



Configurer les composants matériels de MetroCluster

ONTAP MetroCluster

NetApp

February 27, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-metrocluster/install-ip/concept_parts_of_an_ip_mcc_configuration_mcc_ip.html on February 27, 2026. Always check docs.netapp.com for the latest.

Sommaire

Configurer les composants matériels de MetroCluster	1
En savoir plus sur les interconnexions des composants matériels dans une configuration IP MetroCluster	1
Principaux éléments matériels	1
Groupes de reprise après incident	2
Illustration des paires haute disponibilité locales dans une configuration MetroCluster	2
Illustration du réseau d'interconnexion de cluster et IP de MetroCluster	3
Illustration du réseau de peering de cluster	4
Composants de configuration IP MetroCluster requis et conventions de dénomination	5
Logiciels et matériel pris en charge	5
La redondance matérielle est requise dans une configuration MetroCluster IP	5
Configuration requise pour le cluster ONTAP dans une configuration IP MetroCluster	6
Configuration du commutateur IP requise dans une configuration MetroCluster IP	6
Configuration requise pour le module de contrôleur dans une configuration IP MetroCluster	6
Configuration de la carte Gigabit Ethernet requise dans une configuration IP MetroCluster	7
Exigences relatives au pool et au disque (minimum pris en charge)	8
Considérations relatives à l'emplacement des disques pour les tiroirs partiellement remplis	9
Considérations relatives à l'emplacement des disques pour les disques internes AFF A800	9
Montez les composants matériels de configuration IP MetroCluster	10
Branchez les câbles des commutateurs IP MetroCluster	10
Comment utiliser les tables de ports avec plusieurs configurations IP MetroCluster	10
Affectations de ports de plate-forme pour les commutateurs Cisco 3132Q-V dans une configuration IP MetroCluster	11
Affectations de ports de plate-forme pour les commutateurs Cisco 3232C ou Cisco 9336C à 36 ports dans une configuration IP MetroCluster	15
Affectations de ports de plate-forme pour les commutateurs Cisco 9336C-FX2 à 12 ports dans une configuration IP MetroCluster	26
Affectations de ports de plate-forme pour un commutateur Cisco 9336C-FX2 à 36 ports connectant un stockage NS224 dans une configuration IP MetroCluster	34
Affectations de ports de plate-forme pour les commutateurs IP BES-53248 pris en charge par Broadcom dans une configuration IP MetroCluster	49
Affectations de ports de plate-forme pour les commutateurs IP SN2100 pris en charge par NVIDIA dans une configuration IP MetroCluster	56
Câbler les ports du module de contrôleur ONTAP dans une configuration IP MetroCluster	61
Configuration des commutateurs IP MetroCluster	62
Choisissez la procédure de configuration du commutateur IP MetroCluster appropriée	62
Configurer les commutateurs IP Broadcom pour l'interconnexion de cluster et la connectivité IP MetroCluster backend	62
Configuration des commutateurs IP Cisco	81
Configurez les commutateurs IP NVIDIA	103
Surveiller l'état du commutateur IP MetroCluster	119
En savoir plus sur la surveillance de l'état des commutateurs dans une configuration IP MetroCluster	119
Configurer SNMPv3 pour surveiller la santé des commutateurs IP MetroCluster	119
Configurer la collecte de journaux sur un commutateur IP MetroCluster	137

Gérer la surveillance des commutateurs Ethernet dans une configuration IP MetroCluster	144
Vérifier la surveillance du commutateur Ethernet dans une configuration IP MetroCluster	145

Configurer les composants matériels de MetroCluster

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

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

Principaux éléments matériels

Une configuration MetroCluster IP inclut les éléments matériels clés suivants :

- Contrôleurs de stockage

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

- Réseau IP

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

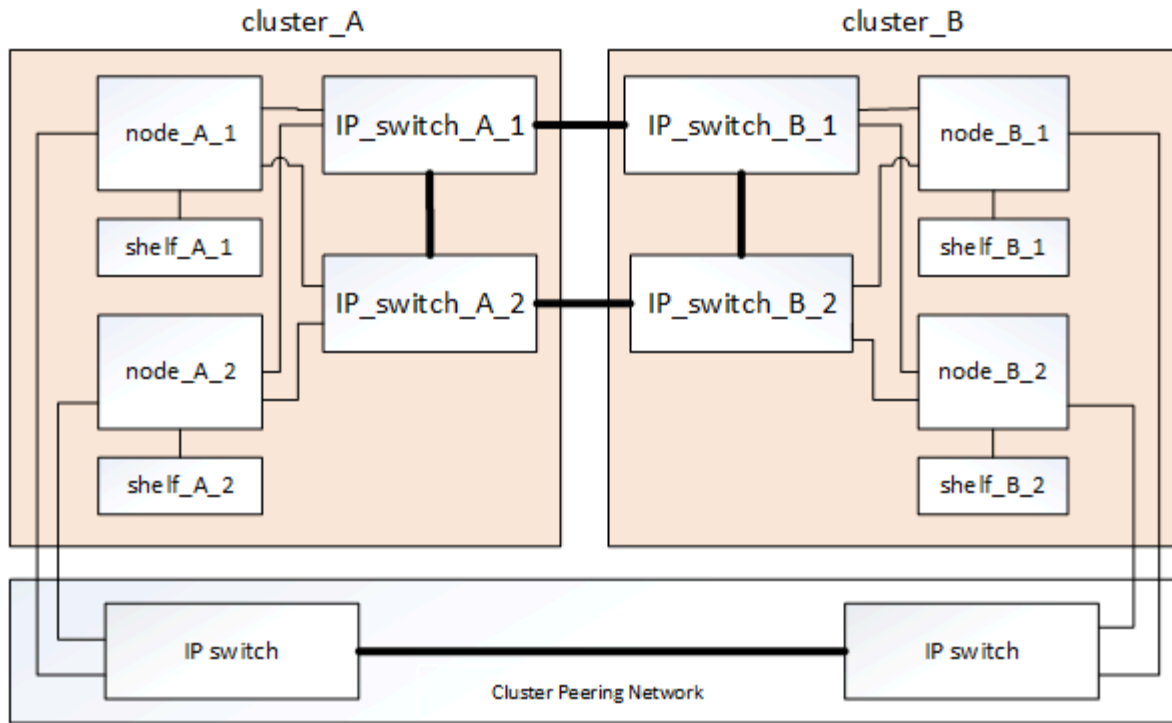
- Connectivité standard du cluster pour les communications intra-cluster.

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

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

- Réseau de peering de cluster

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



Groupes de reprise après incident

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

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

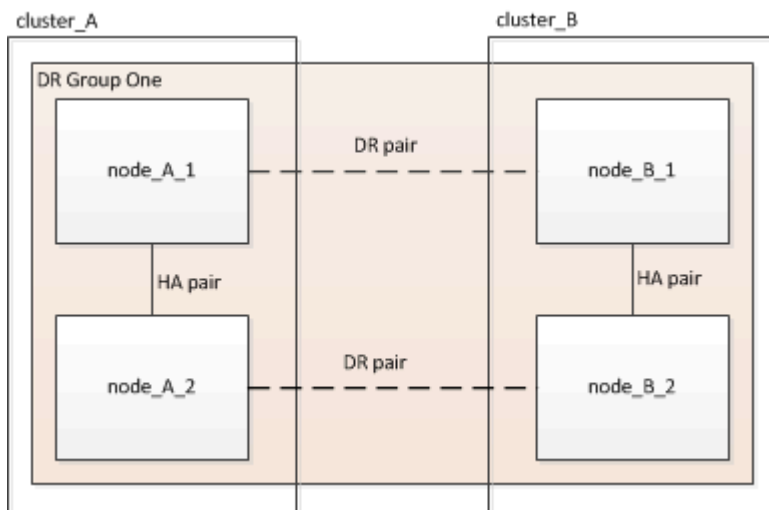
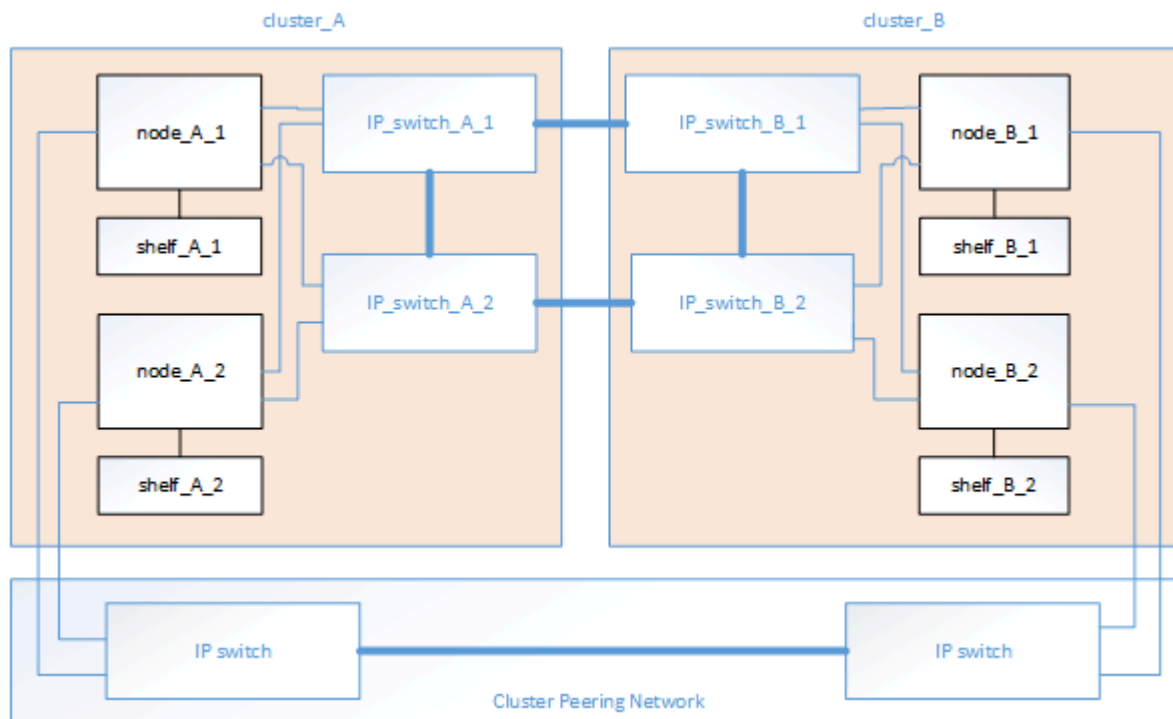


Illustration des paires haute disponibilité locales dans une configuration MetroCluster

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

Les opérations de basculement et de rétablissement de la haute disponibilité locale sont exécutées à l'aide

des commandes de basculement du stockage, de la même manière qu'une configuration non MetroCluster.

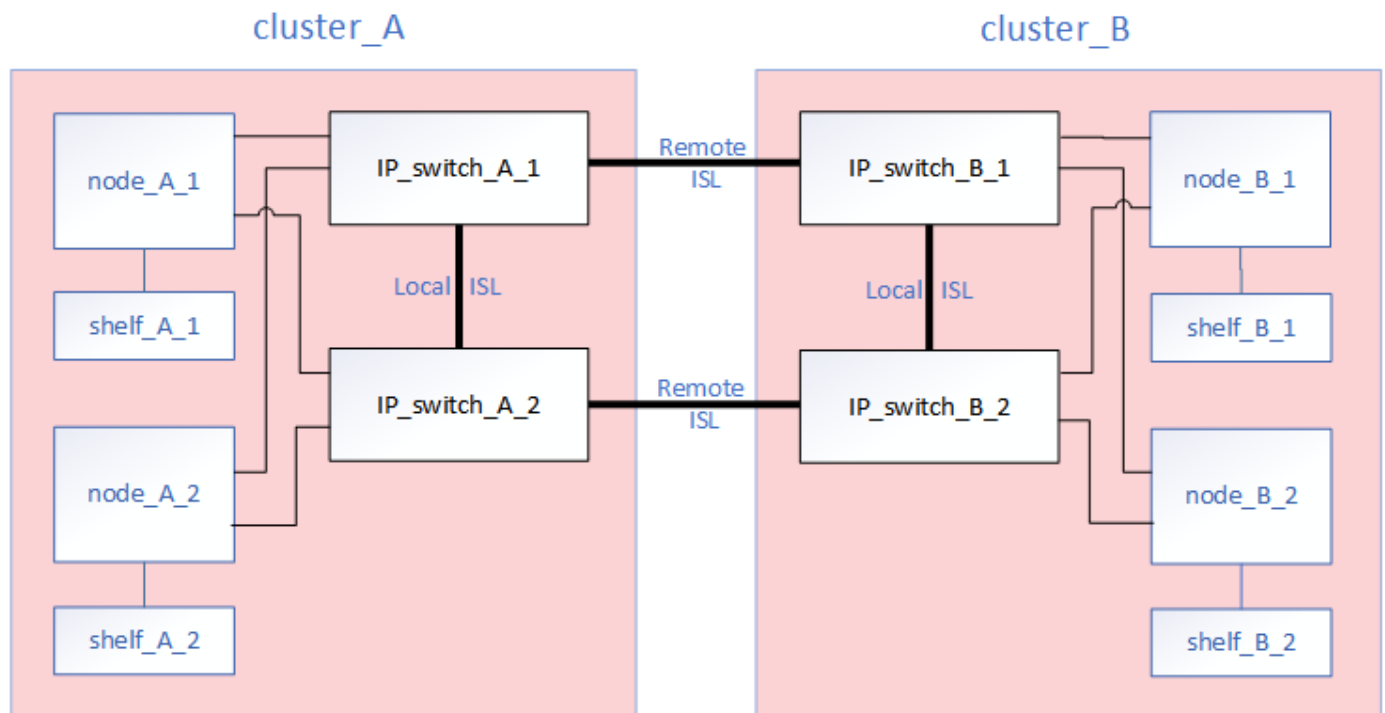


Informations associées

"Concepts relatifs à ONTAP"

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

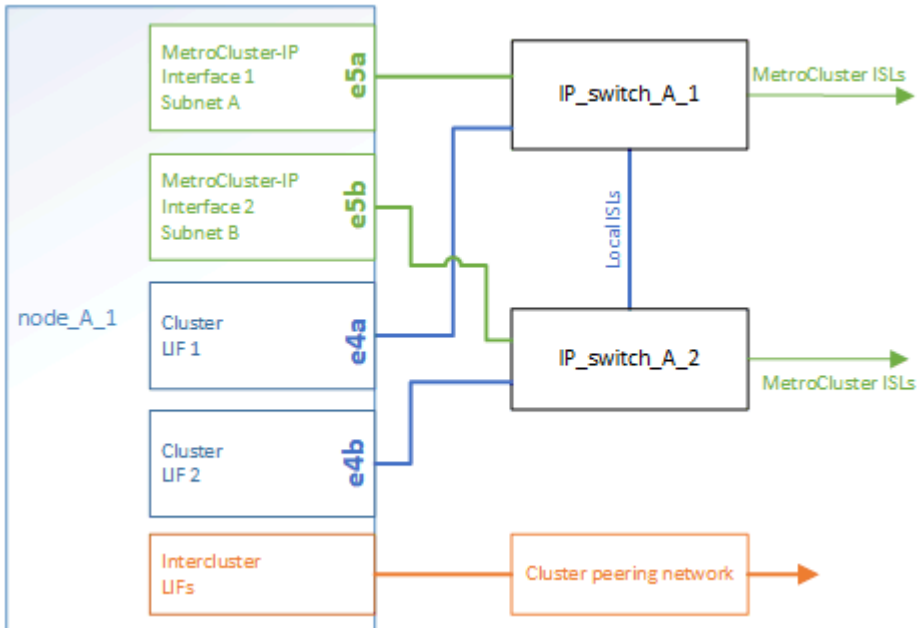
Les clusters ONTAP incluent généralement un réseau d'interconnexion de cluster pour le trafic entre les nœuds du cluster. Dans les configurations IP MetroCluster, ce réseau est également utilisé pour le trafic de réplication des données entre les sites MetroCluster.



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

- Deux interfaces IP MetroCluster
- Deux interfaces locales du cluster

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



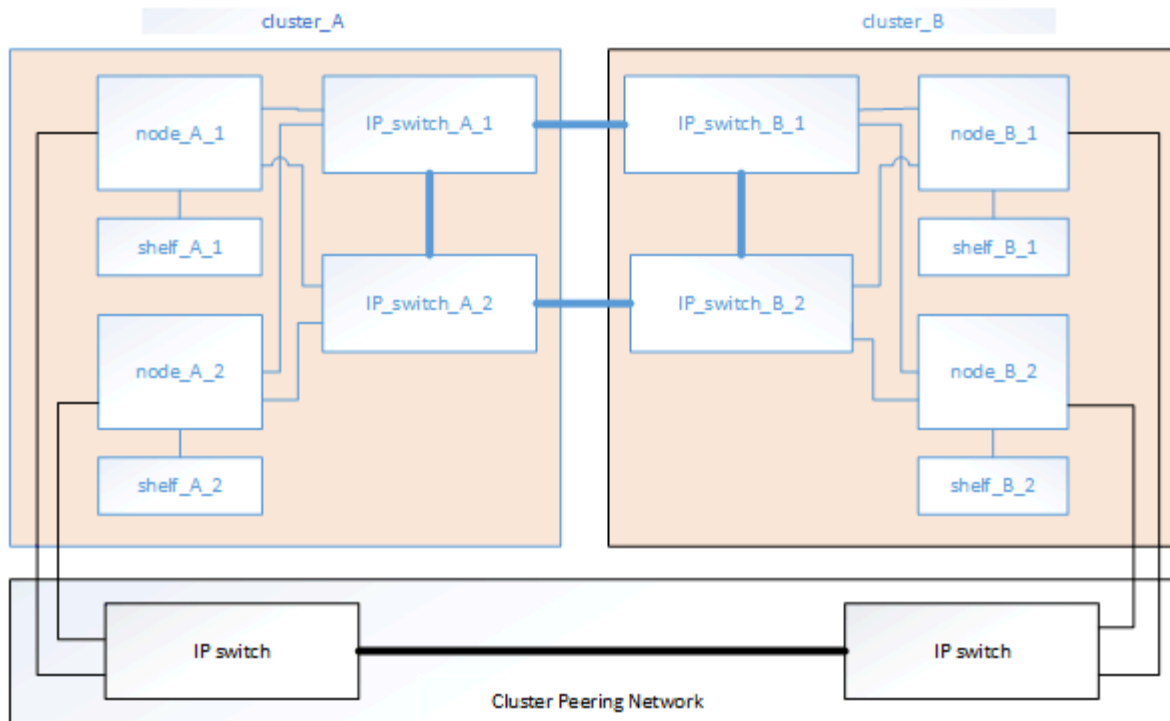
Informations associées

["Considérations relatives aux configurations MetroCluster IP"](#)

Illustration du réseau de peering de cluster

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

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



Informations associées

"Configuration cluster et SVM peering express"

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

"Câblage des connexions de peering de cluster"

"Peering des clusters"

Composants de configuration IP MetroCluster requis et conventions de dénomination

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

Logiciels et matériel pris en charge

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

"NetApp Hardware Universe"

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

La redondance matérielle est requise dans une configuration MetroCluster IP

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

Configuration requise pour le cluster ONTAP dans une configuration IP MetroCluster

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

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

- Site A : cluster_A
- Site B : cluster_B

Configuration du commutateur IP requise dans une configuration MetroCluster IP

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

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

Le nom doit être unique dans la configuration MetroCluster.

Exemples de noms :

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

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

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

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

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

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

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

- Depuis ONTAP 9.5, les nouvelles installations MetroCluster IP sur les systèmes FAS sont prises en charge.

- Depuis ONTAP 9.4, les modules de contrôleur configurés pour ADP sont pris en charge.

Exemples de noms

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

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

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

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



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

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

FAS500f, AFF A250, ASA A250, ASA C250, AFF C250	Ports intégrés	Sans objet	e0c, e0d
AFF A320	Ports intégrés	Sans objet	e0g, e0h
AFF A70, FAS70, AFF C80	X50132A	Emplacement 2	e2a, e2b
AFF A90, AFF A1K, FAS90	X50132A	Emplacement 2, emplacement 3	e2b, e3b Remarque : les ports e2a et e3a doivent rester inutilisés. L'utilisation de ces ports pour les réseaux frontaux ou le peering n'est pas prise en charge.
AFF A50	X60134A	Emplacement 2	e2a, e2b
AFF A30, AFF C30, AFF C60, FAS50	X60134A	Emplacement 2	e2a, e2b
AFF A20	X60132A	Emplacement 4, emplacement 2	e2b, e4b

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

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

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

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

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



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

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

- Trois disques racine
- Trois disques de données

- Un disque de rechange

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

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



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

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

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

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

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

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

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

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

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

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

- Quatre disques au quatrième trimestre : 18, 19, 20, 21

Montez les composants matériels de configuration IP MetroCluster

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

Description de la tâche

Cette tâche doit être effectuée sur les deux sites MetroCluster.

Étapes

1. Planifiez le positionnement des composants MetroCluster.

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

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

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

4. Installez les commutateurs IP sur le rack ou l'armoire.
5. Installez les tiroirs disques, mettez-les sous tension, puis définissez les ID de tiroir.
 - Vous devez mettre chaque tiroir disque hors tension puis sous tension.
 - Il est vivement recommandé d'utiliser des ID de tiroir unique pour chaque tiroir disque SAS dans chaque groupe MetroCluster DR afin de faciliter le dépannage.



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

Branchez les câbles des commutateurs IP MetroCluster

Comment utiliser les tables de ports avec plusieurs configurations IP MetroCluster

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

Avant de commencer

Vérifiez les points suivants avant d'utiliser les tableaux :

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

- Conservez une trace du groupe de ports MetroCluster (MetroCluster 1, MetroCluster 2, etc.). Vous aurez besoin de ces informations lors de l'utilisation de l'outil RcfFileGenerator comme décrit plus loin dans cette procédure de configuration.
- Vous devez câbler tous les nœuds de la même manière. Si différentes options de combinaison de ports sont disponibles pour câbler les nœuds, tous les nœuds doivent utiliser les mêmes combinaisons de ports. Par exemple, e1a sur le nœud 1 et e1a sur le nœud 2 doivent être connectés à un commutateur. De même, le second port des deux nœuds doit être connecté au second switch.
- Le "[RcfFileGenerator pour MetroCluster IP](#)" fournit également une vue d'ensemble du câblage par port pour chaque commutateur. Utilisez cette présentation du câblage pour vérifier votre câblage.

Câblage de deux configurations MetroCluster aux commutateurs

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

Câblage des configurations MetroCluster à 8 nœuds

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

Description de la tâche

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

Par exemple, votre configuration inclut les éléments suivants :

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

Étapes

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

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

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

Consultez ces directives avant d'utiliser les tableaux :

- Si vous configurez le commutateur pour la transition FC vers IP MetroCluster, le port 5, le port 6, le port 13

ou le port 14 peuvent être utilisés pour connecter les interfaces de cluster locales du nœud FC MetroCluster. Reportez-vous à la "[RcfFileGenerator](#)" et les fichiers de câblage générés pour plus de détails sur le câblage de cette configuration. Pour toutes les autres connexions, vous pouvez utiliser les affectations d'utilisation des ports répertoriées dans les tableaux.

Choisissez la table de câblage adaptée à votre configuration

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

Si votre système est...	Utilisez ce tableau de câblage...
FAS2750, AFF A220	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 1)
FAS9000, AFF A700	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 2)
AFF A800, ASAA800	Attributions des ports de la plate-forme Cisco 3132Q-V (groupe 3)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Utilisez cette présentation du câblage pour vérifier votre câblage.

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



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

Choisissez la table de câblage adaptée à votre configuration

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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



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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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



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

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

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

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

Choisissez la table de câblage adaptée à votre configuration

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

Si votre système est...	Utilisez ce tableau de câblage...
AFF A150, ASAA150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 1)
AFF A20	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 2)
AFF A30, AFF C30 FAS50 AFF C60	Le tableau suivant dépend de l'utilisation d'une carte Ethernet 25G (groupe 3a) ou 100G (groupe 3b). • Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3a - 25G) • Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 3b - 100G)
FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 4)
AFF A50	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 5)
AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Affectations de ports de la plateforme Cisco 9336C-FX2 à 12 ports (groupe 7)

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

Passez en revue les affectations de ports de la plate-forme pour câbler un système AFF A150, ASAA150, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 à un commutateur Cisco 9336C-FX2 à 12 ports :

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

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

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

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

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

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

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

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



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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

- Lorsque vous câblez un commutateur Cisco 9336C-FX2 pour connecter un stockage NS224, vous ne pouvez avoir qu'un maximum de deux configurations MetroCluster ou groupes DR. Au moins une configuration MetroCluster ou un groupe DR doit connecter des étagères NS224 au commutateur MetroCluster.

Si l'une de vos configurations MetroCluster ou groupes DR ne connecte pas les étagères NS224 au commutateur MetroCluster, suivez le [Tableaux de câblage pour les contrôleurs ne connectant pas les étagères NS224 connectées par commutateur](#).

- Le RcfFileGenerator affiche uniquement les plates-formes éligibles lorsque la première plate-forme est sélectionnée.
- Si vous étendez une configuration MetroCluster standard qui ne prend pas en charge le stockage NS224 connecté au commutateur et que vous souhaitez ajouter une configuration MetroCluster qui prend en charge le stockage NS224 connecté au commutateur, consultez les informations suivantes :
 - Dans l'"[RcfFileGenerator](#)" outil, vous devez d'abord sélectionner la plateforme qui prend en charge le stockage NS224 connecté au commutateur, puis sélectionner la plateforme qui ne prend pas en charge le stockage NS224 connecté au commutateur.

Cela signifie que lorsque vous générez le RCF pour votre nouvelle configuration, vous devrez peut-être sélectionner les plateformes dans l'outil RcfFileGenerator dans l'ordre suivant :

- i. Sélectionnez la plateforme qui prend en charge le stockage NS224 connecté au commutateur dans le **second champ déroulant**.
 - ii. Sélectionnez la plateforme qui ne prend pas en charge le stockage NS224 connecté au commutateur dans le **premier champ déroulant**.
- La connexion d'une configuration MetroCluster à huit ou deux nœuds requiert ONTAP 9.14.1 ou version ultérieure.

Choisissez la table de câblage adaptée à votre configuration

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

- [Tableaux de câblage pour contrôleurs connectant des tiroirs NS224 reliés par un commutateur](#)
- [Tableaux de câblage pour les contrôleurs ne connectant pas les tiroirs NS224 reliés par un commutateur](#)

Contrôleurs connectant des tiroirs NS224 reliés par un commutateur

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

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

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

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



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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

reliés par un commutateur Cisco 9336C-FX2 :

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

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

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

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

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

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

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

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

- Vous ne pouvez pas utiliser les switches avec des ports ISL distants de différentes vitesses (par exemple,

un port 25 Gbit/s connecté à un port ISL de 10 Gbit/s).

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

Plate-forme cible	Port
FAS500f, AFF C250, ASA C250, AFF A250, ASAA250, FAS8300, AFF C400, ASA C400, AFF A400, ASAA400, ou FAS8700	Ports 1 à 6, 10 Gbits/s.
Plateformes FAS8200 ou AFF A300	Ports 3 - 4 et 9 - 12, 10 Gbits/s.

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

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

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

Choisissez la table de câblage adaptée à votre configuration

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

Si votre système est...	Utilisez ce tableau de câblage...
AFF A150, ASAA150 FAS2750 AVEC AFF A220	Attributions de port de la plate-forme Broadcom BES-53248 (groupe 1)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Attributions de port de la plate-forme Broadcom BES-53248 (groupe 2)
AFF A20	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 3)
AFF C30, AFF A30 FAS500 AFF C60	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 4)
FAS8200, AFF A300	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 5)
AFF A320	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 6)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Attributions des ports de la plate-forme Broadcom BES-53248 (groupe 7)

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

Vérifiez les attributions de port de la plate-forme pour connecter un système AFF A150, ASAA150, FAS2750 ou AFF A220 à un commutateur Broadcom BES-53248 :

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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



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

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

Choisissez la table de câblage adaptée à votre configuration

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

Si votre système est...	Utilisez ce tableau de câblage...
AFF A150, ASAA150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 1)
AFF A20	Affectations des ports de la plate-forme NVIDIA SN2100 (groupe 2)

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

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

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

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

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

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

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

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

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



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

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8		e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Au moins deux ports sur chaque module de contrôleur doivent être utilisés pour le peering de cluster.

La bande passante minimale recommandée pour les ports et la connectivité réseau est de 1 GbE.

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

connectivité réseau avec le cluster partenaire.

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

["Configuration cluster et SVM peering express"](#)

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

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



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

Configuration des commutateurs IP MetroCluster

Choisissez la procédure de configuration du commutateur IP MetroCluster appropriée

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

- ["Configurez les commutateurs IP Broadcom"](#)
- ["Configuration des commutateurs IP Cisco"](#)
- ["Configurez les commutateurs IP NVIDIA"](#)

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

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



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

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

Réinitialisation des paramètres d'usine du commutateur IP Broadcom

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

Description de la tâche

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

Étapes

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

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

2. Effacez la configuration de démarrage et supprimez la bannière

- a. Effacez la configuration de démarrage :

erase startup-config

```
(IP_switch_A_1) #erase startup-config

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

(IP_switch_A_1) #
```

Cette commande n'efface pas la bannière.

- b. Supprimer la bannière :

no set clibanner

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

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

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



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

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

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

```
(Routing) >
```

5. Passer à l'invite de commande surélevée :

```
enable
```

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

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

```
serviceport protocol none
```

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

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

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

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

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

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

```
show serviceport
```

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

```
(Routing) #show serviceport
```

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

```
(Routing) #
```

9. Configurez le serveur SSH.



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

a. Générer des clés RSA.

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

b. Générer des clés DSA (facultatif)

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

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

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

d. Activez le serveur SSH.

Si nécessaire, quittez le contexte de configuration.


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

+



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

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

configure

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

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

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

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

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

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

```

> (Config)# ntp ?

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

>(Config)# ntp server ?

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

>(Config)# ntp server 10.99.99.5

```

12. Configurer le nom du commutateur :

```
hostname IP_switch_A_1
```

L'invite du commutateur affiche le nouveau nom :

```

(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #

```

13. Enregistrez la configuration :

```
write memory
```

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

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully .

Configuration Saved!

```
(IP_switch_A_1) #
```

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

Téléchargement et installation du logiciel du commutateur Broadcom EFOS

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

Description de la tâche

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

Notez ce qui suit :

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

Étapes

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

Exemple 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Exemple 2

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

IP_switch_A_2 #
```

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

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

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

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

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

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



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

Étapes

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

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

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

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

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

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

```
File transfer operation completed successfully.
```

```
(IP_switch_A_1) #
```

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

```
boot system backup
```

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

```
(IP_switch_A_1) #
```

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

```
show bootvar
```

```
(IP_switch_A_1) #show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.4.2	3.4.4.6	3.4.4.2	3.4.4.6

```
(IP_switch_A_1) #
```

4. Enregistrez la configuration :

```
write memory
```

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

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

Configuration Saved!

```
(IP_switch_A_1) #
```

5. Redémarrez le commutateur :

```
reload
```

```
(IP_switch_A_1) #reload
```

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

6. Attendez que le commutateur redémarre.



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

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

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

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

Étapes

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

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

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

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

```

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

```

Le commutateur démarre maintenant en mode d'installation ONIE.

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

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

```

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

```



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

```

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

```

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

```

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

```

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

```

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

```

5. Installez le nouveau logiciel du commutateur

```

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

```

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

6. Vérifier que le nouveau logiciel de commutateur est installé

show bootvar

```

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

```

7. Terminez l'installation

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

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

Téléchargement et installation des fichiers RCF Broadcom

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

Avant de commencer

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

Description de la tâche

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

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

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



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

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

Étapes

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



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

2. Copier les fichiers RCF sur les commutateurs :

- a. Copier les fichiers RCF sur le premier commutateur :

```
copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt  
nvram:script BES-53248_v1.32_Switch-A1.scr
```

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

```

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

Remote Password:*****

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

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

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.

Validating configuration script...

config

set clibanner
"*****
*****

* NetApp Reference Configuration File (RCF)

*

* Switch      : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #

```

b. Vérifiez que le fichier RCF est enregistré comme script :

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name          Size(Bytes)  Date of Modification
-----
BES-53248_v1.32_Switch-A1.scr      852         2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Appliquer le script RCF :

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

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

config

set clibanner
*****
*****

* NetApp Reference Configuration File (RCF)

*

* Switch      : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Enregistrez la configuration :

```
write memory
```



```
(IP_switch_A_1) #write memory

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

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

Configuration Saved!

(IP_switch_A_1) #
```

e. Redémarrez le commutateur :

```
reload
```

```
(IP_switch_A_1) #reload

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

a. Répétez les étapes précédentes pour chacun des trois autres commutateurs en veillant à copier le fichier RCF correspondant sur le commutateur correspondant.

3. Recharger l'interrupteur :

```
reload
```

```
IP_switch_A_1# reload
```

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

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :



Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

Pour plus de détails sur le port ISL

Lancer la commande `show port all`.

Pour plus d'informations sur les canaux de port

Lancer la commande `show port-channel all`.

2. Désactivez les ports ISL et les canaux de port inutilisés.

Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1) (Config)# <port_name>
(SwtichA_1) (Interface 0/15)# shutdown
(SwtichA_1) (Interface 0/15)# end
(SwtichA_1)# write memory
```

Configuration des commutateurs IP Cisco

Configurer les commutateurs IP Cisco pour l'interconnexion des clusters et la connectivité IP MetroCluster backend

Vous devez configurer les switches IP Cisco pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Description de la tâche

Plusieurs procédures de cette section sont des procédures indépendantes et vous n'avez qu'à exécuter celles que vous êtes dirigé vers ou qui sont pertinentes pour votre tâche.

Réinitialisation des paramètres d'usine du commutateur IP Cisco

Avant d'installer un fichier RCF, vous devez effacer la configuration du commutateur Cisco et effectuer une configuration de base. Cette procédure est obligatoire lorsque vous souhaitez réinstaller le même fichier RCF après l'échec d'une installation précédente ou si vous souhaitez installer une nouvelle version d'un fichier RCF.

Description de la tâche

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

Étapes

1. Rétablir les paramètres d'usine du commutateur :

- a. Effacez la configuration existante :

```
write erase
```

b. Recharger le logiciel du contacteur :

```
reload
```

Le système redémarre et entre dans l'assistant de configuration. Au cours du démarrage, si vous recevez l'invite « abandonner la mise en service automatique et poursuivre la configuration normale ? (oui/non) », you should respond `yes pour continuer.

c. Dans l'assistant de configuration, entrez les paramètres de base du commutateur :

- Mot de passe d'administrateur
- Nom du commutateur
- Configuration de gestion hors bande
- Passerelle par défaut
- Service SSH (RSA)

Une fois l'assistant de configuration terminé, le commutateur redémarre.

d. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe pour vous connecter au commutateur.

L'exemple suivant montre les invites et les réponses système lors de la configuration du commutateur. Les supports d'angle (<<<) indique où vous saisissez les informations.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
    Confirm the password for "admin": password
        ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Vous entrez des informations de base dans les invites suivantes, notamment le nom du commutateur, l'adresse de gestion et la passerelle, et sélectionnez SSH avec RSA.



Cet exemple montre les informations minimales requises pour configurer la FCR. Des options supplémentaires peuvent être configurées une fois la FCR appliquée. Par exemple, vous pouvez configurer SNMPv3, NTP ou SCP/SFTP après avoir appliqué le RCF.

```
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name : switch-name **<<<
Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
  Mgmt0 IPv4 address : management-IP-address **<<<
  Mgmt0 IPv4 netmask : management-IP-netmask **<<<
  Configure the default gateway? (yes/no) [y]: y **<<<
  IPv4 address of the default gateway : gateway-IP-address **<<<
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y **<<<
  Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<
  Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Le jeu d'invites final termine la configuration :

The following configuration will be applied:

```
password strength-check
switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
no feature telnet
ssh key rsa 1024 force
feature ssh
system default switchport
system default switchport shutdown
copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown
```

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:

2017 Jun 13 21:24:43 A1 %\$ VDC-1 %\$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[#####] 100%
Copy complete.

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Enregistrez la configuration :

```
IP_switch-A-1# copy running-config startup-config
```

3. Redémarrez le commutateur et attendez que le commutateur se recharge :

```
IP_switch-A-1# reload
```

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

Téléchargement et installation du logiciel du commutateur Cisco NX-OS

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

Description de la tâche

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

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

Vous devez utiliser la version du logiciel de commutation prise en charge.

["NetApp Hardware Universe"](#)

Étapes

1. Téléchargez le fichier logiciel NX-OS pris en charge.

["Téléchargement de logiciels Cisco"](#)

2. Copier le logiciel du commutateur sur le commutateur :

```
copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf  
management
```

Dans cet exemple, le fichier nxos.7.0.3.l4.6.bin et l'image EPLD sont copiés du serveur SFTP 10.10.99.99 vers le bootflash local :

```

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin 100% 666MB 7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

```

3. Vérifiez sur chaque commutateur que les fichiers de commutateur NX-OS sont présents dans le répertoire bootflash de chaque commutateur :

dir bootflash:

L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```

IP_switch_A_1# dir bootflash:
      .
      .
      .
698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
      .
      .
      .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. Installez le logiciel du commutateur :

```
install all nxos bootflash:nxos.version-number.bin
```

Le commutateur se recharge automatiquement (redémarre) après l'installation du logiciel du commutateur.

L'exemple suivant montre l'installation du logiciel sur IP_switch_A_1 :

```

IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS          [#####] 100%
-- SUCCESS

Performing module support checks.          [#####] 100%
-- SUCCESS

Notifying services about system upgrade.    [#####] 100%

```


-- SUCCESS

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version	Upg-Required
1	nxos	7.0(3)I4(1)	7.0(3)I4(6)	yes
1	bios	v04.24(04/21/2016)	v04.24(04/21/2016)	no

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Performing runtime checks. [#####] 100% --
SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#

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

Une fois le commutateur redémarré, l'invite de connexion s'affiche :

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vérifier que le logiciel du commutateur a été installé :
show version

L'exemple suivant montre la sortie :

```

IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time: 04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time: 3/9/2017 22:00:00 [03/10/2017 07:05:18]

Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash: 14900224 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after Mon Jun 10 21:43:52 2017

Reason: Reset due to upgrade
System version: 7.0(3)I4(1)
Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#

```

7. Mettre à niveau l'image EPLD et redémarrer le commutateur.

```

IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module          Type          Upgradable    Impact      Reason
-----
1              SUP              Yes           disruptive   Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type  EPLD              Running-Version  New-Version  Upg-
Required
-----
1  SUP  MI FPGA              0x07            0x07        No
1  SUP  IO FPGA              0x17            0x19        Yes
1  SUP  MI FPGA2             0x02            0x02        No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (      64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module  Type  Upgrade-Result
-----
1  SUP  Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

```

8. après le redémarrage du commutateur, reconnectez-vous et vérifiez que la nouvelle version de EPLD a été chargée avec succès.

```
show version module 1 epld
```

9. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Téléchargement et installation des fichiers Cisco IP RCF

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

Description de la tâche

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

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

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

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

Commutateur	Fichier RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Étapes

1. Générez les fichiers RCF Cisco pour MetroCluster IP.
 - a. Téléchargez le "[RcfFileGenerator pour MetroCluster IP](#)"
 - b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.



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

2. Copier les fichiers RCF sur les commutateurs :
 - a. Copier les fichiers RCF sur le premier commutateur :

```
copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
bootflash: vrf management
```

Dans cet exemple, le fichier RCF NX3232_v1.80_Switch-A1.txt est copié du serveur SFTP à 10.10.99.99 vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```

IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

- a. Répétez la sous-étape précédente pour chacun des trois autres commutateurs en étant sûr de copier le fichier RCF correspondant sur le commutateur correspondant.
3. Vérifiez sur chaque commutateur que le fichier RCF est présent dans le répertoire bootflash de chaque commutateur :

dir bootflash:

L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```

IP_switch_A_1# dir bootflash:
      .
      .
      .
5514   Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
      .
      .
      .

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. Configurez les régions TCAM sur les switchs Cisco 3132Q-V et Cisco 3232C.



Ignorez cette étape si vous ne disposez pas de switchs Cisco 3132Q-V ou Cisco 3232C.

- a. Sur le commutateur Cisco 3132Q-V, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- b. Sur le switch Cisco 3232C, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- c. Après avoir défini les régions du TCAM, enregistrez la configuration et rechargez le commutateur :

```
copy running-config startup-config
reload
```

5. Copiez le fichier RCF correspondant de la mémoire bootflash locale vers la configuration en cours d'exécution sur chaque commutateur :

```
copy bootflash:switch-specific-RCF.txt running-config
```

6. Copiez les fichiers RCF de la configuration en cours d'exécution vers la configuration de démarrage de chaque commutateur :

```
copy running-config startup-config
```

Vous devez voir les résultats similaires à ce qui suit :

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Recharger l'interrupteur :

```
reload
```

```
IP_switch_A_1# reload
```

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

Définition de la correction d'erreurs de renvoi pour les systèmes utilisant une connectivité à 25 Gbit/s.

Si votre système est configuré avec une connectivité 25 Gbit/s, vous devez définir manuellement le paramètre fec (Forward Error correction) sur Off après avoir appliqué le fichier RCF. Le fichier RCF n'applique pas ce paramètre.

Description de la tâche

Les ports 25 Gbit/s doivent être câblés avant d'effectuer cette procédure.

"Affectation des ports de plateforme pour les switches Cisco 3232C ou Cisco 9336C"

Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s :

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.

Étapes

1. Définissez le paramètre fec sur Off sur chaque port 25 Gbit/s connecté à un module de contrôleur, puis copiez la configuration en cours d'exécution sur la configuration de démarrage :
 - a. Passer en mode configuration : `conf t`
 - b. Spécifiez l'interface 25 Gbit/s à configurer : `interface interface-ID`
 - c. Réglez fec sur Arrêt : `fec off`
 - d. Répétez les étapes précédentes pour chaque port 25 Gbit/s du commutateur.
 - e. Quitter le mode de configuration : `exit`

L'exemple suivant montre les commandes de l'interface Ethernet1/25/1 sur le commutateur IP_switch_A_1 :

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Répétez l'étape précédente sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifier les ports ISL et les canaux de port inutilisés :


```
show interface brief
```

2. Désactivez les ports ISL et les canaux de port inutilisés.

Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configurer le cryptage MACsec sur les commutateurs Cisco 9336C dans un site IP MetroCluster



Le cryptage MACsec ne peut être appliqué qu'aux ports WAN ISL.

Configurez le cryptage MACsec sur les commutateurs Cisco 9336C

Vous devez uniquement configurer le cryptage MACsec sur les ports WAN ISL qui s'exécutent entre les sites. Vous devez configurer MACsec après avoir appliqué le fichier RCF correct.

Conditions de licence pour MACsec

MACsec nécessite une licence de sécurité. Pour une explication complète du schéma de licence Cisco NX-OS et de la manière d'obtenir et de demander des licences, consultez le ["Guide des licences Cisco NX-OS"](#)

Activez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous pouvez activer le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL WAN dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Activer MACsec et MKA sur le périphérique :

```
feature macsec
```

```
IP_switch_A_1(config)# feature macsec
```

3. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configurer une chaîne de clé MACsec et des clés

Vous pouvez créer une chaîne de clés MACsec ou des clés sur votre configuration.

Key Lifetime et hitless Key Rollover

Un trousseau MACsec peut avoir plusieurs clés pré-partagées (PSK), chacune configurée avec un ID de clé et une durée de vie facultative. La durée de vie d'une clé indique à quel moment la clé s'active et expire. En l'absence d'une configuration à vie, la durée de vie par défaut est illimitée. Lorsqu'une durée de vie est configurée, MKA passe à la prochaine clé pré-partagée configurée dans le trousseau une fois la durée de vie écoulée. Le fuseau horaire de la clé peut être local ou UTC. Le fuseau horaire par défaut est UTC. Une clé peut se déployer sur une seconde clé dans le même trousseau si vous configurez la seconde clé (dans le trousseau) et configurez une durée de vie pour la première clé. Lorsque la durée de vie de la première clé expire, elle passe automatiquement à la clé suivante de la liste. Si la même clé est configurée sur les deux côtés de la liaison en même temps, le basculement de la clé est sans arrêt (c'est-à-dire, la clé se replace sans interruption de la circulation).

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. Pour masquer la chaîne d'octet de clé cryptée, remplacez la chaîne par un caractère générique dans la sortie du `show running-config` et `show startup-config` commandes :

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```



La chaîne octet est également masquée lorsque vous enregistrez la configuration dans un fichier.

Par défaut, les clés PSK sont affichées au format crypté et peuvent être déchiffrées facilement. Cette commande ne s'applique qu'aux chaînes de clés MACsec.

3. Créer une chaîne de clés MACsec pour contenir un jeu de clés MACsec et entrer le mode de configuration de la chaîne de clés MACsec :

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec  
IP_switch_A_1(config-macseckeychain)#
```

4. Créer une clé MACsec et entrer le mode de configuration de la clé MACsec :

```
key key-id
```

La plage est comprise entre 1 et 32 caractères hexadécimaux, et la taille maximale est de 64 caractères.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000  
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configurez la chaîne d'octet pour la clé :

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |  
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string  
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789  
cryptographic-algorithm AES_256_CMAC
```



L'argument octet-chaîne peut contenir jusqu'à 64 caractères hexadécimaux. La clé octet est codée en interne, de sorte que la clé en texte clair n'apparaît pas dans la sortie du `show running-config macsec` commande.

6. Configurer une durée de vie d'envoi pour la clé (en secondes) :

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00  
Oct 04 2020 duration 100000
```

Par défaut, l'appareil traite l'heure de début comme UTC. L'argument heure de début correspond à l'heure et à la date auxquelles la clé devient active. L'argument de durée est la durée de vie en secondes. La longueur maximale est de 2147483646 secondes (environ 68 ans).

7. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Affiche la configuration du trousseau :

```
show key chain name
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configurez une stratégie MACsec

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. Créer une stratégie MACsec :

```
macsec policy name
```

```
IP_switch_A_1(config)# macsec policy abc  
IP_switch_A_1(config-macsec-policy)#
```

3. Configurez l'un des chiffrements suivants : GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128 ou GCM-AES-XPB-256 :

```
cipher-suite name
```

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configurez la priorité du serveur de clés pour rompre le lien entre les pairs lors d'un échange de clés :

```
key-server-priority number
```

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configurez la stratégie de sécurité pour définir le traitement des données et des paquets de contrôle :

```
security-policy security policy
```

Choisissez une stratégie de sécurité parmi les options suivantes :

- Doit-Secure — les paquets qui ne portent pas les en-têtes MACsec sont supprimés

- Devrait-Secure — les paquets qui ne portent pas d'en-têtes MACsec sont autorisés (il s'agit de la valeur par défaut)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configurez la fenêtre de protection de relecture de sorte que l'interface sécurisée n'accepte pas un paquet dont la taille de fenêtre configurée est inférieure à celle de la fenêtre : `window-size number`



La taille de la fenêtre de protection de relecture représente le nombre maximum de trames hors séquence que MACsec accepte et ne sont pas supprimées. La plage va de 0 à 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configurer le temps en secondes pour forcer une nouvelle touche SAK :

```
sak-expiry-time time
```

Vous pouvez utiliser cette commande pour remplacer la clé de session par un intervalle de temps prévisible. La valeur par défaut est 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configurez l'un des décalages de confidentialité suivants dans la trame de couche 2 où le chiffrement commence :

```
conf-offsetconfidentiality offset
```

Choisissez parmi les options suivantes :

- CONF-OFFSET-0.
- CONF-OFFSET-30.
- CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```



Cette commande peut être nécessaire pour que les commutateurs intermédiaires utilisent des en-têtes de paquets (dmac, smac, etype) comme des balises MPLS.

9. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Afficher la configuration de la stratégie MACsec :

```
show macsec policy
```

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Activez le cryptage Cisco MACsec sur les interfaces

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. Sélectionnez l'interface que vous avez configurée avec le cryptage MACsec.

Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15  
switch(config-if)#
```

3. Ajoutez le trousseau et la stratégie à configurer sur l'interface pour ajouter la configuration MACsec :

```
macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. Répétez les étapes 1 et 2 sur toutes les interfaces où le cryptage MACsec doit être configuré.

5. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Désactivez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous devrez peut-être désactiver le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL du réseau étendu dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. Désactivez la configuration MACsec sur le périphérique :

```
macsec shutdown
```

```
IP_switch_A_1(config)# macsec shutdown
```



La sélection de l'option « non » restaure la fonction MACsec.

3. Sélectionnez l'interface que vous avez déjà configurée avec MACsec.

Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15  
switch(config-if)#
```

4. Supprimez le trousseau et la stratégie configurés sur l'interface pour supprimer la configuration MACsec :

```
no macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

5. Répétez les étapes 3 et 4 sur toutes les interfaces où MACsec est configuré.

6. Copier la configuration en cours d'exécution dans la configuration de démarrage :

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Vérification de la configuration MACsec

Étapes

1. Répétez **tous** des procédures précédentes sur le deuxième commutateur de la configuration pour établir une session MACsec.
2. Exécutez les commandes suivantes pour vérifier que les deux commutateurs sont chiffrés :
 - a. Exécuter : `show macsec mka summary`

- b. Exécuter : `show macsec mka session`
- c. Exécuter : `show macsec mka statistics`

Vous pouvez vérifier la configuration MACsec à l'aide des commandes suivantes :

Commande	Affiche des informations sur...
<code>show macsec mka session interface typeslot/port number</code>	La session MKA de MACsec pour une interface spécifique ou pour toutes les interfaces
<code>show key chain name</code>	La configuration de la chaîne de clés
<code>show macsec mka summary</code>	La configuration MACsec MKA
<code>show macsec policy policy-name</code>	Configuration d'une stratégie MACsec spécifique ou de toutes les politiques MACsec

Configurez les commutateurs IP NVIDIA

Configurer le commutateur NVIDIA IP SN2100 pour l'interconnexion de cluster et la connectivité IP MetroCluster backend

Vous devez configurer les switches IP NVIDIA SN2100 pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Réinitialiser les valeurs par défaut du commutateur NVIDIA IP SN2100

Vous pouvez choisir parmi les méthodes suivantes pour réinitialiser un commutateur sur les paramètres par défaut.

- [Réinitialisez le commutateur à l'aide de l'option de fichier RCF](#)
- [Téléchargez et installez le logiciel Cumulus](#)

Réinitialiser le commutateur à l'aide de l'option de fichier RCF

Avant d'installer une nouvelle configuration RCF, vous devez rétablir les paramètres du commutateur NVIDIA.

Description de la tâche

Pour restaurer les paramètres par défaut du commutateur, exécutez le fichier RCF avec le `restoreDefaults` option. Cette option copie les fichiers d'origine sauvegardés à leur emplacement d'origine, puis redémarre le commutateur. Après le redémarrage, le switch est en ligne avec la configuration d'origine qui existait au moment d'avoir exécuté le fichier RCF pour configurer le switch.

Les détails de configuration suivants ne sont pas réinitialisés :

- Configuration utilisateur et informations d'identification
- Configuration du port réseau de gestion, `eth0`



Toutes les autres modifications de configuration qui se produisent pendant l'application du fichier RCF sont rétablies à la configuration d'origine.

Avant de commencer

- Vous devez configurer le commutateur conformément à [Téléchargez et installez le fichier RCF NVIDIA](#). Si vous n'avez pas configuré cette méthode ou si des fonctionnalités supplémentaires ont été configurées avant d'exécuter le fichier RCF, vous ne pouvez pas suivre cette procédure.
- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur par une connexion de console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Vérifiez que la configuration RCF a été appliquée avec succès avec la même version ou une version de fichier RCF compatible et que les fichiers de sauvegarde sont bien en place.



Le résultat de cette commande peut afficher les fichiers de sauvegarde, les fichiers conservés, ou les deux. Si les fichiers de sauvegarde ou les fichiers conservés n'apparaissent pas dans le résultat, vous ne pouvez pas utiliser cette procédure.

```

cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
Backup files exist.
Preserved files exist.
Listing completion of the steps:
    Success: Step: 1: Performing Backup and Restore
    Success: Step: 2: updating MOTD file
    Success: Step: 3: Disabling apt-get
    Success: Step: 4: Disabling cdp
    Success: Step: 5: Adding lldp config
    Success: Step: 6: Creating interfaces
    Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
    Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
    Success: Step: 9: Configuring switch basic settings: ecn
    Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
    Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
    Success: Step: 12: Configuring switch basic settings: traffic
classification
    Success: Step: 13: Configuring LAG load balancing policies
    Success: Step: 14: Configuring the VLAN bridge
    Success: Step: 15: Configuring local cluster ISL ports
    Success: Step: 16: Configuring MetroCluster ISL ports
    Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
    Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
    Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
    Success: Step: 20: Configuring L2FC for MetroCluster interfaces
    Success: Step: 21: Configuring the interface to UP
    Success: Step: 22: Final commit
    Success: Step: 23: Final reboot of the switch
Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$

```

2. Exécutez le fichier RCF avec la possibilité de restaurer les valeurs par défaut : `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Répondez « oui » à l'invite. Le commutateur revient à la configuration d'origine et redémarre.
4. Attendez que le commutateur redémarre.

Le commutateur est réinitialisé et conserve la configuration initiale, telle que la configuration du réseau de gestion et les identifiants actuels qu'ils existaient avant d'appliquer le fichier RCF. Après le redémarrage, vous pouvez appliquer une nouvelle configuration en utilisant la même version ou une version différente du fichier RCF.

Téléchargez et installez le logiciel Cumulus

Description de la tâche

Suivez ces étapes pour réinitialiser complètement le commutateur en appliquant l'image Cumulus.

Avant de commencer

- Vous devez être connecté au commutateur par une connexion de console série.
- L'image logicielle du commutateur Cumulus est accessible via HTTP.



Pour plus d'informations sur l'installation de Cumulus Linux, voir ["Présentation de l'installation et de la configuration des switches NVIDIA SN2100"](#)

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.

Étapes

1. À partir de la console Cumulus, téléchargez et mettez en file d'attente l'installation du logiciel du commutateur avec la commande `onie-install -a -i` suivi du chemin du fichier vers le logiciel du commutateur :

Dans cet exemple, le fichier du micrologiciel `cumulus-linux-4.4.3-mlx-amd64.bin` Est copié du serveur HTTP '50.50.50.50' sur le commutateur local.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
#####
# 100.0%
```

```
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
```

```
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Répondez `y` à l'invite pour confirmer l'installation lors du téléchargement et de la vérification de l'image.
3. Redémarrez le commutateur pour installer le nouveau logiciel : `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```



Le commutateur redémarre et entre dans l'installation du logiciel du commutateur, ce qui prend un certain temps. Une fois l'installation terminée, le commutateur redémarre et reste à l'invite de connexion.

4. Configurer les paramètres de base du commutateur
 - a. Lorsque le commutateur est démarré et que vous êtes invité à ouvrir une session, connectez-vous et modifiez le mot de passe.



Le nom d'utilisateur est 'cumulus' et le mot de passe par défaut est 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configuration de l'interface réseau de gestion

Les commandes que vous utilisez dépendent de la version du micrologiciel du commutateur que vous exécutez.



L'exemple de commandes suivant configure le nom d'hôte en tant que IP_Switch_A_1, l'adresse IP en tant que 10.10.10.10, le masque de réseau en tant que 255.255.255.0 (24) et l'adresse de la passerelle en tant que 10.10.10.1.

Cumulus 4.4.x

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant Cumulus 4.4.x.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending
```

```
.
```

```
cumulus@cumulus:mgmt:~$ net commit
```

```
.
```

```
net add/del commands since the last "net commit"
```

User Timestamp Command

```
cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1
```

```
cumulus@cumulus:mgmt:~$
```

Cumulus 5.4.x et versions ultérieures

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant Cumulus 5.4.x. ou ultérieure.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. Redémarrez le commutateur à l'aide du `sudo reboot` commande.

```
cumulus@cumulus:~$ sudo reboot
```

Lorsque le commutateur redémarre, vous pouvez appliquer une nouvelle configuration en suivant les étapes de la section [Téléchargez et installez le fichier RCF NVIDIA](#).

Télécharger et installer les fichiers RCF NVIDIA

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

Avant de commencer

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.
- Le logiciel du commutateur est installé et le réseau de gestion est configuré.
- Vous avez suivi les étapes d'installation initiale du commutateur à l'aide de la méthode 1 ou de la méthode 2.
- Vous n'avez appliqué aucune configuration supplémentaire après l'installation initiale.



Si vous effectuez une autre configuration après la réinitialisation du commutateur et avant d'appliquer le fichier RCF, cette procédure ne peut pas être utilisée.

Description de la tâche

Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration IP MetroCluster (nouvelle installation) ou sur le commutateur de remplacement (remplacement du commutateur).

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Étapes

1. Générer les fichiers RCF NVIDIA pour MetroCluster IP.
 - a. Téléchargez le "[RcfFileGenerator pour MetroCluster IP](#)".
 - b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

- c. Accédez à votre répertoire personnel. Si vous êtes enregistré en tant que 'culus', le chemin du fichier est /home/cumulus.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

- d. Téléchargez le fichier RCF dans ce répertoire. L'exemple suivant montre que vous utilisez SCP pour télécharger le fichier SN2100_v2.0.0_IP_switch_A_1.txt du serveur '50.50.50.50' à votre répertoire personnel et enregistrez-le sous SN2100_v2.0.0_IP_switch_A_1.py:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*****
**
Banner of the SCP server
*****
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Exécutez le fichier RCF. Le fichier RCF requiert une option permettant d'appliquer une ou plusieurs étapes. Sauf instruction contraire du support technique, exécutez le fichier RCF sans l'option de ligne de commande. Pour vérifier l'état d'achèvement des différentes étapes du fichier RCF, utilisez l'option '-1' ou 'All' pour appliquer toutes les étapes (en attente).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes
```

... the steps will apply - this is generating a lot of output ...

Running Step 24: Final reboot of the switch

... The switch will reboot if all steps applied successfully ...

3. Si votre configuration utilise des câbles DAC, activez l'option DAC sur les ports de commutateur :

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

L'exemple suivant active l'option DAC pour le port swp7:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
Running cumulus version : 5.4.0
Running RCF file version : v2.00
Running command: Enabling the DacOption for port swp7
runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
runCmd: committed, ret: 0
Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. Redémarrez le commutateur après avoir activé l'option DAC sur les ports de commutateur :

```
sudo reboot
```



Lorsque vous définissez l'option DAC pour plusieurs ports de commutateur, vous ne devez redémarrer le commutateur qu'une seule fois.

Définissez la correction d'erreur de transfert pour les systèmes utilisant une connectivité de 25 Gbit/s.

Si votre système est configuré avec une connectivité de 25 Gbit/s, définissez manuellement le paramètre correction d'erreur de transfert (fec) sur Désactivé après l'application de la FCR. La FCR n'applique pas ce paramètre.

Description de la tâche

- Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s. Reportez-vous à la ["Affectations des ports de plateforme pour les switches IP SN2100 pris en charge par NVIDIA"](#).
- Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Définissez le `fec` paramètre sur Off pour le premier port de commutateur qui utilise une connectivité 25 Gbit/s :

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
```

2. Répétez l'étape pour chaque port de commutateur 25 Gbit/s connecté à un module de contrôleur.

Définissez la vitesse du port de commutateur pour les interfaces IP MetroCluster

Description de la tâche

- Utilisez cette procédure pour régler la vitesse du port de commutation sur 100 G pour les systèmes suivants :
 - AFF A70, AFF A90, AFF A1K, AFF C80
 - AFF A30, AFF C30, AFF A50, AFF C60
 - FAS50, FAS70, FAS90
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étape

1. Utilisez le fichier RCF avec `runCmd` l'option pour définir la vitesse. Ceci applique le paramètre et enregistre la configuration.

Les commandes suivantes définissent la vitesse des interfaces MetroCluster `swp7` et `swp8`:

```
sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
```

```
sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
```

Exemple

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
Running cumulus version : 5.4.0
Running RCF file version : v2.20
Running command: Setting switchport swp7 to 100G speed
runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
runCmd: 'nv set interface swp7 link speed 100G', ret: 0
runCmd: committed, ret: 0
Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles. Vous devez désactiver chaque port ou canal de port individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :



Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

```
net show interface
```

2. Désactivez les ports ISL et les canaux de port inutilisés à l'aide du fichier RCF.

```

cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version   : 5.4.0
    Running RCF file version  : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
    to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
        You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
        This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$

```

L'exemple de commande suivant désactive le port « swp14 » :

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Répétez cette étape pour chaque port ou canal de port non utilisé identifié.

Installer le fichier de configuration Ethernet Switch Health Monitor pour un commutateur IP NVIDIA SN2100 MetroCluster

Pour configurer la surveillance de l'état du commutateur Ethernet sur les commutateurs Ethernet NVIDIA, suivez cette procédure.

Ces instructions s'appliquent si les commutateurs NVIDIA X190006-PE et X190006-PI ne sont pas détectés

correctement, ce qui peut être confirmé en exécutant `system switch ethernet show` et vérifiez si **AUTRE** est affiché pour votre modèle. Pour identifier votre modèle de commutateur NVIDIA, recherchez sa référence à l'aide de la commande `nv show platform hardware` pour NVIDIA CL 5.8 et versions antérieures ou `nv show platform` pour les versions ultérieures.



Ces étapes sont également recommandées si vous souhaitez que la surveillance de l'intégrité et la collecte des journaux fonctionnent correctement lors de l'utilisation de NVIDIA CL 5.11.x avec les versions ONTAP suivantes. Bien que la surveillance de l'intégrité et la collecte des journaux puissent fonctionner sans ces étapes, leur respect garantit le bon fonctionnement de l'ensemble.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 et versions ultérieures des correctifs

Avant de commencer

- Assurez-vous que le cluster ONTAP est opérationnel.
- Activez SSH sur le commutateur pour utiliser toutes les fonctionnalités disponibles dans CSHM.
- Effacez le `/mroot/etc/cshm_nod/nod_sign/` répertoire sur tous les nœuds :

- a. Entrez le nodeshell :

```
system node run -node <name>
```

- b. Passer au privilège avancé :

```
priv set advanced
```

- c. Répertoriez les fichiers de configuration dans le `/etc/cshm_nod/nod_sign` répertoire. Si le répertoire existe et contient des fichiers de configuration, il répertorie les noms des fichiers.

```
ls /etc/cshm_nod/nod_sign
```

- d. Supprimez tous les fichiers de configuration correspondant à vos modèles de commutateurs connectés.

Si vous n'êtes pas sûr, supprimez tous les fichiers de configuration pour les modèles pris en charge répertoriés ci-dessus, puis téléchargez et installez les derniers fichiers de configuration pour ces mêmes modèles.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Vérifiez que les fichiers de configuration supprimés ne se trouvent plus dans le répertoire :

```
ls /etc/cshm_nod/nod_sign
```

Étapes

1. Téléchargez le fichier zip de configuration du moniteur d'état du commutateur Ethernet basé sur la version ONTAP correspondante. Ce fichier est disponible à partir de la "[Switchs Ethernet NVIDIA](#)" page.
 - a. Sur la page de téléchargement du logiciel NVIDIA SN2100, sélectionnez **Nvidia CSHM File**.
 - b. Sur la page attention/doit lire, cochez la case pour accepter.

- c. Sur la page Contrat de licence utilisateur final, cochez la case accepter et cliquez sur **accepter et continuer**.
- d. Sur la page Nvidia CSHM File - Download, sélectionnez le fichier de configuration applicable. Les fichiers suivants sont disponibles :

ONTAP 9.15.1 et versions ultérieures

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 à 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. chargez le fichier zip applicable sur votre serveur Web interne.
2. Accédez au paramètre de mode avancé à partir d'un des systèmes ONTAP du cluster.

```
set -privilege advanced
```

3. Exécutez la commande switch Health Monitor configure.

```
cluster1::> system switch ethernet configure-health-monitor
```

4. Vérifiez que le résultat de la commande se termine par le texte suivant pour votre version de ONTAP :

ONTAP 9.15.1 et versions ultérieures

La surveillance de l'état du commutateur Ethernet a installé le fichier de configuration.

ONTAP 9.11.1 à 9.14.1

SHM a installé le fichier de configuration.

ONTAP 9.10.1

Le package CSHM téléchargé a été traité avec succès.

En cas d'erreur, contactez le support NetApp.

1. attendez jusqu'à deux fois l'intervalle d'interrogation du moniteur d'état du commutateur Ethernet, détecté en exécutant `system switch ethernet polling-interval show`, avant de terminer l'étape suivante.
2. Exécutez la commande `system switch ethernet configure-health-monitor show` sur le système ONTAP et assurez-vous que les commutateurs du cluster sont détectés avec le champ surveillé

défini sur **Vrai** et le champ du numéro de série n'affichant pas **Inconnu**.

```
cluster1::> system switch ethernet configure-health-monitor show
```



Si votre modèle affiche toujours **OTHER** après avoir appliqué le fichier de configuration, contactez le support NetApp.

Voir le ["configuration-santé-surveillance du commutateur Ethernet du système"](#) commande pour plus de détails.

Et la suite ?

["Configurer la surveillance de l'état des commutateurs"](#).

Surveiller l'état du commutateur IP MetroCluster

En savoir plus sur la surveillance de l'état des commutateurs dans une configuration IP MetroCluster

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage.

Remarques importantes pour la configuration de CSHM dans une configuration IP MetroCluster

Cette section présente les étapes générales de configuration de SNMPv3 et de collecte de journaux sur les commutateurs Cisco, Broadcom et NVIDIA SN2100. Vous devez suivre les étapes correspondant à la version du firmware du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le ["Hardware Universe"](#) pour vérifier les versions de firmware prises en charge.

Dans une configuration MetroCluster, vous configurez la surveillance de l'état sur les commutateurs de cluster locaux uniquement.

Pour la collecte des journaux avec les commutateurs Broadcom et Cisco, un nouvel utilisateur doit être créé sur le commutateur pour chaque cluster dont la collecte des journaux est activée. Dans une configuration MetroCluster, cela signifie que MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d'un utilisateur distinct sur les commutateurs. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l'utilisateur.

Avant de configurer le CSHM, vous devez désactiver les ISL inutilisés pour éviter toute alerte ISL inutile.

Configurer SNMPv3 pour surveiller la santé des commutateurs IP MetroCluster

Dans les configurations MetroCluster IP, vous pouvez configurer SNMPv3 pour surveiller l'état des commutateurs IP.

Cette procédure montre les étapes génériques de configuration de SNMPv3 sur un commutateur. Certaines versions du micrologiciel du commutateur répertoriées peuvent ne pas être prises en charge dans une configuration IP MetroCluster.

Vous devez suivre les étapes correspondant à la version du micrologiciel du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le "[Hardware Universe](#)" pour vérifier les versions de firmware prises en charge.



- SNMPv3 n'est pris en charge que sur ONTAP 9.12.1 et versions ultérieures.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 et les versions ultérieures corrigent ces deux problèmes :
 - "[Pour la surveillance de l'état ONTAP des commutateurs Cisco, le trafic SNMPv2 peut toujours être visible après le passage à SNMPv3 pour la surveillance](#)"
 - "[Alertes de ventilateur et d'alimentation de commutateur faussement positives en cas de pannes SNMP](#)"

Description de la tâche

Les commandes suivantes sont utilisées pour configurer un nom d'utilisateur SNMPv3 sur les commutateurs **Broadcom**, **Cisco** et **NVIDIA** :

Commutateurs Broadcom

Configurez un nom d'utilisateur SNMPv3 OPÉRATEUR RÉSEAU sur les commutateurs Broadcom BES-53248.

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-md5|auth-sha] [priv-aes128|priv-des]
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp  
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version  
SNMPv3 -community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp status
```

```
(sw1) (Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>
```

```
(cs1) (Config)# show snmp user snmp
```

Name	Group Name	Auth Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>

```

4. Après avoir attendu la période d'interrogation CSHM, vérifiez que le numéro de série est renseigné pour le commutateur Ethernet.

```

system switch ethernet polling-interval show

```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: <username>
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

```

Commutateurs Cisco

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs Cisco 9336C-FX2 :

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3_USER NoAuth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp user
```

```
(sw1) (Config) # snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config) # show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config) #
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1  
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true
```

```
cluster1::*> security login create -user-or-group-name <username>  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance
```

```
Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
```

```
Cluster/HA/RDMA
```

```
cluster1::*>
```

```
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

```
cluster1::*>
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```



```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>

```

NVIDIA - CL 5.4.0

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.4.0 :

- Pour **pas d'authentification** :

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          4318
Version 1 and 2c Community String Configured
Version 3 Usernames     Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrorMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```

pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username
SNMPv3User	auth-md5 <password>	encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames     Configured    <---- Configured
here
-----

```

```

cumulus@sw1:~$

```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

NVIDIA - CL 5.11.0

Configurez un nom d'utilisateur SNMPv3 `SNMPv3_USER` sur les commutateurs NVIDIA SN2100 exécutant CLI 5.11.0 :

- Pour **pas d'authentification** :

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server
                                applied
-----
[username]                      SNMPv3_USER
[username]                      limiteduser1
[username]                      testuserauth
[username]                      testuserauthaes
[username]                      testusernoauth
trap-link-up
  check-frequency                60
trap-link-down
  check-frequency                60
[listening-address]             all
[readonly-community]            $nvsec$94d69b56e921aec1790844eb53e772bf
state                           enabled
cumulus@sw1:~$
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```



```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

Configurer la collecte de journaux sur un commutateur IP MetroCluster

Dans une configuration IP MetroCluster, vous pouvez configurer la collecte de journaux pour collecter les journaux de commutation à des fins de débogage.



Sur les commutateurs Broadcom et Cisco, un nouvel utilisateur est requis pour chaque cluster avec collecte de journaux. Par exemple, MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d'un utilisateur distinct sur les commutateurs. L'utilisation de plusieurs clés SSH pour un même utilisateur n'est pas prise en charge.

Description de la tâche

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage. Cette procédure vous guide tout au long du processus de configuration de la collecte, de demande de journaux **support** détaillés et d'activation d'une collecte horaire de données **périodiques** collectées par AutoSupport.

REMARQUE : si vous activez le mode FIPS, vous devez effectuer les opérations suivantes :



1. Régénérer les clés SSH sur le commutateur en suivant les instructions du fournisseur.
2. Régénérer les clés SSH dans ONTAP à l'aide de `debug system regenerate-systemshell-key-pair`
3. Réexécutez la routine de configuration de la collecte des journaux à l'aide de la `system switch ethernet log setup-password` commande

Avant de commencer

- L'utilisateur doit avoir accès aux commandes du commutateur `show`. S'ils ne sont pas disponibles, créez un nouvel utilisateur et accordez les autorisations nécessaires à l'utilisateur.
- La surveillance de l'état du commutateur doit être activée pour le commutateur. Vérifiez cela en vous assurant que `Is Monitored`: le champ est défini sur **true** dans la sortie du `system switch ethernet show` commande.
- Pour la collecte de journaux avec les commutateurs Broadcom et Cisco :
 - L'utilisateur local doit disposer de privilèges d'administrateur réseau.
 - Un nouvel utilisateur doit être créé sur le commutateur pour chaque configuration de cluster avec la collecte des journaux activée. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l'utilisateur.
- Pour la prise en charge de la collecte de journaux avec les commutateurs NVIDIA, *user* pour la collecte de journaux doit être autorisé à exécuter la `cl-support` commande sans avoir à fournir de mot de passe. Pour autoriser cette utilisation, lancer la commande :

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee  
-a' visudo -f /etc/sudoers.d/cumulus
```

Étapes

ONTAP 9.15.1 et versions ultérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

REMARQUE : Si vous répondez **y** à l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessaires comme indiqué dans [Avant de commencer](#) .

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs1
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs2
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```



Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Activer la collecte périodique des journaux :

```
system switch ethernet log modify -device <switch-name> -periodic  
-enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs1: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs2: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	true	scheduled
never-run		
cs2	true	scheduled
never-run		

2 entries were displayed.

2. Demander la collecte du journal de support :

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1
```

cs1: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> system switch ethernet log collect-support-log -device
cs2
```

cs2: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> *system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	false	halted
initiated		
cs2	true	scheduled
initiated		

2 entries were displayed.

3. Pour afficher tous les détails de la collecte des journaux, y compris l'activation, le message d'état, l'horodatage précédent et le nom de fichier de la collecte périodique, l'état de la demande, le message d'état, ainsi que l'horodatage précédent et le nom de fichier de la collection de support, utilisez les éléments suivants :

```
system switch ethernet log show -instance
```

```

cluster1::*> system switch ethernet log show -instance

Switch Name: cs1
Periodic Log Enabled: true
Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
Last Periodic Log Timestamp: 3/11/2024 11:02:59
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:14:20
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

Switch Name: cs2
Periodic Log Enabled: false
Periodic Log Status: Periodic collection has been
halted.
Last Periodic Log Timestamp: 3/11/2024 11:05:18
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:18:54
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.

```

ONTAP 9.14.1 et versions antérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

REMARQUE : si vous répondez à y l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessaires [Avant de commencer](#), comme indiqué dans .

```
system switch ethernet log setup-password
```

```

cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

```



Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Pour demander la collecte des journaux d'assistance et activer la collecte périodique, exécutez la commande suivante. Ceci lance les deux types de collecte de journaux : les journaux détaillés Support et une collecte de données toutes les heures Periodic .

```

system switch ethernet log modify -device <switch-name> -log-request
true

```



```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Attendez 10 minutes, puis vérifiez que la collecte des journaux se termine :

```
system switch ethernet log show
```



Si des États d'erreur sont signalés par la fonction de collecte de journaux (visible dans la sortie de `system switch ethernet log show`), voir ["Dépannage de la collecte des journaux"](#) pour plus de détails.

Gérer la surveillance des commutateurs Ethernet dans une configuration IP MetroCluster

Dans la plupart des cas, les commutateurs Ethernet sont automatiquement détectés par ONTAP et surveillés par CSHM. Le fichier de configuration de référence (RCF) appliqué au commutateur, entre autres, active le protocole CDP (Cisco Discovery Protocol) et/ou le protocole LLDP (Link Layer Discovery Protocol). Cependant, vous devrez peut-être ajouter manuellement un commutateur qui n'est pas détecté ou supprimer un commutateur qui n'est plus utilisé. Vous pouvez également arrêter la surveillance active tout en maintenant le commutateur dans la configuration, par exemple pendant la maintenance.

Créez une entrée de commutateur afin que ONTAP puisse la surveiller

Description de la tâche

Utilisez `system switch ethernet create` la commande pour configurer et activer manuellement la surveillance d'un commutateur Ethernet spécifié. Ceci est utile si ONTAP n'ajoute pas automatiquement le commutateur, ou si vous avez précédemment supprimé le commutateur et souhaitez le rajouter.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshml! -model NX3132V -type
cluster-network
```

Un exemple type est l'ajout d'un commutateur nommé [DeviceName], avec l'adresse IP 1.2.3.4, et les informations d'identification SNMPv2c définies sur **cshml!**. Utilisez `-type storage-network` plutôt que `-type cluster-network` si vous configurez un commutateur de stockage.

Désactiver la surveillance sans supprimer le commutateur

Si vous souhaitez mettre en pause ou arrêter la surveillance d'un certain commutateur, mais le conserver pour une surveillance future, modifiez son `is-monitoring-enabled-admin` paramètre au lieu de le supprimer.

Par exemple :

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Cela vous permet de préserver les détails et la configuration du commutateur sans générer de nouvelles alertes ou de nouvelles découvertes.

Retirez un commutateur dont vous n'avez plus besoin

Utiliser `system switch ethernet delete` pour supprimer un commutateur qui a été déconnecté ou n'est plus nécessaire :

```
system switch ethernet delete -device DeviceName
```

Par défaut, cette commande réussit uniquement si ONTAP ne détecte pas actuellement le commutateur via CDP ou LLDP. Pour supprimer un commutateur découvert, utilisez le `-force` paramètre :

```
system switch ethernet delete -device DeviceName -force
```

Lorsque `-force` est utilisé, le commutateur peut être ajouté automatiquement si ONTAP le détecte à nouveau.

Vérifier la surveillance du commutateur Ethernet dans une configuration IP MetroCluster

Le moniteur d'état du commutateur Ethernet (CSHM) tente automatiquement de surveiller les commutateurs qu'il découvre ; cependant, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

Confirmez la surveillance des commutateurs Ethernet connectés

Description de la tâche

Pour vérifier que les commutateurs Ethernet connectés sont surveillés, exécutez :

```
system switch ethernet show
```

Si la colonne affiche **OTHER** ou si Model le IS Monitored champ affiche **FALSE**, ONTAP ne peut pas surveiller le commutateur. Une valeur de **AUTRE** indique généralement que ONTAP ne prend pas en charge ce commutateur pour la surveillance de l'intégrité.

Le IS Monitored champ est défini sur **FALSE** pour la raison spécifiée dans le Reason champ.



Si un commutateur n'est pas répertorié dans la sortie de commande, ONTAP ne l'a probablement pas découvert. Vérifiez que le commutateur est correctement câblé. Si nécessaire, vous pouvez ajouter le commutateur manuellement. Voir ["Gérer la surveillance des commutateurs Ethernet"](#) pour plus de détails.

Vérifiez que les versions du firmware et des fichiers RCF sont à jour

Assurez-vous que le commutateur exécute le micrologiciel le plus récent pris en charge et qu'un fichier RCF compatible a été appliqué. Plus d'informations sont disponibles sur le ["Page des téléchargements du support NetApp"](#).

Par défaut, le moniteur d'intégrité utilise SNMPv2c avec la chaîne de communauté **csbm1!** pour la surveillance, mais SNMPv3 peut également être configuré.

Si vous devez modifier la chaîne de communauté SNMPv2c par défaut, assurez-vous que la chaîne de communauté SNMPv2c souhaitée a été configurée sur le commutateur.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c  
-community-or-username newCommunity!
```



Pour plus d'informations sur la configuration de SNMPv3 pour utilisation, reportez-vous à la section ["Facultatif : configurer SNMPv3"](#).

Confirmez la connexion au réseau de gestion

Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

Une connexion de port de gestion correcte est requise pour que ONTAP puisse effectuer des requêtes SNMP et collecter des journaux.

Informations associées

- ["Résolution des alertes"](#)

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.