stretch MetroCluster à deux nœuds avec connexion Bridge-Attached	13
Composants matériels MetroCluster requis et conventions de nommage pour les configurations extensibles à deux nœuds	14
Fiche technique pour la collecte d'informations sur les ponts FC-SAS	16
Installez et cachez les composants MetroCluster	18
Installez des ponts FC-SAS et des tiroirs disques SAS	20
Configuration du logiciel MetroCluster dans ONTAP	33
Fiche d'informations sur le réseau IP pour le site A	34
Fiche d'informations sur le réseau IP pour le site B	36
Similarités et différences entre les configurations cluster standard et MetroCluster	38
Restauration des paramètres par défaut du système et configuration du type de HBA sur un module de contrôleur	39
Configuration des ports FC-VI sur une carte X1132A-R6 à quatre ports sur les systèmes FAS8020	41
Vérification de l'affectation du disque en mode maintenance dans une configuration à deux nœuds	43
Vérification de l'état des composants HA	45
Configuration d'ONTAP dans une configuration MetroCluster à deux nœuds	46
Configuration des clusters dans une configuration MetroCluster	48
Vérification des erreurs de configuration MetroCluster avec Config Advisor	71
Vérification du basculement, de la résolution et du rétablissement	71
Protection des fichiers de sauvegarde de configuration	72
Considérations relatives à l'utilisation du protocole IP virtuel et de passerelle de frontières avec une configuration MetroCluster	72
Test de la configuration MetroCluster	75
Vérification du basculement négocié	75
Vérification de la correction et du rétablissement manuel	76
Perte d'un seul pont FC-SAS	79

Vérification du fonctionnement après une interruption de la ligne d'alimentation	81
Vérification de l'opération après la perte d'un tiroir de stockage	82
Supprimer les configurations MetroCluster	93
Comment utiliser Active IQ Unified Manager et ONTAP System Manager pour obtenir des informations supplémentaires sur la configuration et le contrôle	94
Utilisez Active IQ Unified Manager et ONTAP System Manager pour une configuration et un contrôle supplémentaires.	94
Synchronisez l'heure du système à l'aide du protocole NTP	94
Considérations relatives à l'utilisation de ONTAP dans une configuration MetroCluster	95
Considérations relatives aux licences	96
Considération de SnapMirror	96
Prise en charge de FlexCache dans une configuration MetroCluster	96
Prise en charge de FabricPool dans les configurations MetroCluster	96
Prise en charge de FlexGroup dans les configurations MetroCluster	97
Planifications de travaux dans une configuration MetroCluster	97
Peering de cluster depuis le site de MetroCluster vers un troisième cluster	97
Réplication de la configuration du client LDAP dans une configuration MetroCluster	98
Instructions de création de LIF et de mise en réseau pour les configurations MetroCluster	98
Reprise après incident de SVM dans une configuration MetroCluster	102
Résultat des commandes Storage disk show et Storage shelf show dans une configuration MetroCluster étendue à deux nœuds	104
Le résultat de la commande plex show de l'agrégat de stockage est indéterminé après un basculement de MetroCluster	105
Modification des volumes pour définir l'indicateur NVFAIL en cas de basculement	105
Passer d'une configuration Stretch à une configuration MetroCluster Fabric-Attached	105
Où trouver des informations complémentaires	106
MetroCluster et informations diverses	106

Installez une configuration MetroCluster extensible

Présentation

Pour installer votre configuration Stretch MetroCluster, vous devez effectuer plusieurs procédures dans le bon ordre.

- ["Préparation de l'installation et compréhension de toutes les exigences"](#)
- ["Choisissez la procédure d'installation correcte"](#)
- Brancher les composants
 - ["Configuration SAS à deux nœuds"](#)
 - ["Configuration à deux nœuds avec connexion par pont"](#)
- ["Configurez le logiciel"](#)
- ["Tester la configuration"](#)

La préparation de l'installation de MetroCluster

Différences entre les 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 nœuds	Deux nœuds	Connexion pont à deux nœuds	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"](#).

Peering de clusters

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.

Considérations relatives à l'utilisation d'agrégats non mis en miroir

Considérations relatives à l'utilisation d'agrégats non mis en miroir

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

Considérations relatives aux agrégats non mis en miroir lors de tâches de maintenance nécessitant l'arrêt d'alimentation

Si vous effectuez un basculement négocié pour des raisons de maintenance requérant un arrêt de l'alimentation à l'échelle du site, vous devez d'abord mettre manuellement hors ligne les agrégats non mis en miroir qui appartiennent au site de reprise sur incident.

Si vous ne mettez pas d'agrégats non mis en miroir hors ligne, les nœuds du site survivant peuvent tomber en panne en raison de la présence de incohérences de plusieurs disques. Cela peut se produire lorsqu'un basculement sur des agrégats non mis en miroir est hors ligne ou lorsqu'ils sont manquants en raison de la perte de connectivité au stockage sur le site de secours. Cela est le résultat d'un arrêt de courant ou d'une

perte de liens ISL.

Considérations relatives aux agrégats non mis en miroir et aux 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.

Considérations relatives aux agrégats non mis en miroir et aux volumes de métadonnées CRS et aux volumes racines des 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 négociées de basculement et de rétablissement sont vetotées. La commande MetroCluster check fournit un avertissement si c'est le cas.

Considérations relatives aux SVM et aux agrégats sans miroir

Les SVM doivent être configurés sur des agrégats en miroir uniquement ou sur des agrégats sans miroir uniquement. La configuration d'une combinaison d'agrégats non mis en miroir et en miroir peut entraîner un basculement supérieur à 120 secondes et entraîner une panne des données en cas d'indisponibilité des agrégats non mis en miroir.

Considérations relatives aux agrégats sans miroir et à SAN

Dans les versions ONTAP antérieures à 9.9.1, un LUN ne doit pas être situé sur un agrégat sans 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.

Utilisation du pare-feu sur les sites MetroCluster

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

Choix de la procédure d'installation adaptée à votre configuration

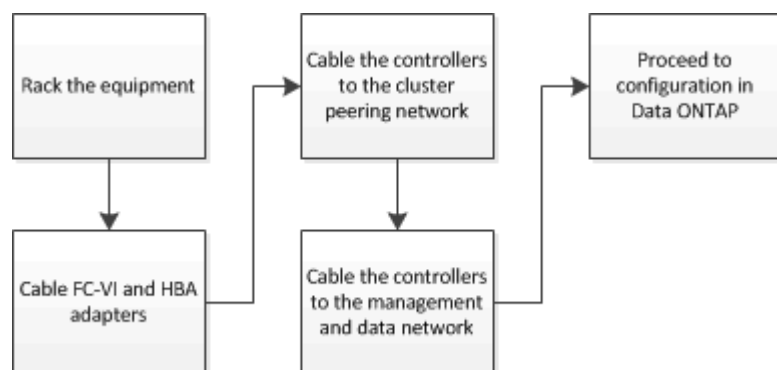
Vous devez choisir la procédure d'installation appropriée en fonction de la manière dont les contrôleurs de stockage se connectent aux étagères de stockage.

Pour ce type d'installation...	Utilisez ces procédures...
Configuration Stretch à deux nœuds avec ponts FC-SAS	1. "Câblage d'une configuration MetroCluster extensible à deux nœuds Bridge-Attached" 2. "Configuration du logiciel MetroCluster dans ONTAP"
Configuration d'extension à deux nœuds avec câblage SAS à connexion directe	1. "Câblage d'une configuration Stretch MetroCluster à deux nœuds avec connexion SAS" 2. "Configuration du logiciel MetroCluster dans ONTAP"

Reliez une configuration Stretch MetroCluster à deux nœuds avec connexion SAS

Câblage d'une configuration Stretch MetroCluster à deux nœuds avec connexion SAS

Les composants MetroCluster doivent être installés, câblés et configurés physiquement sur les deux sites géographiques.



Composants d'une configuration Stretch MetroCluster à deux nœuds avec disques SAS

La configuration MetroCluster à deux nœuds avec connexion SAS nécessite plusieurs composants, notamment deux clusters à un seul nœud dans lesquels les contrôleurs de

stockage sont directement connectés au stockage par le biais de câbles SAS.

La configuration MetroCluster inclut les éléments matériels clés suivants :

- Contrôleurs de stockage

Les contrôleurs de stockage se connectent directement au stockage à l'aide de câbles SAS.

Chaque contrôleur de stockage est configuré comme partenaire de reprise après incident sur un contrôleur de stockage du site partenaire.

- Des câbles SAS en cuivre peuvent être utilisés pour des distances plus courtes.
- Vous pouvez utiliser des câbles SAS optiques sur de longues distances.

["Matrice d'interopérabilité NetApp"](#)

Dans le IMT, vous pouvez utiliser le champ solution de stockage pour sélectionner votre solution MetroCluster. Utilisez **Explorateur de composants** pour sélectionner les composants et la version ONTAP pour affiner votre recherche. Vous pouvez cliquer sur **Afficher les résultats** pour afficher la liste des configurations prises en charge qui correspondent aux critères.

- Réseau de peering de cluster

Le réseau de peering de cluster assure la connectivité en miroir de la configuration de la machine virtuelle de stockage (SVM). La configuration de tous les SVM sur un cluster est mise en miroir sur le cluster partenaire.

Composants matériels MetroCluster requis et instructions de nommage pour les configurations Stretch SAS-Attached à deux nœuds

La configuration MetroCluster nécessite divers composants matériels. Pour plus de clarté et de commodité, des noms standard de composants sont utilisés dans la documentation MetroCluster. Un site est appelé site A et l'autre site est appelé site B.

Logiciels et matériel pris en charge

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

["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.

Redondance matérielle dans la configuration MetroCluster

En raison de la redondance matérielle dans la configuration 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 composants individuels.

Deux clusters ONTAP à un seul nœud

La configuration Stretch MetroCluster basée sur SAS requiert deux clusters ONTAP à un seul nœud.

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

- Site A : cluster_A
- Site B : cluster_B

Deux modules de contrôleur de stockage

La configuration Stretch MetroCluster basée sur SAS requiert deux modules de contrôleur de stockage.

- Le nom doit être unique dans la configuration MetroCluster.
- Tous les modules de contrôleur de la configuration MetroCluster doivent exécuter la même version de ONTAP.
- Tous les modules de contrôleur d'un groupe DR doivent être du même modèle.
- Tous les modules de contrôleur d'un groupe de reprise sur incident doivent utiliser la même configuration FC-VI.

Certains modules de contrôleur prennent en charge deux options pour la connectivité FC-VI :

- Ports FC-VI intégrés
- Une carte FC-VI dans le logement 1

Les configurations utilisant un module de contrôleur utilisant des ports FC-VI intégrés et une autre utilisant une carte FC-VI add-on ne sont pas prises en charge. Par exemple, si un nœud utilise la configuration FC-VI intégrée, tous les autres nœuds du groupe de reprise sur incident doivent également utiliser la configuration FC-VI intégrée.

Exemples de noms :

- Site A : Controller_A_1
- Site B : Controller_B_1

Au moins quatre tiroirs disques SAS (recommandé)

La configuration Stretch MetroCluster (SAS-Attached) requiert au moins deux tiroirs disques SAS. Quatre tiroirs disques SAS sont recommandés.

Deux tiroirs sont recommandés sur chaque site pour permettre la propriété du disque par tiroir. Au moins un tiroir est pris en charge sur chaque site.

Exemples de noms :

- Site A :
 - Shelf_A_1_1
 - Shelf_A_1_2
- Site B :
 - Shelf_B_1_1
 - Shelf_B_1_2

Installez et câbez les composants MetroCluster pour les configurations étendues reliées à SAS à deux nœuds

Installation et câblage des composants MetroCluster pour les configurations Stretch SAS-Attached à deux nœuds

Les contrôleurs de stockage doivent être reliés au support de stockage et reliés entre eux. Les contrôleurs de stockage doivent également être câblés au réseau de données et de gestion.

Avant de commencer une procédure dans ce document

Les exigences générales suivantes doivent être respectées avant d'effectuer cette tâche :

- Avant l'installation, vous devez vous familiariser avec les considérations et les meilleures pratiques d'installation et de câblage des tiroirs disques pour votre modèle de tiroir disque.
- Tous les composants MetroCluster doivent être pris en charge.

["Matrice d'interopérabilité NetApp"](#)

Dans le IMT, vous pouvez utiliser le champ solution de stockage pour sélectionner votre solution MetroCluster. Utilisez **Explorateur de composants** pour sélectionner les composants et la version ONTAP pour affiner votre recherche. Vous pouvez cliquer sur **Afficher les résultats** pour afficher la liste des configurations prises en charge qui correspondent aux critères.

Description de la tâche

- Les termes « nœud » et « contrôleur » sont utilisés de manière interchangeable.

Mise en rack des composants matériels

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

Cette tâche doit être effectuée sur les deux sites MetroCluster.

Étapes

1. Planifiez le positionnement des composants MetroCluster.

La quantité d'espace rack nécessaire dépend du modèle de plateforme des contrôleurs de stockage, des types de commutateurs et du nombre de piles de tiroirs disques dans votre configuration.

2. Le respect des pratiques d'atelier standard pour travailler avec des équipements électriques permet de vous assurer que vous êtes correctement mis à la terre.
3. Installez les contrôleurs de stockage sur le rack ou l'armoire.

["Documentation des systèmes matériels ONTAP"](#)

4. Installez les tiroirs disques, connectez-les en série dans chaque pile, mettez-les sous tension et définissez les identifiants des tiroirs.

Pour plus d'informations sur la configuration des tiroirs disques et sur la configuration des identifiants de

tiroirs, reportez-vous au guide approprié pour votre modèle de tiroir disque.



Ils doivent être uniques pour chaque tiroir disque SAS dans chaque groupe DR MetroCluster (y compris les deux sites). Lorsque vous définissez manuellement les ID de tiroir, vous devez mettre le tiroir disque sous tension.

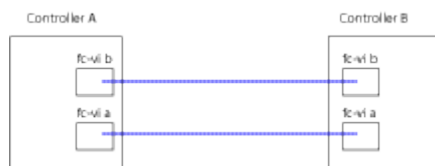
Câblage des contrôleurs les uns aux autres et des tiroirs de stockage

Les adaptateurs FC-VI du contrôleur doivent être câblés directement les uns aux autres. Les ports SAS du contrôleur doivent être câblés à la fois aux piles de stockage distantes et locales.

Cette tâche doit être effectuée sur les deux sites MetroCluster.

Étapes

1. Brancher les ports FC-VI.

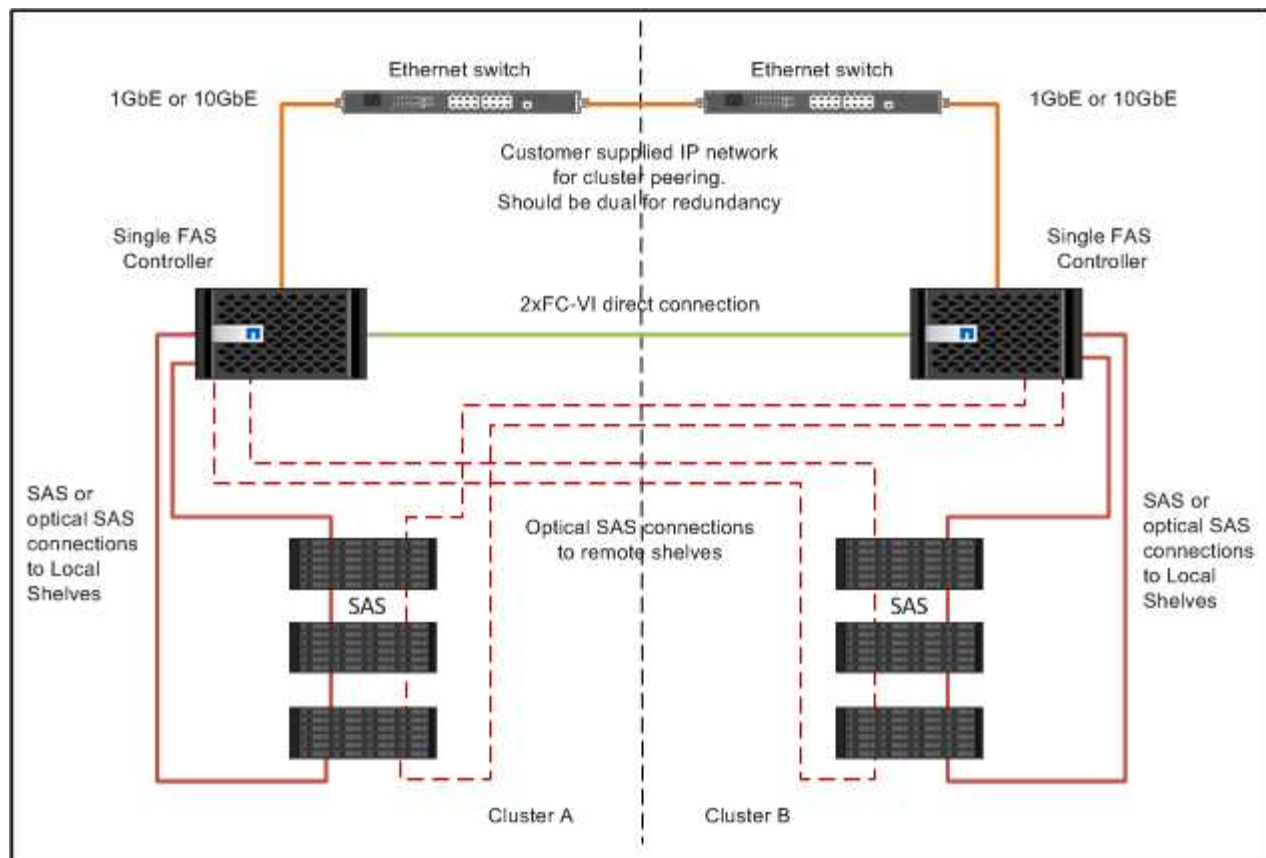


L'illustration ci-dessus est une connexion de câble représentative type. Les ports FC-VI spécifiques varient en fonction du module de contrôleur.

- Vous pouvez commander des modules de contrôleur FAS8200 et AFF A300 avec l'une des deux options de connectivité FC-VI :
 - Les ports intégrés 0e et 0f sont configurés en mode FC-VI.
 - Les ports 1a et 1b sur une carte FC-VI sont placés dans l'emplacement 1.
- Les modules de contrôleur des systèmes de stockage AFF A700 et FAS9000 utilisent chacun quatre ports FC-VI.
- Les modules contrôleurs des systèmes de stockage AFF A400 et FAS8300 utilisent les ports FC-VI 2a et 2b.

2. Reliez les ports SAS.

L'illustration suivante montre les connexions. L'utilisation de vos ports peut être différente selon les ports SAS et FC-VI disponibles sur le module de contrôleur.



Câblage des connexions de peering de cluster

Vous devez câbler les ports du module de contrôleur utilisés pour le peering de cluster, de sorte qu'ils aient une connectivité avec le cluster sur leur site partenaire.

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.

Étapes

1. Identifier et câbler au moins deux ports pour peering de cluster et vérifier qu'ils disposent d'une connectivité réseau avec le cluster partenaire.

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"](#)

Câblage de la gestion et des connexions de données

Vous devez câbler les ports de gestion et de données de chaque contrôleur de stockage pour les réseaux du site.

Cette tâche doit être répétée pour chaque nouveau contrôleur des deux sites MetroCluster.

Vous pouvez connecter les ports de gestion du contrôleur et du commutateur de cluster aux commutateurs existants de votre réseau. Vous pouvez également connecter le contrôleur aux nouveaux commutateurs réseau dédiés, tels que les commutateurs de gestion du cluster NetApp CN1601.

Étapes

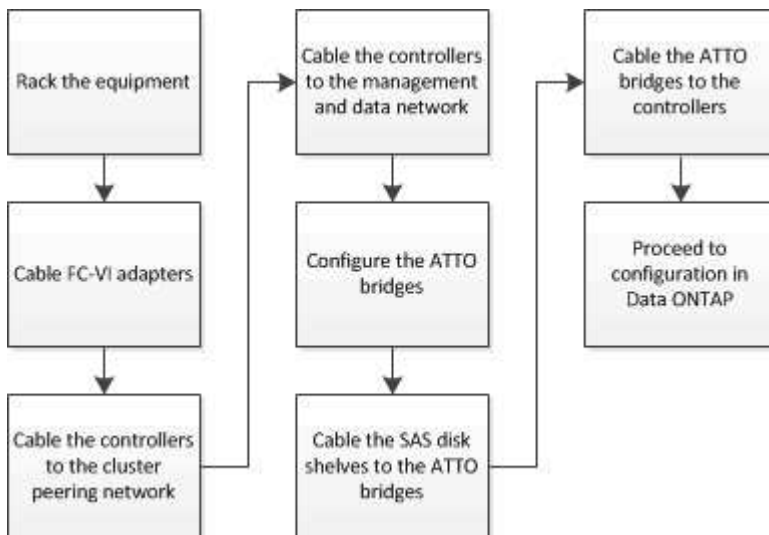
1. Reliez les ports de gestion et de données du contrôleur aux réseaux de gestion et de données du site local.

["Documentation des systèmes matériels ONTAP"](#)

Câble constitue une configuration MetroCluster extensible à deux nœuds (Bridge-Attached)

Câblage d'une configuration MetroCluster extensible à deux nœuds Bridge-Attached

Les composants MetroCluster doivent être installés, câblés et configurés physiquement sur les deux sites géographiques.



Composants d'une configuration Stretch MetroCluster à deux nœuds avec connexion Bridge-Attached

Lorsque vous planifiez votre configuration MetroCluster, vous devez comprendre les éléments de la configuration et leur fonctionnement commun.

La configuration MetroCluster inclut les éléments matériels clés suivants :

- Contrôleurs de stockage

Les contrôleurs de stockage ne sont pas directement connectés au stockage, mais sont connectés à des ponts FC-SAS. Les contrôleurs de stockage sont reliés par des câbles FC entre les adaptateurs FC-VI de chaque contrôleur.

Chaque contrôleur de stockage est configuré comme partenaire de reprise après incident sur un contrôleur de stockage du site partenaire.

- Ponts FC-SAS

Le pont FC-to-SAS relie les piles de stockage SAS aux ports d'initiateur FC des contrôleurs, offrant ainsi une passerelle entre les deux protocoles.

- Réseau de peering de cluster

Le réseau de peering de cluster assure la connectivité en miroir de la configuration de la machine virtuelle de stockage (SVM). La configuration de tous les SVM sur un cluster est mise en miroir sur le cluster partenaire.

L'illustration suivante présente une vue simplifiée de la configuration MetroCluster. Pour certaines connexions, une seule ligne représente plusieurs connexions redondantes entre les composants. Les connexions du réseau de gestion et de données ne sont pas affichées.

- La configuration se compose de deux clusters à un seul nœud.
- Chaque site dispose d'une ou plusieurs piles de stockage SAS.



Les tiroirs SAS des configurations MetroCluster ne sont pas pris en charge avec le câblage ACP.

D'autres piles de stockage sont prises en charge, mais une seule s'affiche sur chaque site.

Composants matériels MetroCluster requis et conventions de nommage pour les configurations extensibles à deux nœuds

Lorsque vous planifiez votre configuration MetroCluster, vous devez comprendre les composants matériels et logiciels requis et pris en charge. Pour plus de commodité et de clarté, vous devez également comprendre les conventions de dénomination utilisées pour les composants dans les exemples de la documentation. Par exemple, un site est appelé site A et l'autre site est appelé site B.

Logiciels et matériel pris en charge

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

"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.

Redondance matérielle dans la configuration MetroCluster

En raison de la redondance matérielle dans la configuration 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 composants individuels.

Condition requise pour deux clusters ONTAP à un nœud

La configuration Stretch MetroCluster à connexion Bridge-Attached requiert deux clusters ONTAP à un seul

nœud.

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

- Site A : cluster_A
- Site B : cluster_B

Configuration requise pour deux modules de contrôleur de stockage

La configuration Stretch MetroCluster à connexion Bridge-Attached requiert deux modules de contrôleur de stockage.

Les contrôleurs doivent répondre aux exigences suivantes :

- Le nom doit être unique dans la configuration MetroCluster.
- Tous les modules de contrôleur de la configuration MetroCluster doivent exécuter la même version de ONTAP.
- Tous les modules de contrôleur d'un groupe DR doivent être du même modèle.
- Tous les modules de contrôleur d'un groupe de reprise sur incident doivent utiliser la même configuration FC-VI.

Certains modules de contrôleur prennent en charge deux options pour la connectivité FC-VI :

- Ports FC-VI intégrés
- Une carte FC-VI dans le logement 1

Les configurations utilisant un module de contrôleur utilisant des ports FC-VI intégrés et une autre utilisant une carte FC-VI add-on ne sont pas prises en charge. Par exemple, si un nœud utilise la configuration FC-VI intégrée, tous les autres nœuds du groupe de reprise sur incident doivent également utiliser la configuration FC-VI intégrée.

Exemples de noms :

- Site A : Controller_A_1
- Site B : Controller_B_1

Conditions requises pour les ponts FC-SAS

La configuration Stretch MetroCluster à connexion Bridge-Attached nécessite au moins deux ponts FC-SAS à chaque site.

Ces ponts connectent les tiroirs disques SAS aux modules de contrôleur.



Les ponts FiberBridge 6500N ne sont pas pris en charge dans les configurations exécutant ONTAP 9.8 et versions ultérieures.

- Les ponts FiberBridge 7600N et 7500N prennent en charge jusqu'à quatre piles SAS.
- Chaque pile peut utiliser différents modèles d'E/S, mais tous les tiroirs d'une pile doivent utiliser le même modèle.

Les modèles de module d'E/S pris en charge dépendent de la version ONTAP que vous exécutez.

- Le nom doit être unique dans la configuration MetroCluster.

Les noms suggérés sont utilisés comme exemples dans cette procédure pour identifier le module de contrôleur auquel le pont se connecte et le port.

Exemples de noms :

- Site A :
 - Bridge_A_1_*port-number*
 - Pont_A_2_*port-number*
- Site B :
 - Pont_B_1_*port-number*
 - Pont_B_2_*port-number*

Configuration requise pour au moins quatre tiroirs SAS (recommandé)

La configuration Stretch MetroCluster (Bridge-Attached) requiert au moins deux tiroirs SAS. Cependant, deux tiroirs sont recommandés sur chaque site pour permettre la propriété des disques par tiroir, pour un total de quatre tiroirs SAS.

Au moins un tiroir est pris en charge sur chaque site.

Exemples de noms :

- Site A :
 - Shelf_A_1_1
 - Shelf_A_1_2
- Site B :
 - Shelf_B_1_1
 - Shelf_B_1_2

Fiche technique pour la collecte d'informations sur les ponts FC-SAS

Vous devez collecter les informations de configuration requises avant de commencer à configurer les sites MetroCluster.

Site A, pont FC-to-SAS 1 (FC_Bridge_A_1a)

Chaque pile SAS requiert au moins deux ponts FC-SAS.

Chaque pont se connecte au Controller_A_1_*port-number* Et Controller_B_1_*port-number*.

Site A	Votre valeur
Adresse IP Bridge_A_1a	

Nom d'utilisateur Bridge_A_1a	
Mot de passe Bridge_A_1a	

Site A, pont FC-to-SAS 2 (FC_Bridge_A_1b)

Chaque pile SAS requiert au moins deux ponts FC-SAS.

Chaque pont se connecte au Controller_A_1_ *port-number* Et Controller_B_1_ *port-number*.

Site A	Votre valeur
Adresse IP Bridge_A_1b	
Nom d'utilisateur Bridge_A_1b	
Mot de passe Bridge_A_1b	

Site B, pont FC-to-SAS 1 (FC_Bridge_B_1a)

Chaque pile SAS requiert au moins deux ponts FC-SAS.

Chaque pont se connecte au Controller_A_1_ *port-number* et au Controller_B_1_ *port-number*'.

Site B	Votre valeur
Adresse IP Bridge_B_1a	
Bridge_B_1a Nom d'utilisateur	
Mot de passe Bridge_B_1a	

Site B, pont FC-to-SAS 2 (FC_Bridge_B_1b)

Chaque pile SAS requiert au moins deux ponts FC-SAS.

Chaque pont se connecte au Controller_A_1_ *port-number* et au Controller_B_1_ *port-number*'.

Site B	Votre valeur
Adresse IP Bridge_B_1b	
Bridge_B_1b Nom d'utilisateur	
Mot de passe Bridge_B_1b	

Installez et cachez les composants MetroCluster

Mise en rack des composants matériels

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

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 contrôleurs de stockage, des types de commutateurs et du nombre de piles de tiroirs disques de votre configuration.

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

"Documentation des systèmes matériels ONTAP"

4. Installez les tiroirs disques, mettez-les sous tension et définissez les ID de tiroir.
 - Vous devez mettre chaque tiroir disque hors tension puis sous tension.
 - Ils doivent être uniques pour chaque tiroir disque SAS dans chaque groupe DR MetroCluster (y compris les deux sites).
5. Installer chaque pont FC-to-SAS :
 - a. Fixez les supports « L » à l'avant du pont à l'avant du rack (montage encastré) à l'aide des quatre vis.

Les ouvertures des supports « L » du pont sont conformes à la norme de rack ETA-310-X pour les racks de 19 pouces (482.6 mm).

Pour plus d'informations et une illustration de l'installation, reportez-vous au Manuel d'installation et d'utilisation de *ATTO FibreBridge pour votre modèle de pont*.
 - b. Connectez chaque pont à une source d'alimentation qui fournit une mise à la masse correcte.
 - c. Mettez chaque pont sous tension.



Pour une résilience maximale, les ponts reliés à la même pile de tiroirs disques doivent être connectés à différentes sources d'alimentation.

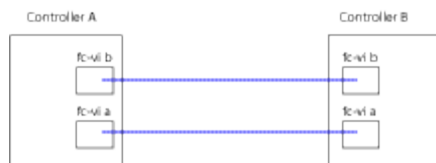
Le voyant de l'état prêt du pont peut prendre jusqu'à 30 secondes pour indiquer que le pont a terminé sa séquence d'auto-test de mise sous tension.

Câblage des contrôleurs les uns aux autres

Les adaptateurs FC-VI de chaque contrôleur doivent être câblés directement à son partenaire.

Étapes

1. Brancher les ports FC-VI.



L'illustration ci-dessus présente une représentation type du câblage requis. Les ports FC-VI spécifiques varient en fonction du module de contrôleur.

- Vous pouvez commander des modules de contrôleur AFF A300 et FAS8200 avec l'une des deux options de connectivité FC-VI :
 - Ports intégrés 0e et 0f configurés en mode FC-VI.
 - Ports 1a et 1b sur une carte FC-VI dans l'emplacement 1.
- Les modules de contrôleur des systèmes de stockage AFF A700 et FAS9000 utilisent chacun quatre ports FC-VI.

Câblage des connexions de peering de cluster

Vous devez câbler les ports du module de contrôleur utilisés pour le peering de cluster, de sorte qu'ils aient une connectivité avec le cluster sur leur site partenaire.

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.

Étapes

1. Identifier et câbler au moins deux ports pour peering de cluster et vérifier qu'ils disposent d'une connectivité réseau avec le cluster partenaire.

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"](#)

Câblage de la gestion et des connexions de données

Vous devez câbler les ports de gestion et de données de chaque contrôleur de stockage pour les réseaux du site.

Cette tâche doit être répétée pour chaque nouveau contrôleur des deux sites MetroCluster.

Vous pouvez connecter les ports de gestion du contrôleur et du commutateur de cluster aux commutateurs existants de votre réseau. Vous pouvez également connecter le contrôleur aux nouveaux commutateurs réseau dédiés, tels que les commutateurs de gestion du cluster NetApp CN1601.

Étapes

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

["Documentation des systèmes matériels ONTAP"](#)

Installez des ponts FC-SAS et des tiroirs disques SAS

Installez et câblez les ponts FibreBridge et les tiroirs disques SAS ATTO lorsque vous ajoutez un nouveau stockage à la configuration.

Description de la tâche

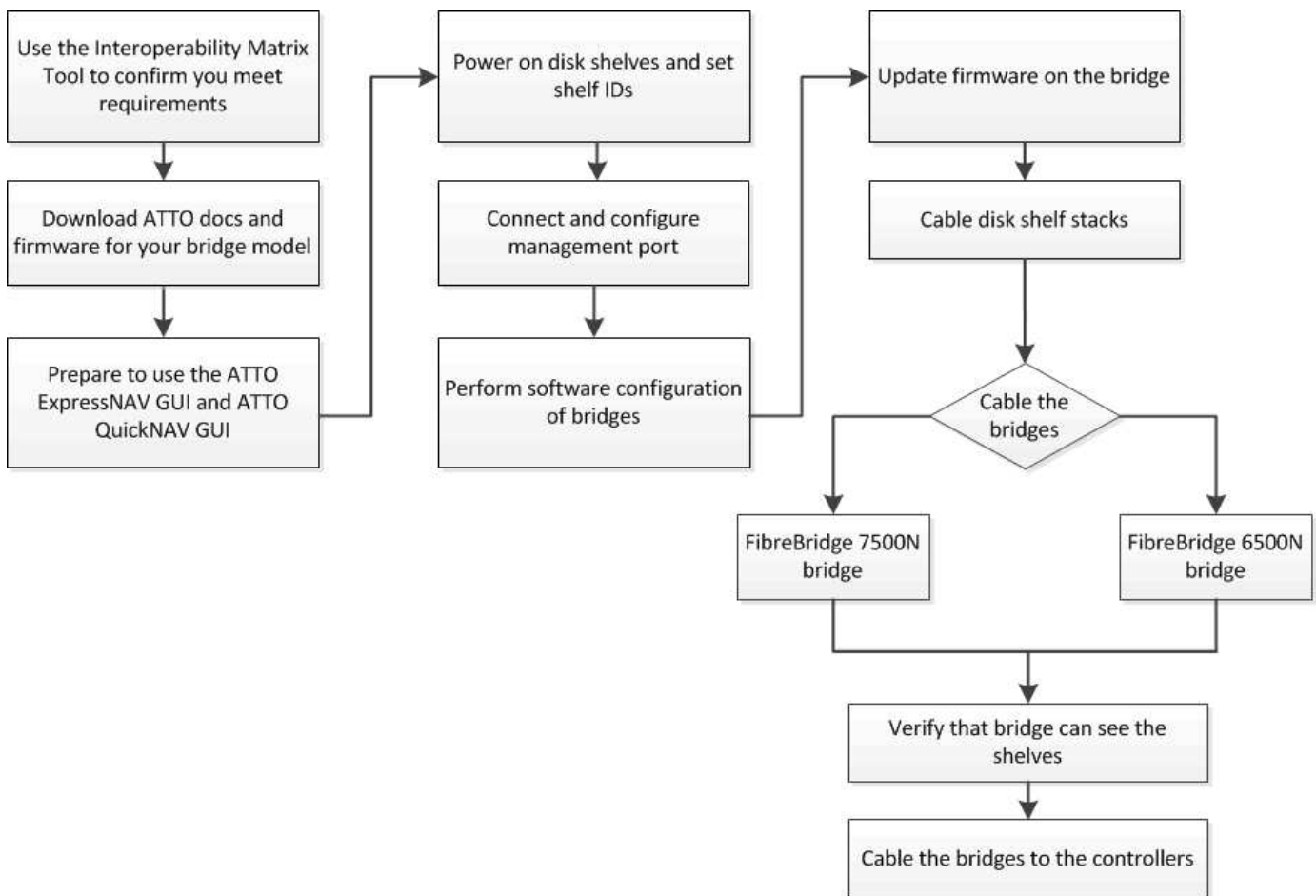
Pour les systèmes reçus en usine, les ponts FC-SAS sont préconfigurés et ne requièrent pas de configuration supplémentaire.

Cette procédure est rédigée avec l'hypothèse que vous utilisez les interfaces de gestion des ponts recommandées : l'interface graphique utilisateur graphique ATTO ExpressNAV et l'utilitaire ATTO Quickmenu.

L'interface graphique ATTO ExpressNAV permet de configurer et de gérer un pont, ainsi que de mettre à jour le micrologiciel du pont. Utilisez l'utilitaire ATTO Quicknavigation pour configurer le port de gestion Ethernet de pont 1.

Vous pouvez utiliser d'autres interfaces de gestion, si nécessaire, comme un port série ou Telnet pour configurer et gérer un pont et pour configurer le port de gestion Ethernet 1, et FTP pour mettre à jour le micrologiciel du pont.

Cette procédure utilise le workflow suivant :



Gestion intrabande des ponts FC-SAS

Depuis ONTAP 9.5 avec des ponts FiberBridge 7500N ou 7600N, *gestion intrabande* des ponts est pris en charge comme alternative à la gestion IP des ponts. Depuis la version ONTAP 9.8, la gestion hors bande est

obsolète.



Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Lors de l'utilisation de la gestion intrabande, les ponts peuvent être gérés et surveillés à partir de l'interface de ligne de commande ONTAP via la connexion FC au pont. L'accès physique au pont via les ports Ethernet du pont n'est pas nécessaire, ce qui réduit la vulnérabilité de sécurité du pont.

La disponibilité de la gestion intrabande des ponts dépend de la version de ONTAP :

- Depuis ONTAP 9.8, les ponts sont gérés via des connexions intrabande par défaut et la gestion hors bande des ponts via SNMP est déconseillée.
- ONTAP 9.5 à 9.7 : la gestion intrabande ou la gestion SNMP hors bande est prise en charge.
- Avant ONTAP 9.5, seule la gestion SNMP hors bande est prise en charge.

Les commandes CLI Bridge peuvent être émises à partir de la commande d'interface ONTAP `storage bridge run-cli -name <bridge_name> -command <bridge_command_name>` au niveau de l'interface ONTAP.



Il est recommandé d'utiliser la gestion intrabande avec l'accès IP désactivé pour améliorer la sécurité en limitant la connectivité physique du pont.

Limites de pont FibreBridge 7600N et 7500N et règles de connexion

Passez en revue les limites et les considérations lors de la fixation des ponts FibreBridge 7600N et 7500N.

Limites de pont FibreBridge 7600N et 7500N

- Le nombre maximum de disques durs et SSD combinés est de 240.
- Le nombre maximum de disques SSD est de 96.
- Le nombre maximal de disques SSD par port SAS est de 48.
- Le nombre maximum de tiroirs par port SAS est de 10.

Règles de connexion des ponts FibreBridge 7600N et 7500N

- Ne mélangez pas des disques SSD et HDD sur le même port SAS.
- Répartissez les tiroirs de manière homogène entre les ports SAS.
- Vous ne devez pas avoir de tiroirs DS460 sur le même port SAS que d'autres types de tiroirs (par exemple, tiroirs DS212 ou DS224).

Exemple de configuration

Voici un exemple de configuration permettant de connecter quatre tiroirs DS224 avec des disques SSD et six tiroirs DS224 avec des disques durs :

Port SAS	Tiroirs et disques
Port SAS A	2 tiroirs DS224 avec disques SSD
Port SAS B	2 tiroirs DS224 avec disques SSD

Port SAS	Tiroirs et disques
Port SAS C	3 tiroirs DS224 avec disques durs
Port SAS D	3 tiroirs DS224 avec disques durs

Préparer l'installation

Lorsque vous vous préparez à installer les ponts dans le cadre de votre nouveau système MetroCluster, vous devez vérifier que votre système répond à certaines exigences, y compris la configuration requise pour les ponts. Il est également nécessaire de télécharger les documents nécessaires, l'utilitaire ATTO Quickmenu et le firmware du pont.

Avant de commencer

- Votre système doit déjà être installé dans un rack s'il n'a pas été livré dans une armoire système.
- Votre configuration doit utiliser les modèles matériels et les versions logicielles pris en charge.

Dans le "[Matrice d'interopérabilité NetApp \(IMT\)](#)", vous pouvez utiliser le champ **solution de stockage** pour sélectionner votre solution MetroCluster. Vous pouvez utiliser **Explorateur de composants** pour sélectionner les composants et la version ONTAP afin d'affiner votre recherche. Vous pouvez sélectionner **Afficher les résultats** pour afficher la liste des configurations prises en charge qui correspondent aux critères.

- Chaque contrôleur FC doit disposer d'un port FC disponible pour qu'un pont puisse se connecter à celui-ci.
- Vous devez connaître la gestion des câbles SAS ainsi que les considérations et les meilleures pratiques en matière d'installation et de câblage des tiroirs disques.

Le *Guide d'installation et de services* de votre modèle de tiroir disque décrit les considérations et les meilleures pratiques.

- L'ordinateur que vous utilisez pour configurer les ponts doit exécuter un navigateur Web pris en charge par ATTO pour utiliser l'interface graphique ATTO ExpressNAV.

Les notes de mise à jour *ATTO Product Release Notes* disposent d'une liste à jour des navigateurs Web pris en charge. Vous pouvez accéder à ce document à partir du site Web ATTO comme décrit dans les étapes suivantes.

Étapes

1. Téléchargez le *Guide d'installation et de maintenance* pour votre modèle de tiroir disque :
 - a. Accédez au site Web ATTO à l'aide du lien fourni pour votre modèle FibreBridge et téléchargez le manuel et l'utilitaire du menu à navigation rapide.



Le Manuel d'installation et d'utilisation *ATTO FibreBridge* pour votre pont modèle contient plus d'informations sur les interfaces de gestion.

Vous pouvez accéder à ce contenu et à d'autres contenus sur le site Web d'ATTO en utilisant le lien fourni sur la page de description d'ATTO FibreBridge.

2. Rassemblez le matériel et les informations nécessaires pour utiliser les interfaces de gestion des ponts recommandées, l'interface graphique ATTO ExpressNAV et l'utilitaire ATTO Quicknavigation :
 - a. Déterminez un nom d'utilisateur et un mot de passe non par défaut (pour accéder aux ponts).

Vous devez modifier le nom d'utilisateur et le mot de passe par défaut.

- b. Si vous configurez la gestion IP des ponts, vous avez besoin du câble Ethernet blindé fourni avec les ponts (qui se connecte du port de gestion Ethernet du pont 1 à votre réseau).
- c. Si vous configurez la gestion IP des ponts, vous devez disposer d'une adresse IP, d'un masque de sous-réseau et d'informations de passerelle pour le port de gestion Ethernet 1 de chaque pont.
- d. Désactivez les clients VPN sur l'ordinateur que vous utilisez pour la configuration.

Les clients VPN actifs provoquent l'échec de la recherche du menu à menu rapide pour les ponts.

Installez le pont FC à SAS et les tiroirs SAS

Après avoir vérifié que le système répond à toutes les exigences de la section « préparation de l'installation », vous pouvez installer votre nouveau système.

Description de la tâche

- La configuration de tiroir et de disque au niveau des deux sites doit être identique.

Si un agrégat non mis en miroir est utilisé, la configuration du disque et du tiroir sur chaque site peut être différente.



Tous les disques du groupe de reprise après incident doivent utiliser le même type de connexion et être visibles pour tous les nœuds du groupe de reprise après incident, quels que soient les disques utilisés pour les agrégats en miroir ou non mis en miroir.

- Les exigences de connectivité du système pour les distances maximales pour les tiroirs disques, les contrôleurs FC et les dispositifs de sauvegarde sur bande utilisant des câbles à fibre optique multimode de 50 microns s'appliquent également aux ponts FibreBridge.

"NetApp Hardware Universe"



La technologie ACP intrabande est prise en charge sans câblage supplémentaire au niveau des tiroirs et des ponts FiberBridge 7500N ou 7600N :

- IOM12 (DS460C) derrière un pont 7500N ou 7600N avec ONTAP 9.2 et versions ultérieures
- IOM12 (DS212C et DS224C) derrière un pont 7500N ou 7600N avec ONTAP 9.1 et versions ultérieures



Les tiroirs SAS des configurations MetroCluster ne prennent pas en charge le câblage ACP.

Activez l'accès au port IP sur le pont FiberBridge 7600N si nécessaire

Si vous utilisez une version ONTAP antérieure à 9.5 ou si vous prévoyez d'utiliser un accès hors bande au pont FiberBridge 7600N à l'aide de telnet ou d'autres protocoles et services de port IP (FTP, ExpressNAV, ICMP ou Quickmenu), vous pouvez activer les services d'accès via le port de console.

Description de la tâche

Contrairement aux ponts ATTO FibreBridge 7500N, le pont FibreBridge 7600N est livré avec tous les protocoles et services de port IP désactivés.

Depuis ONTAP 9.5, *gestion intrabande* des ponts est pris en charge. Cela signifie que les ponts peuvent être

configurés et surveillés depuis l'interface de ligne de commande de ONTAP via la connexion FC au pont. L'accès physique au pont via les ports Ethernet du pont n'est pas nécessaire et les interfaces utilisateur du pont ne sont pas requises.

Depuis ONTAP 9.8, la fonction *gestion intrabande* des ponts est prise en charge par défaut et la gestion SNMP hors bande est déconseillée.

Cette tâche est obligatoire si vous utilisez **pas** la gestion intrabande pour gérer les ponts. Dans ce cas, vous devez configurer le pont via le port de gestion Ethernet.

Étapes

1. Accédez à l'interface de la console du pont en connectant un câble série au port série du pont FibreBridge 7600N.
2. À l'aide de la console, activez les services d'accès, puis enregistrez la configuration :

```
set closeport none
```

```
saveconfiguration
```

Le `set closeport none` commande active tous les services d'accès sur le pont.

3. Désactivez un service, si vous le souhaitez, en émettant le `set closeport` commande et répétition de la commande si nécessaire jusqu'à ce que tous les services souhaités soient désactivés :

```
set closeport service
```

Le `set closeport` commande désactive un seul service à la fois.

Le paramètre `service` peut être spécifié comme l'un des éléments suivants :

- espresso
- ftp
- icmp
- menu à menu rapide
- snmp
- telnet

Vous pouvez vérifier si un protocole spécifique est activé ou désactivé à l'aide du `get closeport` commande.

4. Si vous activez SNMP, vous devez également lancer la commande suivante :

```
set SNMP enabled
```

SNMP est le seul protocole qui nécessite une commande d'activation distincte.

5. Enregistrez la configuration :

```
saveconfiguration
```

Configurez les ponts FC-SAS

Avant de câbler votre modèle des ponts FC-SAS, vous devez configurer les paramètres du logiciel FibreBridge.

Avant de commencer

Vous devriez décider si vous allez utiliser la gestion en bande des ponts.



Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Description de la tâche

Si vous utilisez la gestion intrabande du pont plutôt que la gestion IP, les étapes de configuration du port Ethernet et des paramètres IP peuvent être ignorées, comme indiqué dans les étapes correspondantes.

Étapes

1. Configurez le port série console sur ATTO FibreBridge en définissant la vitesse du port sur 115000 bauds :

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Si vous configurez la gestion intrabande, connectez un câble du port série FibreBridge RS-232 au port série (COM) d'un ordinateur personnel.

La connexion série sera utilisée pour la configuration initiale, puis la gestion intrabande via ONTAP et les ports FC peuvent être utilisés pour surveiller et gérer le pont.

3. Si vous configurez pour la gestion IP, connectez le port de gestion Ethernet 1 de chaque pont à votre réseau à l'aide d'un câble Ethernet.

Dans les systèmes exécutant ONTAP 9.5 ou version ultérieure, la gestion intrabande peut être utilisée pour accéder au pont via les ports FC plutôt que par le port Ethernet. Depuis ONTAP 9.8, seule la gestion intrabande est prise en charge et la gestion SNMP est obsolète.

Le port de gestion Ethernet 1 vous permet de télécharger rapidement le micrologiciel de pont (via ATTO ExpressNAV ou des interfaces de gestion FTP) et de récupérer les fichiers principaux et d'extraire les journaux.

4. Si vous configurez pour la gestion IP, configurez le port Ethernet de gestion 1 pour chaque pont en suivant la procédure décrite dans la section 2.0 du Manuel d'installation et d'exploitation *ATTO FibreBridge* pour

votre modèle de pont.

Dans les systèmes exécutant ONTAP 9.5 ou version ultérieure, la gestion intrabande peut être utilisée pour accéder au pont via les ports FC plutôt que par le port Ethernet. Depuis ONTAP 9.8, seule la gestion intrabande est prise en charge et la gestion SNMP est obsolète.

Lors de l'exécution du menu à navigation pour configurer un port de gestion Ethernet, seul le port de gestion Ethernet connecté par le câble Ethernet est configuré. Par exemple, si vous souhaitez également configurer le port Ethernet Management 2, vous devez connecter le câble Ethernet au port 2 et exécuter le menu à navigation rapide.

5. Configurer le pont.

Notez le nom d'utilisateur et le mot de passe que vous désignez.



Ne configurez pas la synchronisation de l'heure sur ATTO FibreBridge 7600N ou 7500N. La synchronisation de l'heure pour ATTO FibreBridge 7600N ou 7500N est définie sur l'heure du cluster après la découverte du pont par ONTAP. Il est également synchronisé périodiquement une fois par jour. Le fuseau horaire utilisé est GMT et n'est pas modifiable.

a. Si vous configurez pour la gestion IP, configurez les paramètres IP du pont.

Dans les systèmes exécutant ONTAP 9.5 ou version ultérieure, la gestion intrabande peut être utilisée pour accéder au pont via les ports FC plutôt que par le port Ethernet. Depuis ONTAP 9.8, seule la gestion intrabande est prise en charge et la gestion SNMP est obsolète.

Pour définir l'adresse IP sans l'utilitaire de navigation rapide, vous devez disposer d'une connexion série à FiberBridge.

Si vous utilisez l'interface de ligne de commandes, vous devez exécuter les commandes suivantes :

```
set ipaddress mp1 ip-address  
  
set ipsubnetmask mp1 subnet-mask  
  
set ipgateway mp1 x.x.x.x  
  
set ipdhcp mp1 disabled  
  
set ethernetspeed mp1 1000
```

b. Configurer le nom du pont.

Les ponts doivent chacun avoir un nom unique dans la configuration MetroCluster.

Exemples de noms de pont pour un groupe de piles sur chaque site :

- Bridge_A_1a
- Bridge_A_1b
- Bridge_B_1a
- Bridge_B_1b

Si vous utilisez l'interface de ligne de commandes, vous devez exécuter la commande suivante :

```
set bridgename <bridge_name>
```

- c. Si vous exécutez ONTAP 9.4 ou une version antérieure, activez SNMP sur le pont :

```
set SNMP enabled
```

Dans les systèmes exécutant ONTAP 9.5 ou version ultérieure, la gestion intrabande peut être utilisée pour accéder au pont via les ports FC plutôt que par le port Ethernet. Depuis ONTAP 9.8, seule la gestion intrabande est prise en charge et la gestion SNMP est obsolète.

6. Configurez les ports FC du pont.

- a. Configurer le débit de données/vitesse des ports FC du pont.

Le débit de données FC pris en charge dépend du pont de votre modèle.

- Le pont FibreBridge 7600N prend en charge jusqu'à 32, 16 ou 8 Gbit/s.
- Le pont FibreBridge 7500N prend en charge jusqu'à 16, 8 ou 4 Gbit/s.



La vitesse FCDataRate que vous sélectionnez est limitée à la vitesse maximale prise en charge par le pont et le port FC du module de contrôleur auquel le port de pont se connecte. Les distances de câblage ne doivent pas dépasser les limites des SFP et autres matériels.

Si vous utilisez l'interface de ligne de commandes, vous devez exécuter la commande suivante :

```
set FCDataRate <port-number> <port-speed>
```

- b. Si vous configurez un pont FibreBridge 7500N, configurez le mode de connexion utilisé par le port sur « ptp ».



Le paramètre FCConnMode n'est pas nécessaire lors de la configuration d'un pont FiberBridge 7600N.

Si vous utilisez l'interface de ligne de commandes, vous devez exécuter la commande suivante :

```
set FCConnMode <port-number> ptp
```

- c. Si vous configurez un pont FiberBridge 7600N ou 7500N, vous devez configurer ou désactiver le port FC2.

- Si vous utilisez le second port, vous devez répéter les sous-étapes précédentes pour le port FC2.
- Si vous n'utilisez pas le second port, vous devez désactiver le port :

```
FCPortDisable <port-number>
```

L'exemple suivant montre la désactivation du port FC 2 :

```
FCPortDisable 2
```

```
Fibre Channel Port 2 has been disabled.
```

- a. Si vous configurez un pont FiberBridge 7600N ou 7500N, désactivez les ports SAS inutilisés :

```
SASPortDisable sas-port
```



Les ports SAS A à D sont activés par défaut. Vous devez désactiver les ports SAS qui ne sont pas utilisés.

Si seul le port SAS A est utilisé, les ports SAS B, C et D doivent être désactivés. L'exemple suivant montre la désactivation du port SAS B. Vous devez également désactiver les ports SAS C et D :

```
SASPortDisable b
```

```
SAS Port B has been disabled.
```

7. Sécuriser l'accès au pont et enregistrer la configuration du pont. Choisissez une option parmi les suivantes en fonction de la version de ONTAP que votre système exécute.

Version ONTAP	Étapes
ONTAP 9.5 ou version ultérieure	a. Afficher l'état des ponts : <pre>storage bridge show</pre> La sortie indique quel pont n'est pas sécurisé. b. Fixer le pont : <pre>securebridge</pre>

ONTAP 9.4 ou version antérieure

a. Afficher l'état des ponts :

```
storage bridge show
```

La sortie indique quel pont n'est pas sécurisé.

b. Vérifier l'état des ports du pont non sécurisé :

```
info
```

La sortie indique l'état des ports Ethernet MP1 et MP2.

c. Si le port Ethernet MP1 est activé, exécutez :

```
set EthernetPort mp1 disabled
```

Si le port Ethernet MP2 est également activé, répétez la sous-étape précédente pour le port MP2.

d. Enregistrez la configuration du pont.

Vous devez exécuter les commandes suivantes :

```
SaveConfiguration
```

```
FirmwareRestart
```

Vous êtes invité à redémarrer le pont.

8. Une fois la configuration MetroCluster terminée, utilisez le `flashimages` Commande pour vérifier votre version du micrologiciel FiberBridge et, si les ponts n'utilisent pas la dernière version prise en charge, mettez à jour le micrologiciel de tous les ponts de la configuration.

"Gérer les composants MetroCluster"

Reliez un pont FibreBridge 7600N ou 7500N aux tiroirs disques à l'aide de modules IOM12

Après avoir configuré le pont, vous pouvez commencer à câbler votre nouveau système.

Description de la tâche

Pour les tiroirs disques, vous insérez un connecteur de câble SAS avec la languette de retrait orientée vers le bas (sous le connecteur).

Étapes

1. Connectez en série les tiroirs disques de chaque pile :
 - a. En commençant par le premier tiroir logique de la pile, connectez le port 3 du module d'E/S au port 1 du module d'E/S sur le tiroir suivant jusqu'à ce que chaque module d'E/S A de la pile soit connecté.
 - b. Répétez la sous-étape précédente pour l'IOM B.
 - c. Répétez les sous-étapes précédentes pour chaque pile.

Le *Guide d'installation et de maintenance* de votre modèle de tiroir disque fournit des informations

détaillées sur la configuration en série des tiroirs disques.

2. Mettez les tiroirs sous tension, puis définissez les ID de tiroir.

- Vous devez mettre chaque tiroir disque hors tension puis sous tension.
- Ils doivent être uniques pour chaque tiroir disque SAS dans chaque groupe DR MetroCluster (y compris les deux sites).

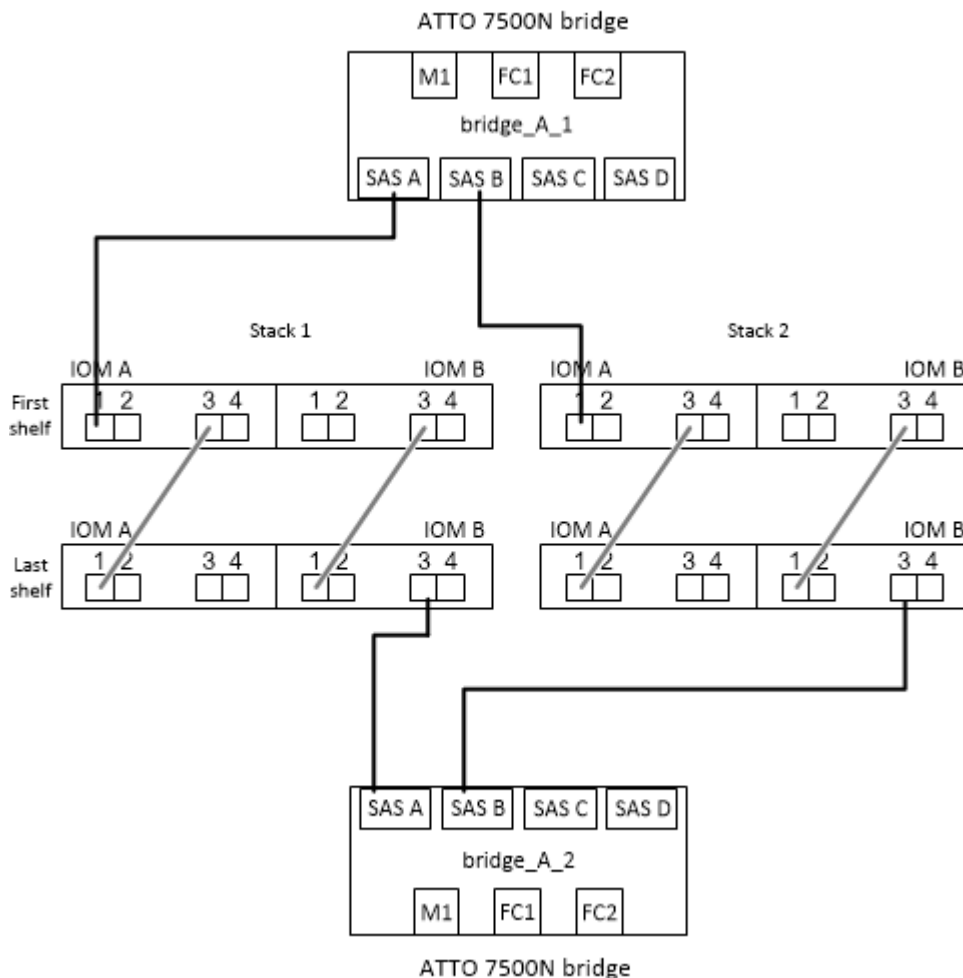
3. Reliez les tiroirs disques aux ponts FiberBridge.

- Pour la première pile de tiroirs disques, reliez le module d'E/S Par câble A du premier tiroir au port SAS A du FibreBridge A, et reliez le module d'E/S par câble B du dernier tiroir au port SAS A du FibreBridge B.
- Pour les piles de tiroirs supplémentaires, répétez l'étape précédente en utilisant le port SAS suivant disponible sur les ponts FiberBridge, en utilisant le port B pour la deuxième pile, le port C pour la troisième pile et le port D pour la quatrième pile.
- Lors du câblage, connectez les piles basées sur les modules IOM12 au même pont à condition qu'elles soient connectées à des ports SAS distincts.



Chaque pile peut utiliser différents modèles d'E/S, mais tous les tiroirs disques d'une pile doivent utiliser le même modèle.

L'illustration suivante montre les tiroirs disques connectés à une paire de ponts FiberBridge 7600N ou 7500N :



Vérifiez la connectivité du pont et connectez les ponts FC à SAS aux ports FC du contrôleur

Vous devez connecter les ponts aux ports FC du contrôleur dans une configuration MetroCluster à deux nœuds connectée par un pont.

Étapes

- 1. Vérifiez que chaque pont peut détecter tous les disques et tiroirs disques auxquels le pont est connecté :

```
sastargets
```

Le `sastargets` le résultat de la commande affiche les périphériques (disques et tiroirs disques) connectés au pont. Les lignes de sortie sont numérotées de façon séquentielle afin que vous puissiez rapidement compter les périphériques.

Le résultat suivant indique que 10 disques sont connectés :

Tgt	VendorID	ProductID	Type	SerialNumber
0	NETAPP	X410_S15K6288A15	DISK	3QP1CLE300009940UHJV
1	NETAPP	X410_S15K6288A15	DISK	3QP1ELF600009940V1BV
2	NETAPP	X410_S15K6288A15	DISK	3QP1G3EW00009940U2M0
3	NETAPP	X410_S15K6288A15	DISK	3QP1EWMP00009940U1X5
4	NETAPP	X410_S15K6288A15	DISK	3QP1FZLE00009940G8YU
5	NETAPP	X410_S15K6288A15	DISK	3QP1FZLF00009940TZKZ
6	NETAPP	X410_S15K6288A15	DISK	3QP1CEB400009939MGXL
7	NETAPP	X410_S15K6288A15	DISK	3QP1G7A900009939FNNTT
8	NETAPP	X410_S15K6288A15	DISK	3QP1FY0T00009940G8PA
9	NETAPP	X410_S15K6288A15	DISK	3QP1FXW600009940VERQ

- 2. Vérifiez que le résultat de la commande indique que le pont est connecté aux disques et tiroirs disques appropriés dans la pile.

Si la sortie est...	Alors...
Exact	Recommencez Étape 1 pour chaque pont restant.
Incorrect	a. Vérifiez que les câbles SAS ne sont pas correctement branchés ou corrigez le câblage SAS en réétiquetage des tiroirs disques aux ponts. Reliez un pont FibreBridge 7600N ou 7500N aux tiroirs disques à l'aide de modules IOM12 b. Recommencez Étape 1 pour chaque pont restant.

- 3. Connectez les câbles de chaque pont aux ports FC du contrôleur :
 - a. Reliez le port FC 1 du pont à un port FC du contrôleur dans `cluster_A`.
 - b. Reliez le port FC 2 du pont à un port FC du contrôleur dans `cluster_B`.
 - Si le contrôleur est configuré avec un adaptateur FC à quatre ports, assurez-vous que les ponts

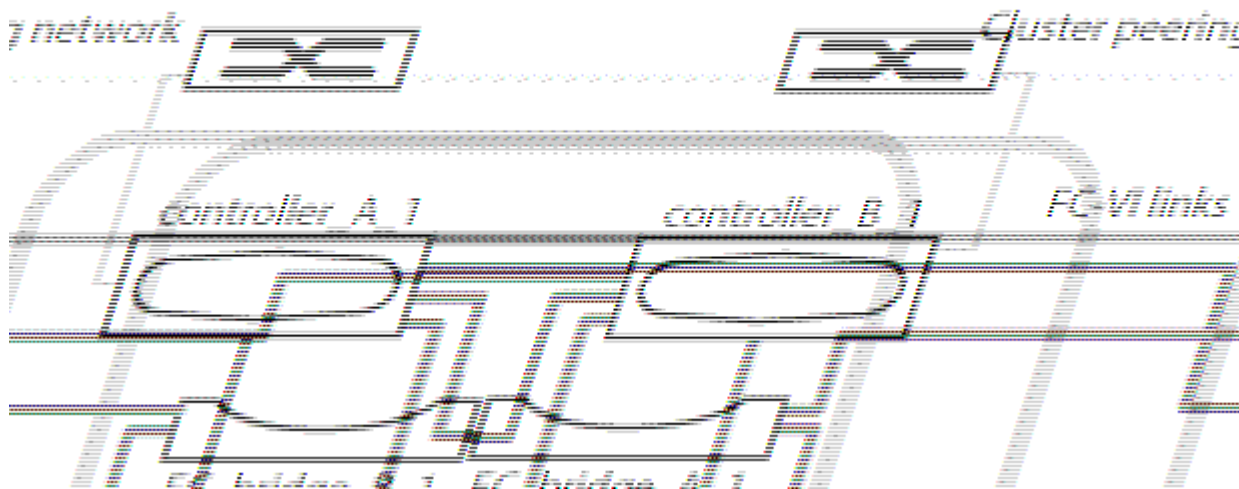
situés à chaque extrémité de la pile de stockage ne sont pas connectés à deux ports FC sur le même ASIC. Par exemple :

- Les ports a et b partagent le même ASIC.
- Les ports c et d partagent le même ASIC.

Dans cet exemple, connectez FC_Bridge_A_1 au port a et FC_Bridge_A2 au port c.

- Si le contrôleur est configuré avec plusieurs adaptateurs FC, ne connectez pas les ponts, de chaque côté de la pile de stockage, au même adaptateur.

Dans ce scénario, vous devez connecter FC_Bridge_A_1 à un port FC intégré et connecter FC_Bridge_A_2 à un port FC d'un adaptateur situé dans un slot d'extension.



4. Recommencez [Étape 3](#) sur les autres ponts jusqu'à ce que tous les ponts aient été câblés.

Fixez ou défixez le pont FibreBridge

Pour désactiver facilement les protocoles Ethernet potentiellement non sécurisés sur un pont, à partir de ONTAP 9.5, vous pouvez sécuriser le pont. Ceci désactive les ports Ethernet du pont. Vous pouvez également réactiver l'accès Ethernet.

Description de la tâche

- La sécurisation du pont désactive les protocoles et services Telnet et d'autres ports IP (FTP, ExpressNAV, ICMP ou Quickmenu) sur le pont.
- Cette procédure utilise la gestion hors bande à l'aide de l'invite ONTAP, disponible à partir de ONTAP 9.5.

Vous pouvez lancer les commandes à partir de la CLI de pont si vous n'utilisez pas la gestion hors bande.

- Le `unsecurebridge` La commande peut être utilisée pour réactiver les ports Ethernet.
- Dans ONTAP 9.7 et versions antérieures, exécutant le `securebridge` Il se peut que la commande ATTO FibreBridge ne mette pas à jour correctement l'état du pont sur le cluster partenaire. Dans ce cas, exécutez le `securebridge` commande provenant du cluster partenaire.



Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Étapes

1. Dans l'invite ONTAP du cluster contenant le pont, sécuriser ou désécuriser le pont.

- La commande suivante sécurise Bridge_A_1 :

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
```

- La commande suivante désécurise Bridge_A_1 :

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. Dans l'invite ONTAP du cluster contenant le pont, enregistrez la configuration du pont :

```
storage bridge run-cli -bridge <bridge-name> -command saveconfiguration
```

La commande suivante sécurise Bridge_A_1 :

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command  
saveconfiguration
```

3. Dans l'invite ONTAP du cluster contenant le pont, redémarrez le firmware du pont :

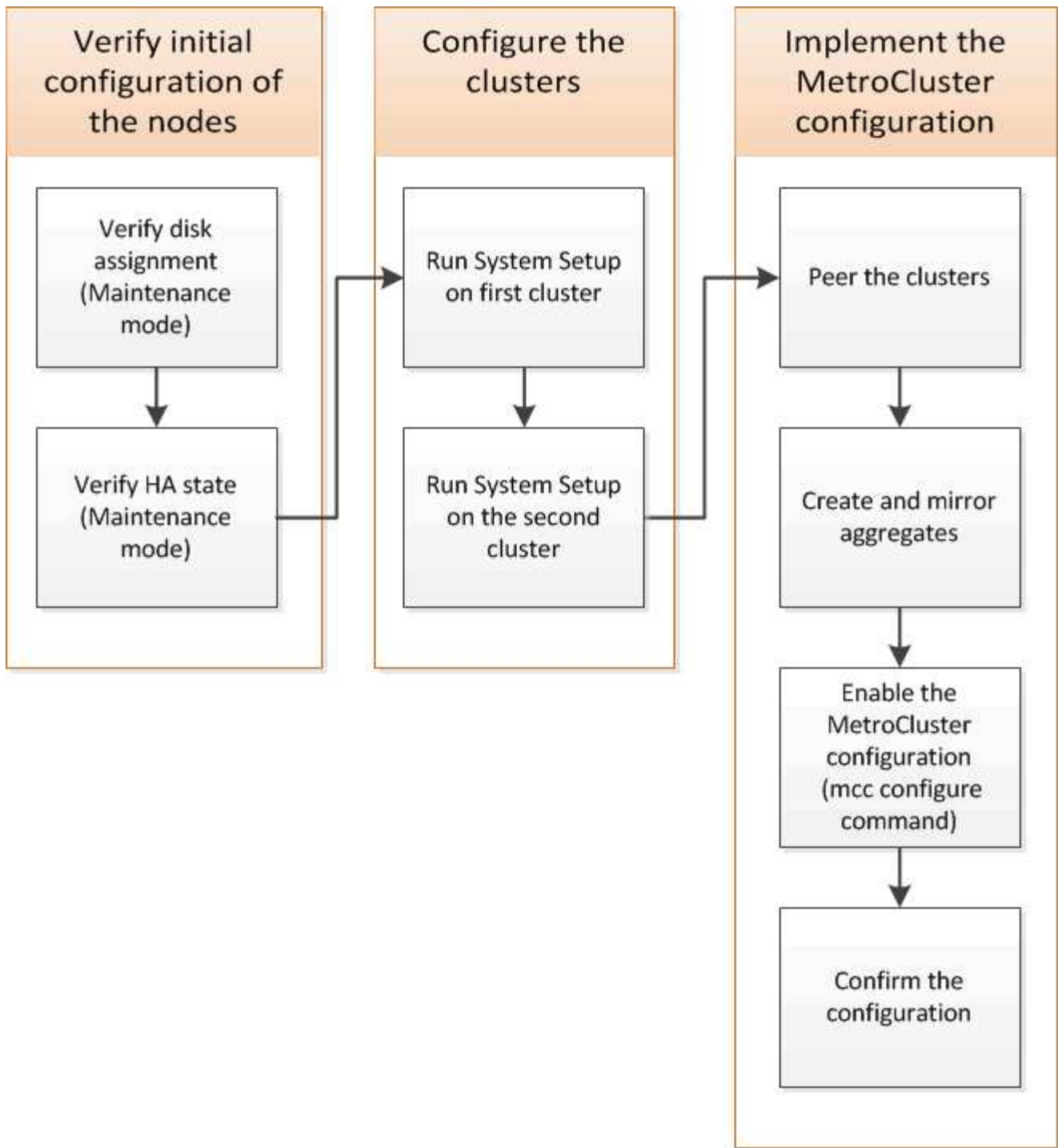
```
storage bridge run-cli -bridge <bridge-name> -command firmwarerestart
```

La commande suivante sécurise Bridge_A_1 :

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```

Configuration du logiciel MetroCluster dans ONTAP

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.



Étapes

1. Collectez les adresses IP requises pour les modules de contrôleur avant de commencer le processus de configuration.
2. Complétez la fiche d'informations sur le réseau IP pour le site A.

Fiche d'informations sur le réseau IP pour le site A

Avant de configurer le système, vous devez obtenir des adresses IP et d'autres informations réseau pour le premier site MetroCluster (site A) de votre administrateur réseau.

Informations de création du site À partir d'un cluster

Lors de la création du cluster, vous avez besoin des informations suivantes :

Type d'information	Vos valeurs
Nom du cluster. Exemple utilisé dans cette information : site_A	
Domaine DNS	
Serveurs de noms DNS	
Emplacement	
Mot de passe administrateur	

Information sur un nœud du site

Vous avez besoin d'une adresse IP de gestion, d'un masque de réseau et d'une passerelle par défaut pour chaque nœud du cluster.

Nœud	Port	Adresse IP	Masque de réseau	Passerelle par défaut
Nœud 1. Exemple utilisé dans ces informations : Controller_A_1				
Nœud 2. Non requis si vous utilisez une configuration MetroCluster à deux nœuds (un nœud sur chaque site). Exemple utilisé dans ces informations : Controller_A_2				

Site A LIFs et ports pour le peering de cluster

Pour chaque nœud du cluster, vous devez disposer des adresses IP de deux LIF intercluster, y compris un masque de réseau et une passerelle par défaut. Les LIFs intercluster sont utilisés pour mutualiser les clusters.

Nœud	Port	Adresse IP du LIF intercluster	Masque de réseau	Passerelle par défaut
IC node 1 LIF 1				

Nœud 1 ci LIF 2				
-----------------	--	--	--	--

Informations sur le serveur de temps du site A.

Vous devez synchroniser l'heure, qui nécessite un ou plusieurs serveurs de temps NTP.

Nœud	Nom d'hôte	Adresse IP	Masque de réseau	Passerelle par défaut
Serveur NTP 1				
Serveur NTP 2				

Site A nbsp; informations AutoSupport

Vous devez configurer le AutoSupport sur chaque nœud, qui nécessite les informations suivantes :

Type d'information	Vos valeurs	
De l'adresse e-mail		Hôtes de messagerie
Noms ou adresses IP		Protocole de transport
HTTP, HTTPS OU SMTP		Serveur proxy
	Adresses e-mail ou listes de distribution du destinataire	Messages longs
	Messages concis	

Site A informations sur le processeur de service

Vous devez activer l'accès au processeur de service de chaque nœud pour le dépannage et la maintenance. Pour ce faire, les informations réseau suivantes sont nécessaires pour chaque nœud :

Nœud	Adresse IP	Masque de réseau	Passerelle par défaut
Nœud 1			

Fiche d'informations sur le réseau IP pour le site B

Avant de configurer le système, vous devez obtenir des adresses IP et d'autres informations réseau pour le second site MetroCluster (site B) de votre administrateur réseau.

Informations de création de cluster du site B

Lors de la création du cluster, vous avez besoin des informations suivantes :

Type d'information	Vos valeurs
Nom du cluster. Exemple utilisé dans cette information : site_B	
Domaine DNS	
Serveurs de noms DNS	
Emplacement	
Mot de passe administrateur	

Informations sur le nœud du site B.

Vous avez besoin d'une adresse IP de gestion, d'un masque de réseau et d'une passerelle par défaut pour chaque nœud du cluster.

Nœud	Port	Adresse IP	Masque de réseau	Passerelle par défaut
Nœud 1. Exemple utilisé dans ces informations : Controller_B_1				
Nœud 2. Non requis pour les configurations MetroCluster à deux nœuds (un nœud sur chaque site). Exemple utilisé dans ces informations : Controller_B_2				

Les LIF du site B et les ports pour le peering de clusters

Pour chaque nœud du cluster, vous devez disposer des adresses IP de deux LIF intercluster, y compris un masque de réseau et une passerelle par défaut. Les LIFs intercluster sont utilisés pour mutualiser les clusters.

Nœud	Port	Adresse IP du LIF intercluster	Masque de réseau	Passerelle par défaut
IC node 1 LIF 1				
Nœud 1 ci LIF 2				

Informations sur le serveur de temps du site B.

Vous devez synchroniser l'heure, qui nécessite un ou plusieurs serveurs de temps NTP.

Nœud	Nom d'hôte	Adresse IP	Masque de réseau	Passerelle par défaut
Serveur NTP 1				
Serveur NTP 2				

Site B nbsp; informations AutoSupport

Vous devez configurer le AutoSupport sur chaque nœud, qui nécessite les informations suivantes :

Type d'information	Vos valeurs	
De l'adresse e-mail		Hôtes de messagerie
Noms ou adresses IP		Protocole de transport
HTTP, HTTPS OU SMTP		Serveur proxy
	Adresses e-mail ou listes de distribution du destinataire	Messages longs
	Messages concis	

Site B nbsp; informations SP

Vous devez activer l'accès au processeur de service de chaque nœud pour le dépannage et la maintenance. Pour ce faire, vous devez disposer des informations réseau suivantes pour chaque nœud :

Nœud	Adresse IP	Masque de réseau	Passerelle par défaut
Nœud 1 (contrôleur_B_1)			

Similarités et différences entre les configurations cluster standard 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.

Restauration des paramètres par défaut du système et configuration du type de HBA sur un module de contrôleur

Pour garantir la réussite de l'installation de MetroCluster, réinitialisez et restaurez les valeurs par défaut sur les modules de contrôleur.

Important

Cette tâche n'est requise que pour les configurations étendues utilisant des ponts FC-SAS.

Étapes

1. Dans l'invite DU CHARGEUR, renvoie les variables environnementales à leur paramètre par défaut :

```
set-defaults
```

2. Démarrer le nœud en mode Maintenance, puis configurer les paramètres des HBA du système :

- a. Démarrage en mode maintenance :

```
boot_ontap maint
```

- b. Vérifiez les paramètres actuels des ports :

```
ucadmin show
```

- c. Mettez à jour les paramètres de port selon vos besoins.

Si vous disposez de ce type de HBA et du mode souhaité...	Utilisez cette commande...
FC CNA	<code>ucadmin modify -m fc -t initiator adapter_name</code>
Ethernet CNA	<code>ucadmin modify -mode cna adapter_name</code>

Cible FC	<code>fcadmin config -t target <i>adapter_name</i></code>
Initiateur FC	<code>fcadmin config -t initiator <i>adapter_name</i></code>

3. Quitter le mode Maintenance :

```
halt
```

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

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

```
boot_ontap maint
```

5. Vérifiez les modifications que vous avez effectuées :

Si vous disposez de ce type de HBA...	Utilisez cette commande...
CNA	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

6. Quitter le mode Maintenance :

```
halt
```

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

7. Démarrez le nœud sur le menu de démarrage :

```
boot_ontap menu
```

Une fois que vous avez exécuté la commande, attendez que le menu de démarrage s'affiche.

8. Effacez la configuration du nœud en tapant « wipconconfig » 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.

Configuration des ports FC-VI sur une carte X1132A-R6 à quatre ports sur les systèmes FAS8020

Si vous utilisez la carte X1132A-R6 à quatre ports sur un système FAS8020, vous pouvez passer en mode de maintenance pour configurer les ports 1a et 1b pour FC-VI et pour l'utilisation d'un initiateur. Cela n'est pas nécessaire pour les systèmes MetroCluster reçus en usine, dans lesquels les ports sont configurés de façon appropriée pour votre configuration.

Description de la tâche

Cette tâche doit être effectuée en mode Maintenance.



La conversion d'un port FC en port FC-VI avec la commande `ucadmin` n'est prise en charge que sur les systèmes FAS8020 et AFF 8020. La conversion de ports FC en ports FCVI n'est pas prise en charge sur toute autre plateforme.

Étapes

1. Désactiver les ports :

```
storage disable adapter 1a
```

```
storage disable adapter 1b
```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Vérifiez que les ports sont désactivés :

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
...					
1a	fc	initiator	-	-	offline
1b	fc	initiator	-	-	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

3. Définir les ports a et b en mode FC-VI :

```
ucadmin modify -adapter 1a -type fcvi
```

La commande définit le mode sur les deux ports de la paire de ports 1a et 1b (même si seul 1a est spécifié dans la commande).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. Vérifiez que la modification est en attente :

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
...					
1a	fc	initiator	-	fcvi	offline
1b	fc	initiator	-	fcvi	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

5. Arrêter le contrôleur, puis redémarrer en mode maintenance.

6. Confirmer le changement de configuration :

```
ucadmin show local
```

Node	Adapter	Mode	Type	Mode	Type	Status
...						
controller_B_1	1a	fc	fcvi	-	-	online
controller_B_1	1b	fc	fcvi	-	-	online
controller_B_1	1c	fc	initiator	-	-	online
controller_B_1	1d	fc	initiator	-	-	online

6 entries were displayed.

Vérification de l'affectation du disque en mode maintenance dans une configuration à deux nœuds

Avant de démarrer entièrement le système sur ONTAP, vous pouvez également démarrer le système en mode maintenance et vérifier l'affectation des disques sur les nœuds. Il convient d'attribuer aux disques pour créer une configuration entièrement symétrique avec les deux sites possédant leurs propres tiroirs disques et servant les données, où chaque nœud et chaque pool disposent d'un nombre égal de disques en miroir qui leur sont affectés.

Avant de commencer

Le système doit être en mode Maintenance.

Description de la tâche

Les attributions de disques des nouveaux systèmes MetroCluster sont réalisées avant l'expédition.

Le tableau suivant présente des exemples d'affectations de pools pour une configuration MetroCluster. Les disques sont affectés à des pools par tiroir.

Tiroir disque (<i>exemple name</i>)...	Sur le site...	Appartient à...	Et est attribué à ce nœud...
Tiroir disque 1 (tiroir_A_1_1)	Site A	Nœud A 1	Pool 0
Tiroir disque 2 (tiroir_A_1_3)	Tiroir disque 3 (tiroir_B_1_1)	Nœud B 1	Piscine 1
Tiroir disque 4 (tiroir_B_1_3)	Tiroir disque 9 (tiroir_B_1_2)	Site B	Nœud B 1
Pool 0	Tiroir disque 10 (tiroir_B_1_4)	Tiroir disque 11 (tiroir_A_1_2)	Nœud A 1

Si votre configuration inclut des tiroirs disques DS460C, il est conseillé d'attribuer manuellement les disques en suivant les instructions suivantes pour chaque tiroir 12 disques :

Affectez ces disques dans le tiroir...	À ce nœud et pool...
1 - 6	Pool du nœud local 0
7 - 12	Pool du partenaire de reprise après incident 1

Ce modèle d'affectation des disques minimise l'effet sur un agrégat en cas de mise hors ligne d'un tiroir.

Étapes

1. Si vous avez reçu l'usine de votre système, confirmez les attributions de tiroirs :

```
disk show -v
```

2. Si nécessaire, vous pouvez explicitement attribuer des disques aux tiroirs disques connectés au pool approprié

```
disk assign
```

Les tiroirs disques du même site que le nœud sont affectés au pool 0 et les tiroirs disques situés sur le site partenaire sont affectés au pool 1. Vous devez affecter un nombre égal de tiroirs à chaque pool.

- a. Si ce n'est pas le cas, démarrez chaque système en mode maintenance.
- b. Sur le nœud du site A, attribuer systématiquement les tiroirs disques locaux à pool 0 et les tiroirs disques distants à pool 1:

```
disk assign -shelf disk_shelf_name -p pool
```

Si le contrôleur de stockage node_A_1 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

- c. Sur le nœud du site distant (site B), attribuer systématiquement ses tiroirs disques locaux à Pool 0 et ses tiroirs disques distants à pool 1:

```
disk assign -shelf disk_shelf_name -p pool
```

Si le contrôleur de stockage node_B_1 dispose de quatre tiroirs, vous exécutez les commandes suivantes :

```
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
```

- a. Affiche les ID de tiroir disque et les baies pour chaque disque :

```
disk show -v
```

Vérification de l'état des composants HA

Dans une configuration MetroCluster étendue qui n'est pas préconfigurée en usine, vous devez vérifier que l'état HA du contrôleur et du composant de châssis est défini sur « `mcc-2n` » pour qu'ils s'démarrent correctement. Pour les systèmes reçus en usine, cette valeur est préconfigurée et vous n'avez pas besoin de la vérifier.

Avant de commencer

Le système doit être en mode Maintenance.

Étapes

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

```
ha-config show
```

Le module de contrôleur et le châssis doivent indiquer la valeur "mcc-2n".

2. Si l'état système affiché du contrôleur n'est pas « `mcc-2n` », définissez l'état HA du contrôleur :

```
ha-config modify controller mcc-2n
```

3. Si l'état système affiché du châssis n'est pas "mcc-2n", définissez l'état HA du châssis :

```
ha-config modify chassis mcc-2n
```

Arrêtez le nœud.

Attendez que le nœud soit de nouveau à l'invite DU CHARGEUR.

4. Répétez cette procédure sur chaque nœud de la configuration MetroCluster.

Configuration d'ONTAP dans une configuration MetroCluster à deux nœuds

Dans une configuration MetroCluster à deux nœuds, sur chaque cluster, vous devez démarrer le nœud, quitter l'assistant de configuration du cluster et utiliser `cluster setup` commande permettant de configurer le nœud dans un cluster à un seul nœud.

Avant de commencer

Vous ne devez pas avoir configuré le processeur de service.

Description de la tâche

Cette tâche est destinée aux configurations MetroCluster à deux nœuds qui utilisent un stockage NetApp natif.

Cette tâche doit être effectuée sur les deux clusters en configuration MetroCluster.

Pour obtenir des informations plus générales sur la configuration de ONTAP, reportez-vous au ["Configuration ONTAP"](#)

Étapes

1. Mettez le premier nœud sous tension.



Vous devez répéter cette étape sur le nœud sur le site de reprise d'activité.

Le nœud démarre, puis l'assistant de configuration du cluster démarre sur la console vous informant que AutoSupport sera activé automatiquement.

```
::> Welcome to the cluster setup wizard.
```

You can enter the following commands at any time:

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.
```

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
<http://support.netapp.com/autosupport/>

```
Type yes to confirm and continue {yes}: yes
```

```
Enter the node management interface port [e0M]:
```

```
Enter the node management interface IP address [10.101.01.01]:
```

```
Enter the node management interface netmask [101.010.101.0]:
```

```
Enter the node management interface default gateway [10.101.01.0]:
```

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

2. Créez un nouveau cluster :

```
create
```

3. Indiquez si le nœud doit être utilisé comme un cluster à un seul nœud.

```
Do you intend for this node to be used as a single node cluster? {yes,  
no} [yes]:
```

4. Acceptez les valeurs par défaut du système « oui » en appuyant sur entrée ou entrez vos propres valeurs

en tapant « non », puis en appuyant sur entrée.

5. Suivez les invites pour compléter l'assistant **Cluster Setup**, en appuyant sur entrée pour accepter les valeurs par défaut ou en saisissant vos propres valeurs, puis en appuyant sur entrée.

Les valeurs par défaut sont déterminées automatiquement en fonction de votre plate-forme et de votre configuration réseau.

6. Une fois l'assistant **Cluster Setup** terminé et qu'il quitte, vérifiez que le cluster est actif et que le premier nœud fonctionne correctement :

```
cluster show
```

L'exemple suivant montre un cluster dans lequel le premier nœud (cluster 1-01) est sain et peut participer :

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
cluster1-01                        true    true
```

S'il est nécessaire de modifier les paramètres que vous avez saisis pour le SVM admin ou le SVM node, vous pouvez accéder à l'assistant **Cluster Setup** en utilisant le `cluster setup` commande.

Configuration des clusters dans une configuration 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.

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

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 dans « cluster01 » :

```
cluster01::> network port show
```

(Mbps)							Speed
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 à des LIF :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port

Cluster cluster01-01_clus1  e0a      e0a
Cluster cluster01-01_clus2  e0b      e0b
Cluster cluster01-02_clus1  e0a      e0a
Cluster cluster01-02_clus2  e0b      e0b
cluster01
    cluster_mgmt            e0c      e0c
cluster01
    cluster01-01_mgmt1      e0c      e0c
cluster01
    cluster01-02_mgmt1      e0c      e0c
```

3. Créer un failover group pour les ports dédiés :

```
network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical_or_logical_ports
```

L'exemple suivant attribue les ports « e0e » et « e0f » au groupe de basculement « Intercluster01 » sur le SVM système « cluster01 » :

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

```
network interface failover-groups show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster01-01:e0a, cluster01-01:e0b, cluster01-02:e0a, cluster01-02:e0b
cluster01	Default	cluster01-01:e0c, cluster01-01:e0d, cluster01-02:e0c, cluster01-02:e0d, cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f
	intercluster01	cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

Version ONTAP	Commande
ONTAP 9.6 et versions ultérieures	network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask -failover-group failover_group
ONTAP 9.5 et versions antérieures	network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » dans le groupe de basculement « intercluster01 » :

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. Vérifier que les LIFs intercluster ont été créés :

Version ONTAP	Commande
ONTAP 9.6 et versions ultérieures	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9.5 et versions antérieures	<code>network interface show -role intercluster</code>

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
Home				Port
-----	-----	-----	-----	-----
-----	-----			
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 :

Version ONTAP	Commande
---------------	----------

ONTAP 9.6 et versions ultérieures	<code>network interface show -service-policy default-intercluster -failover</code>
Dans ONTAP 9.5 et versions antérieures	<code>network interface show -role intercluster -failover</code>

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant montre que les LIFs intercluster « `cluster01_icl01` » et « `cluster01_icl02` » sur le port SVM « `e0e` » basculeront vers le port « `e0f` ».

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

	Logical	Home	Failover	Failover
Vserver	Interface	Node:Port	Policy	Group
cluster01				
	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01				
		Failover Targets:	cluster01-01:e0e,	
			cluster01-01:e0f	
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01				
		Failover Targets:	cluster01-02:e0e,	
			cluster01-02:e0f	

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 dans « `cluster01` » :


```
cluster01::> network port show
```

(Mbps)						Speed
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 :

Version ONTAP	Commande
ONTAP 9.6 et versions ultérieures	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service-policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
ONTAP 9.5 et versions antérieures	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée les LIFs intercluster « cluster01_icl01 » et « cluster01_icl02 » :

```
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 :

Version ONTAP	Commande
ONTAP 9.6 et versions ultérieures	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9.5 et versions antérieures	<code>network interface show -role intercluster</code>

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 :

Version ONTAP	Commande
ONTAP 9.6 et versions ultérieures	<code>network interface show -service-policy default-intercluster -failover</code>
ONTAP 9.5 et versions antérieures	<code>network interface show -role intercluster -failover</code>

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
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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 devez créer la relation entre clusters MetroCluster.

Création d'une relation entre clusters

Vous pouvez utiliser le `cluster peer create` commande permettant de 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.

Avant de commencer

- 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-addr peer_LIF_IPs -ipspace ipspace
```

Si vous spécifiez les deux `-generate-passphrase` et `-peer-addr`, Uniquement le cluster dont les LIFs intercluster sont spécifiés dans `-peer-addr` 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-addr peer_LIF_IPs -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-addr
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
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default

```

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 d'une relation de cluster peer-to-peer (ONTAP 9.2 et versions antérieures)

Vous pouvez utiliser le `cluster peer create` commande permettant de lancer une demande de relation de peering entre un cluster local et distant. Une fois la relation homologue demandée par le cluster local, vous

pouvez l'exécuter `cluster peer create` sur le cluster distant pour accepter la relation.

Avant de commencer

- Vous devez avoir créé des LIFs intercluster sur chaque nœud des clusters en cours de peering.
- Les administrateurs du cluster doivent avoir accepté la phrase de passe que chaque cluster utilisera pour s'authentifier auprès de l'autre.

Étapes

1. Sur le cluster cible de protection des données, créez une relation de pairs avec le cluster source de protection des données :

```
cluster peer create -peer-addr peer_LIF_IPs -ip-space ip-space
```

Vous pouvez ignorer `-ip-space` 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 avec le cluster distant aux adresses IP LIF intercluster 192.168.2.201 et 192.168.2.202 :

```
cluster02::> cluster peer create -peer-addr 192.168.2.201,192.168.2.202
Enter the passphrase:
Please enter the passphrase again:
```

Entrez la phrase de passe de la relation homologue lorsque vous y êtes invité.

2. Sur le cluster source de protection des données, authentifiez le cluster source sur le cluster destination :

```
cluster peer create -peer-addr peer_LIF_IPs -ip-space ip-space
```

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 192.140.112.203 et 192.140.112.204 de LIF intercluster :

```
cluster01::> cluster peer create -peer-addr 192.168.2.203,192.168.2.204
Please confirm the passphrase:
Please confirm the passphrase again:
```

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
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. Vérifier la connectivité et l'état des nœuds de la relation peer-to-peer :

```
cluster peer health show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
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	

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"](#)

["Concepts relatifs à ONTAP"](#)

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.

Avant de commencer

- 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.

Description de la tâche

- 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"](#)

- 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 des disques avec différents RPM sont autorisés pour plus d'informations sur ces options, reportez-vous à la section `storage aggregate create` page de manuel.

La commande suivante crée un agrégat en miroir avec 10 disques :

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Vérifier le groupe RAID et les disques de votre nouvel agrégat :

```
storage aggregate show-status -aggregate aggregate-name
```

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.

Avant de commencer

- 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 pouvez vérifier que le type de disque approprié est sélectionné.

Exemple 1. Description de la tâche

ATTENTION : dans les configurations FC MetroCluster, les agrégats non mis en miroir ne seront en ligne qu'après un basculement si les disques distants de l'agrégat sont accessibles. En cas de panne de liens ISL, le nœud local risque de ne pas pouvoir accéder aux données dans les disques distants sans mise en miroir. La défaillance d'un agrégat peut entraîner le redémarrage du nœud local.



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.
- Le "[Gestion des disques et des agrégats](#)" contient plus d'informations sur la mise en miroir des agrégats.

Étapes

1. Afficher la liste des pièces de rechange disponibles :

```
storage disk show -spare -owner node_name
```

2. Créer l'agrégat :

```
storage aggregate create
```

Si vous êtes connecté au cluster depuis l'interface de gestion du cluster, vous pouvez créer un agrégat sur n'importe quel nœud du cluster. Pour vérifier que l'agrégat est créé sur un nœud spécifique, il est important d'utiliser le `-node` paramètre ou spécifiez les disques qui sont détenus par ce nœud.

Vous 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
- Si des disques avec différents RPM sont autorisés pour plus d'informations sur ces options, reportez-vous à la section `storage aggregate create` page de manuel.

La commande suivante crée un agrégat sans mise en miroir avec 10 disques :

```

controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE

```

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.

Avant de commencer

- Chaque cluster doit contenir au moins deux agrégats de données en miroir non racines.

Les agrégats de données supplémentaires peuvent être mis en miroir ou non.

Vérifier les types d'agrégats :

```
storage aggregate show
```



Si vous souhaitez utiliser un seul agrégat de données en miroir, reportez-vous à la section ["Configurer le logiciel MCC dans ONTAP"](#) pour obtenir des instructions.

- L'état ha-config des contrôleurs et du châssis doit être "mcc-2n".

Description de la tâche

Vous pouvez lancer le `metrocluster configure` Commande unique, sur l'un des nœuds, 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.

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 : <code>metrocluster configure node-name</code>

Un seul agrégat de données en miroir	a. Depuis l'invite de n'importe quel nœud, passez au niveau de privilège avancé : <pre>set -privilege advanced</pre> Vous devez répondre par « y » lorsque vous êtes invité à continuer en mode avancé et que vous voyez l'invite du mode avancé (*>). b. Configurez le MetroCluster avec le <code>-allow-with-one-aggregate true</code> paramètre : <pre>metrocluster configure -allow-with-one-aggregate true node-name</pre> c. Revenir au niveau de privilège admin : <pre>set -privilege admin</pre>
--------------------------------------	--



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 la configuration de 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 :

```
cluster_A::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) 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

```
7 entries were displayed.
```

3. Vérifier la configuration MetroCluster des deux sites de la configuration MetroCluster.

a. Vérifier la configuration à partir du site A :

```
metrocluster show
```

```
cluster_A::> metrocluster show
```

Cluster	Entry Name	State

Local: cluster_A	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		
Remote: cluster_B	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		

b. Vérifier la configuration à partir du site B :

```
metrocluster show
```

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

Configuration de ponts FC-SAS pour le contrôle de l'état du système

Dans les systèmes exécutant des versions ONTAP antérieures à 9.8, si votre configuration inclut des ponts FC-SAS, vous devez effectuer quelques étapes de configuration spéciales pour surveiller les ponts FC-SAS dans la configuration MetroCluster.

- Les outils de surveillance SNMP tiers ne sont pas pris en charge pour les ponts FiberBridge.
- Depuis la version ONTAP 9.8, les ponts FC-SAS sont surveillés par défaut via des connexions intrabande, ce qui n'est pas nécessaire.



Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Étapes

1. Dans l'invite de cluster ONTAP, ajoutez le pont au contrôle de l'état de santé :
 - a. Ajoutez le pont à l'aide de la commande pour votre version de ONTAP :

Version ONTAP	Commande
ONTAP 9.5 et versions ultérieures	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>
ONTAP 9.4 et versions antérieures	<code>storage bridge add -address <i>bridge-ip-address</i> -name <i>bridge-name</i></code>

- b. Vérifiez que le pont a été ajouté et est correctement configuré :

```
storage bridge show
```

Il peut s'avérer nécessaire de prendre jusqu'à 15 minutes pour refléter toutes les données à cause de l'intervalle d'interrogation. Le moniteur d'intégrité ONTAP peut contacter et surveiller le pont si la valeur de la colonne "état" est ""ok"" et si d'autres informations, telles que le nom mondial (WWN), sont affichées.

L'exemple suivant montre que les ponts FC-SAS sont configurés :

```
controller_A_1:> storage bridge show
```

Bridge Model	Symbolic Name	Is Monitored	Monitor Status	Vendor
	Bridge WWN			
ATTO_10.10.20.10	atto01	true	ok	Atto
FibreBridge 7500N	20000010867038c0			
ATTO_10.10.20.11	atto02	true	ok	Atto
FibreBridge 7500N	20000010867033c0			
ATTO_10.10.20.12	atto03	true	ok	Atto
FibreBridge 7500N	20000010867030c0			
ATTO_10.10.20.13	atto04	true	ok	Atto
FibreBridge 7500N	2000001086703b80			

```
4 entries were displayed
```

```
controller_A_1:>
```

Vérification de la configuration MetroCluster

Vous pouvez vérifier que les composants et les relations de la configuration MetroCluster fonctionnent correctement. Vous devez effectuer un contrôle après la configuration initiale et après avoir apporté des modifications à la configuration MetroCluster. Vous devez également effectuer une vérification avant le basculement (prévu) ou le rétablissement.

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.

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. Afficher des résultats plus détaillés :

```
metrocluster check run
```

```
metrocluster check aggregate show
```

```
metrocluster check cluster show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

Le `metrocluster check show` les commandes affichent les résultats des plus récentes `metrocluster check run` commande. Vous devez toujours exécuter le `metrocluster check run` avant d'utiliser le `metrocluster check show` commandes de manière à ce que les informations affichées soient à jour.

L'exemple suivant montre le `metrocluster check aggregate show` Résultat de la commande pour une configuration MetroCluster à quatre nœuds saine :

```
cluster_A:> metrocluster check aggregate show
```

```
Last Checked On: 8/5/2014 00:42:58
```

Node	Aggregate	Check
Result		
-----	-----	-----
controller_A_1	controller_A_1_aggr0	mirroring-status
ok		disk-pool-allocation


```

ok
ownership-state
ok
controller_A_1_aggr1
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_1_aggr2
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2      controller_A_2_aggr0
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2_aggr1
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2_aggr2
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
18 entries were displayed.

```

L'exemple suivant montre le `metrocluster check cluster show` Résultat de la commande pour une configuration MetroCluster à quatre nœuds saine. Il indique que les clusters sont prêts à effectuer un basculement négocié si nécessaire.

Last Checked On: 9/13/2017 20:47:04

Cluster	Check	Result
mccint-fas9000-0102	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok
mccint-fas9000-0304	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok

10 entries were displayed.

Informations associées

["Gestion des disques et des agrégats"](#)

["Gestion du réseau et des LIF"](#)

Vérification des erreurs de configuration MetroCluster avec Config Advisor

Vous pouvez accéder au site de support NetApp et télécharger l'outil Config Advisor pour vérifier les erreurs de configuration courantes.

Config Advisor est un outil de validation de la configuration et de vérification de l'état de santé. Vous pouvez le déployer sur des sites sécurisés et sur des sites non sécurisés à des fins de collecte des données et d'analyse du système.



Le support pour Config Advisor est limité et n'est disponible qu'en ligne.

1. Accédez à la page de téléchargement Config Advisor et téléchargez l'outil.

["Téléchargement NetApp : Config Advisor"](#)

2. Exécutez Config Advisor, examinez les résultats de l'outil et suivez les recommandations du produit pour résoudre tous les problèmes détectés.

Vérification du basculement, de la résolution et du rétablissement

Il est recommandé de vérifier les opérations de basculement, de rétablissement et de rétablissement de la configuration MetroCluster.

1. Utilisez les procédures de basculement négocié, de rétablissement et de rétablissement mentionnées dans le ["Effectuez les opérations de basculement, de rétablissement et de rétablissement"](#).

Protection des fichiers de sauvegarde de configuration

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.

1. Définissez l'URL de la destination distante pour les fichiers de sauvegarde de configuration :

```
system configuration backup settings modify URL-of-destination
```

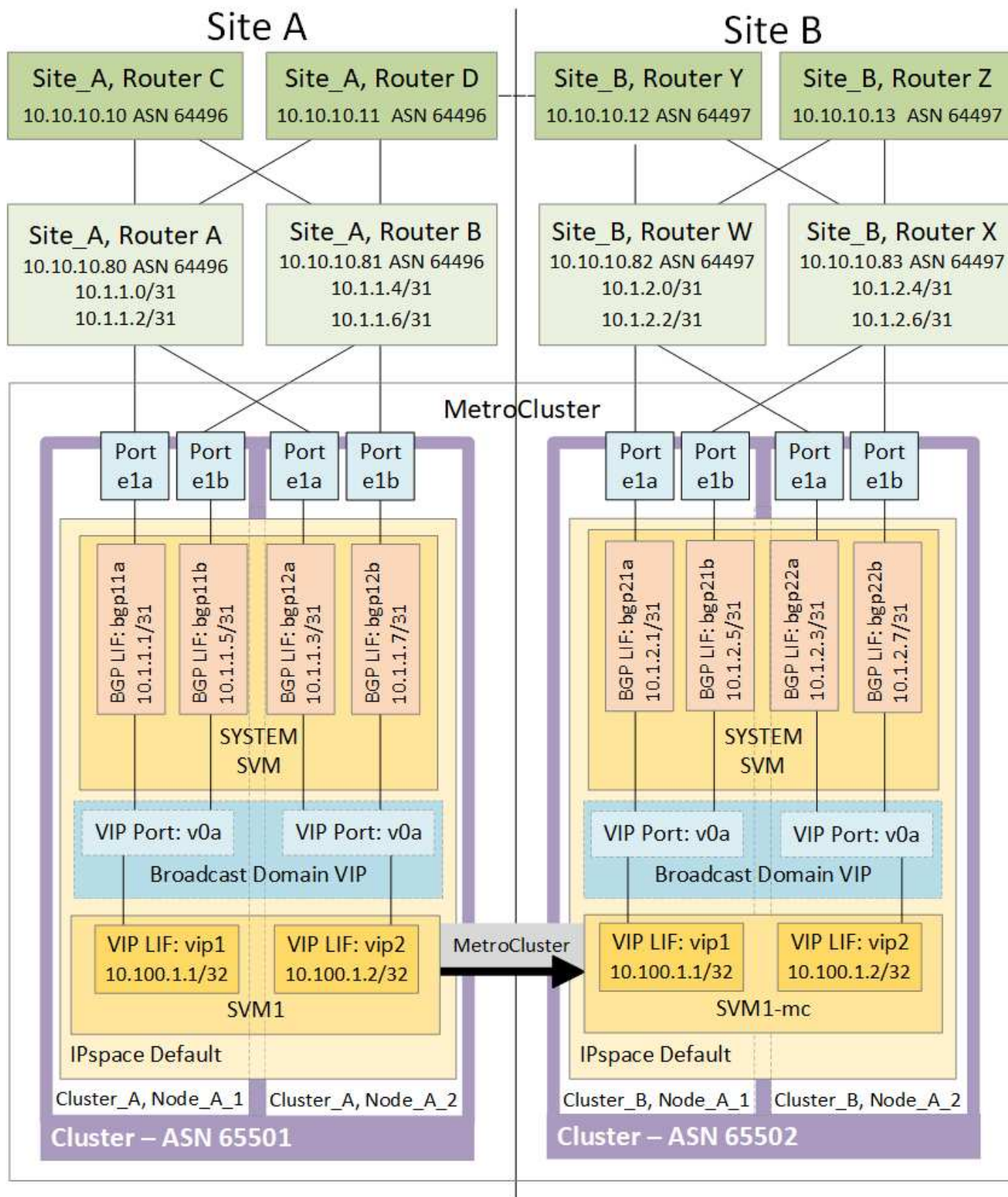
Le ["Gestion du cluster via l'interface de ligne de commandes"](#) Contient des informations supplémentaires sous la section *gestion des sauvegardes de configuration*.

Considérations relatives à l'utilisation du protocole IP virtuel et de passerelle de frontières avec une configuration 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. Dans ONTAP 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 répliquée sur les nœuds du site de reprise après incident.

L'existence du v0a (v0b, etc.) valide la connectivité en continu, garantissant ainsi la réussite d'une migration ou d'un basculement de LIF (contrairement à 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 erronés 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).

Test de la configuration MetroCluster

Vous pouvez tester les scénarios d'échec pour vérifier le bon fonctionnement de la configuration MetroCluster.

Vérification du basculement négocié

Vous pouvez tester une opération de basculement négociée (planifiée) pour confirmer la disponibilité des données sans interruption.

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.

Ce test devrait prendre environ 30 minutes.

Cette procédure devrait permettre de revenir aux nœuds de départ des services.

Étapes

1. Vérifiez que la correction est terminée :

```
metrocluster node show
```

L'exemple suivant montre la réussite de la commande :

```
cluster_A::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
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.
```

2. Vérifier que tous les agrégats sont bien mirrored:

```
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  -
```

3. Démarrez les nœuds à partir du site de reprise sur incident.

4. Vérifier l'état de la restauration en cas de rétablissement :

```
metrocluster node show
```

```
cluster_A:> metrocluster node show
DR
Group Cluster Node      Configuration  DR
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.
```

5. Effectuez le rétablissement :

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful. Verify switchback
```

6. Confirmer l'état des nœuds :

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR
Group Cluster Node Configuration State DR
Mirroring Mode
-----
1      cluster_A
      node_A_1      configured enabled normal
      cluster_B
      node_B_2      configured enabled normal

2 entries were displayed.
```

7. Confirmer le statut :

```
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: -
```

Perte d'un seul pont FC-SAS

Vous pouvez tester la défaillance d'un seul pont FC-to-SAS pour vous assurer qu'il n'y a pas de point de défaillance unique.

Ce test devrait prendre environ 15 minutes.

Cette procédure présente les résultats attendus suivants :

- Les erreurs doivent être générées lorsque le pont est désactivé.
- Aucun basculement ni perte de service ne doit se produire.
- Un seul chemin entre le module de contrôleur et les lecteurs derrière le pont est disponible.



Avec ONTAP 9.8, le `storage bridge` la commande est remplacée par `system bridge`. Les étapes suivantes présentent le `storage bridge` Mais si vous exécutez ONTAP 9.8 ou version ultérieure, le `system bridge` commande recommandée.

Étapes

1. Coupez les alimentations du pont.
2. Vérifiez que la surveillance du pont indique une erreur :

```
storage bridge show
```

```
cluster_A::> storage bridge show
```

Monitor	Bridge	Symbolic Name	Vendor	Model	Bridge WWN	Is Monitored
ATTO_10.65.57.145	bridge_A_1	Atto	FibreBridge	6500N	200000108662d46c	true

error

3. Vérifiez que les lecteurs derrière le pont sont disponibles avec un seul chemin :

```
storage disk error show
```

```
cluster_A::> storage disk error show
Disk          Error Type          Error Text
-----
-----
1.0.0          onedomain          1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1          onedomain          1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2          onedomain          1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23         onedomain          1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

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.

Il est recommandé de connecter chaque unité d'alimentation d'un composant à une alimentation séparée. 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 et 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. Surveillez le résultat sur la console à l'aide du `system environment sensors show -state fault` et `storage shelf show -errors` commandes.

```
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.

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::> vservers show -type data
```

```
cluster_A::> vservers show -type data
```

Vserver	Type	Subtype	Admin State	Operational State	Root 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 afin de mettre hors tension et 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
```

```
storage aggregate show -r -node node_A_2 !*root
```

L'agrégat avec des disques du shelf hors tension doit avoir un état RAID « défini » et les disques du plex affecté doivent avoir un statut « en panne », comme illustré dans l'exemple suivant :

```

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::> vservers show -type data

cluster_A::> vservers show -type data

```

Vserver	Type	Subtype	Admin State	Operational State	Root 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 un état RAID « de synchronisation », comme illustré dans 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.

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 un contrôle supplémentaires

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"](#)

Synchronisez l'heure du système à l'aide du protocole NTP

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 le basculement.
- Chaque cluster de la configuration Stretch MetroCluster doit disposer de son propre serveur NTP ou de serveurs utilisés par les nœuds de ce site MetroCluster.
- Si vous utilisez le logiciel MetroCluster Tiebreaker, il doit également disposer de son propre serveur NTP.

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.

Considérations relatives à l'utilisation de ONTAP dans une configuration 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.

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.

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 avec `vserver peer repeer` commande.

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 lorsque les clusters impliqués 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 les sites_A et site_C ne sont pas connectés, vous devez modifier manuellement les SVM sur site_B (le cluster de basculement) et site_C à l'aide du `vserver peer repeer` commande 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.

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 agrégats"](#).

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.

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"](#).

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 dans 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 principal.

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

["Concepts relatifs à ONTAP"](#)

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.

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 `metrocluster check lif show` commande. En cas de problème lors de la création du LIF, vous pouvez utiliser le `metrocluster check lif repair-placement` commande permettant de résoudre les problèmes.

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	La capacité d'accessibilité est déterminée en vérifiant la connectivité du nom 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 réachabilité est déterminée par la réponse à une diffusion ARP (Address Resolution Protocol) de chaque port précédemment identifié sur le cluster DR à l'adresse IP source de la LIF à placer. Pour que les vérifications de la réaptitude réussissent, les diffusions ARP doivent être autorisées entre les deux groupes. Chaque port qui reçoit une réponse de la LIF source sera marqué comme possible pour le placement.
Sélection de port	ONTAP catégorise les ports en fonction d'attributs tels que le type d'adaptateur et la vitesse, puis sélectionne les ports avec des attributs correspondants. Si aucun port avec des attributs correspondants n'est trouvé, la LIF est placée sur un port connecté au hasard sur le partenaire DR.	Depuis les ports marqués comme accessibles lors du contrôle de ré-accessibilité, ONTAP préfère les ports qui sont dans le broadcast domain associé au sous-réseau de la LIF. S'il n'y a aucun port réseau disponible sur le cluster DR qui se trouve dans le broadcast domain associé au sous-réseau de la LIF, ONTAP sélectionne les ports qui ont la ré-accessibilité 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.

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.

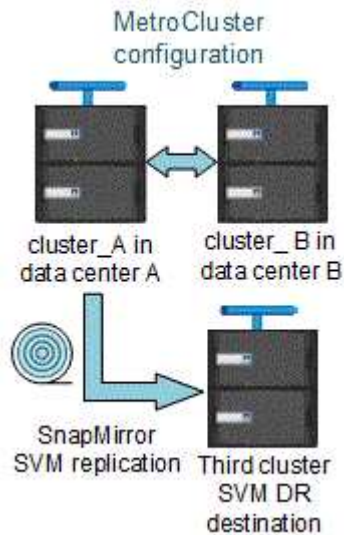
La reprise sur incident SnapMirror doit être consciente des exigences et limitations suivantes, liées à l'utilisation de SVM :

- 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.

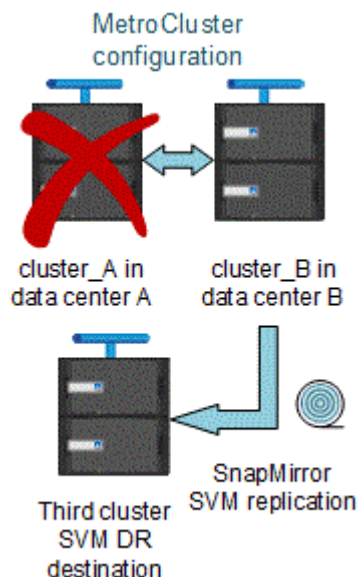
- Lorsqu'une configuration MetroCluster est dans un état stable, le SVM MetroCluster destination ne peut pas être à l'origine d'une relation de reprise d'activité SVM, car les volumes ne sont pas en ligne.

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.

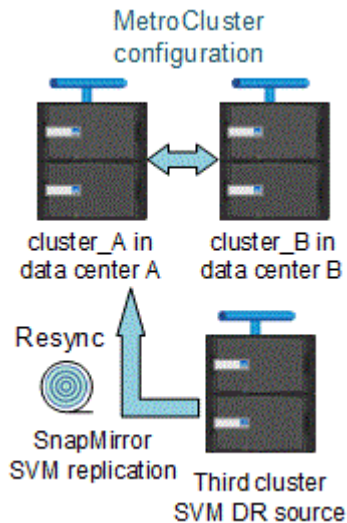
Toutefois, une fois le processus de basculement ou de rétablissement terminé, les mises à jour planifiées de reprise sur incident du SVM suivantes seront appliquées.

Voir la section « réplication de la configuration SVM » dans le ["Protection des données via l'interface de ligne de commandes"](#) 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 recréée 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' ».

Résultat des commandes Storage disk show et Storage shelf show dans une configuration MetroCluster étendue à deux nœuds

Dans une configuration MetroCluster extensible à deux nœuds, le `is-local-attach` champ du `storage disk show` et `storage shelf show` les commandes affichent tous les disques et tiroirs de stockage comme locaux, quel que soit le nœud auquel ils sont connectés.

Le résultat de la commande `plex show` de l'agrégat de stockage est indéterminé après un basculement de MetroCluster

Lorsque vous exécutez le `storage aggregate plex show` Commande après un basculement MetroCluster, l'état du `plex0` de l'agrégat racine commuté est indéterminé et s'affiche sous la forme `failed`. 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.

Étapes

1. Activez la configuration MetroCluster pour déclencher NVFAIL lors du basculement en réglant le `vol -dr -force-nvfail` paramètre à « on » :

```
vol modify -vserver vservice-name -volume volume-name -dr-force-nvfail on
```

Passer d'une configuration Stretch à une configuration MetroCluster Fabric-Attached

Dans une configuration MetroCluster FAS, les nœuds sont situés à différents emplacements. Cette différence géographique augmente la protection contre les incidents. Pour passer d'une configuration Stretch à une configuration MetroCluster Fabric-Attached, vous devez ajouter des commutateurs FC et, le cas échéant, des ponts FC-SAS à la configuration.

- Vous devez désactiver le basculement automatique sur les deux clusters en exécutant la `metrocluster modify -auto-switchover-failure-domain auto-disabled` commande.
- Vous devez avoir arrêté les nœuds.

Cette procédure est perturbatrice.

La configuration MetroCluster doit être transférée sur les deux sites. Une fois la configuration MetroCluster mise à niveau, vous devez activer le basculement automatique sur les deux clusters. Vous devez également valider la configuration en exécutant le `metrocluster check run` commande.

Cette procédure donne un aperçu des étapes requises. Pour les étapes détaillées, vous devez vous référer à des sections spécifiques dans le ["Installation et configuration de la solution Fabric-Attached MetroCluster"](#). Il n'est pas nécessaire d'effectuer une installation et une configuration complètes.

Étapes

1. Préparez la mise à niveau en consultant attentivement la section « préparation de l'installation MetroCluster » du ["Installation et configuration de la solution Fabric-Attached MetroCluster"](#).
2. Installez, câblez et configurez les commutateurs et les ponts FC-SAS requis.



Nous vous recommandons d'utiliser les procédures de la section « câblage d'une configuration MetroCluster reliée à la structure » du ["Installation et configuration de la solution Fabric-Attached MetroCluster"](#).

3. Procédez comme suit pour actualiser la configuration MetroCluster.

N'utilisez pas les procédures de la section « Configuration du logiciel MetroCluster dans ONTAP » du ["Installation et configuration de la solution Fabric-Attached MetroCluster"](#).

- a. Passez en mode de privilège avancé :
set -privilege advanced
- b. Actualisez la configuration MetroCluster :
metrocluster configure -refresh true

La commande suivante actualise la configuration de MetroCluster sur tous les nœuds du groupe DR qui contient Controller_A_1 :

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

- a. Revenir en mode de privilège admin:
set -privilege admin
4. Vérifiez que la configuration MetroCluster ne comporte pas d'erreurs, puis vérifiez qu'elle est opérationnelle.

Vous devez utiliser les procédures décrites dans les sections suivantes du ["Installation et configuration de la solution Fabric-Attached MetroCluster"](#):

- Vérification des erreurs de configuration MetroCluster avec Config Advisor
- Vérification du fonctionnement de la haute disponibilité locale
- Vérification du basculement, de la résolution et du rétablissement

Où trouver des informations complémentaires

Pour en savoir plus sur la configuration et le fonctionnement de MetroCluster,

MetroCluster et informations diverses

Informations	Objet
"Documentation ONTAP 9"	• Tous les guides MetroCluster

	• Présentation technique de la configuration et du fonctionnement de MetroCluster FC. • Meilleures pratiques en matière de configuration MetroCluster FC.
"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 IP de MetroCluster : différences entre les configurations ONTAP MetroCluster"	• Architecture de MetroCluster IP • Câblage de la configuration • Configuration de MetroCluster dans ONTAP
"Gestion et reprise après incident MetroCluster"	• Présentation de la configuration MetroCluster • Basculement, rétablissement et rétablissement • Reprise après incident
"Gérer les composants MetroCluster"	• Instructions relatives à la maintenance dans une configuration MetroCluster FC • Remplacement ou mise à niveau du matériel. Procédure de mise à niveau de firmware pour les ponts FC-à-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 de reprise sur incident dans une configuration MetroCluster FC Fabric-Attached ou Stretch • 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.

"Transition de MetroCluster FC à MetroCluster IP" "Guide de mise à niveau et d'extension de MetroCluster"	• Mise à niveau ou actualisation d'une configuration MetroCluster • Passer d'une configuration MetroCluster FC à une configuration MetroCluster IP • Extension d'une configuration MetroCluster par l'ajout de nœuds supplémentaires
"Installation et configuration du logiciel MetroCluster Tiebreaker"	• Contrôle de la configuration de MetroCluster avec le logiciel MetroCluster Tiebreaker
Documentation Active IQ Unified Manager "Documentation NetApp : guides et ressources produits"	• Contrôle de la configuration et des performances d'MetroCluster
"Transition basée sur la copie"	• Transition des données depuis les systèmes de stockage 7-mode vers les systèmes de stockage en cluster
"Concepts relatifs à ONTAP"	• Fonctionnement des agrégats en miroir

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.