



# **Procédures de maintenance pour les configurations MetroCluster IP**

## **ONTAP MetroCluster**

NetApp  
September 06, 2024

# Sommaire

- Procédures de maintenance pour les configurations MetroCluster IP ..... 1
  - Modifiez les propriétés d'une interface IP MetroCluster..... 1
  - Maintenance et remplacement du commutateur IP ..... 5
  - Identification du stockage dans une configuration MetroCluster IP ..... 31
  - Ajout de tiroirs à un IP MetroCluster à l'aide des commutateurs MetroCluster de stockage partagé ..... 35
  - Configurer le chiffrement de bout en bout dans une configuration MetroCluster IP ..... 51
  - Mettez le système hors tension et sous tension sur un seul site dans une configuration MetroCluster IP .. 55
  - Mise hors tension de l'intégralité d'une configuration MetroCluster IP ..... 62

# Procédures de maintenance pour les configurations MetroCluster IP

## Modifiez les propriétés d'une interface IP MetroCluster

Depuis ONTAP 9.10.1, vous pouvez modifier les propriétés suivantes d'une interface IP MetroCluster : adresse IP et masque, et passerelle. Vous pouvez utiliser n'importe quelle combinaison de paramètres pour la mise à jour.

Vous devrez peut-être mettre à jour ces propriétés, par exemple si une adresse IP dupliquée est détectée ou si une passerelle doit changer dans le cas d'un réseau de couche 3 en raison de modifications de configuration du routeur.

### Description de la tâche

- Vous ne pouvez modifier qu'une interface à la fois. Cette interface entraînera une perturbation du trafic jusqu'à ce que les autres interfaces soient mises à jour et que les connexions soient réétablies.
- Utilisez le `metrocluster configuration-settings interface modify` Commande permettant de modifier toute propriété d'interface IP MetroCluster.



Ces commandes permettent de modifier la configuration d'un nœud spécifique pour un port particulier. Pour restaurer la connectivité réseau complète, des commandes similaires sont nécessaires sur d'autres ports. De même, les commutateurs réseau doivent également mettre à jour leur configuration. Par exemple, si la passerelle est mise à jour, elle est idéalement modifiée sur les deux nœuds d'une paire haute disponibilité, car ils sont identiques. De plus, le switch connecté à ces nœuds doit également mettre à jour sa passerelle.

- Utilisez les `metrocluster configuration-settings interface show` commandes , `\metrocluster connection check` et `\metrocluster connection show` pour vérifier que toutes les connexions fonctionnent dans toutes les interfaces.

## Modifiez l'adresse IP, le masque de réseau et la passerelle

Procédez comme suit pour modifier l'adresse IP, le masque de réseau et la passerelle d'une interface IP MetroCluster.

### Étapes

1. Mettez à jour l'adresse IP, le masque de réseau et la passerelle pour un seul nœud et une seule interface :  
`metrocluster configuration-settings interface modify`

La commande suivante indique comment mettre à jour l'adresse IP, le masque de réseau et la passerelle :

```

cluster_A::~* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsil3:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsil4:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsil5:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsil6:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::~*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful

```

2. Vérifiez que toute la connectivité fonctionne pour toutes les interfaces :metrocluster configuration-settings interface show

La commande suivante indique comment vérifier que toute la connectivité fonctionne pour toutes les interfaces :

```

cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR          Config
Group Cluster Node   Network Address Netmask      Gateway
State
-----
1          cluster_A node_A_2
           Home Port: e0a-10
           192.168.12.201 255.255.254.0 192.168.12.1
completed
           Home Port: e0b-20
           192.168.20.200 255.255.255.0 192.168.20.1
completed
           node_A_1
           Home Port: e0a-10
           192.168.12.101 255.255.254.0 192.168.12.1
completed
           Home Port: e0b-20
           192.168.20.101 255.255.255.0 192.168.20.1
completed
           cluster_B node_B_1
           Home Port: e0a-10
           192.168.11.151 255.255.255.0 192.168.11.1
completed
           Home Port: e0b-20
           192.168.21.150 255.255.255.0 192.168.21.1
completed
           node_B_2
           Home Port: e0a-10
           192.168.11.250 255.255.255.0 192.168.11.1
completed
           Home Port: e0b-20
           192.168.21.250 255.255.255.0 192.168.21.1
completed
8 entries were displayed.

```

### 3. Vérifiez que toutes les connexions fonctionnent :

```
metrocluster configuration-settings connection show
```

La commande suivante indique comment vérifier que toutes les connexions fonctionnent :

```

cluster_A::*> metrocluster configuration-settings connection show
(metrocluster configuration-settings connection show)
DR
Group Cluster Node      Source          Destination
Config State           Network Address Network Address Partner Type
-----
1      cluster_A node_A_2
      Home Port: e0a-10
      192.168.10.200 192.168.10.101 HA Partner
completed
      Home Port: e0a-10
      192.168.10.200 192.168.11.250 DR Partner
completed
      Home Port: e0a-10
      192.168.10.200 192.168.11.151 DR Auxiliary
completed
      Home Port: e0b-20
      192.168.20.200 192.168.20.100 HA Partner
completed
      Home Port: e0b-20
      192.168.20.200 192.168.21.250 DR Partner
completed
      Home Port: e0b-20
      192.168.20.200 192.168.21.150 DR Auxiliary
completed
      node_A_1
      Home Port: e0a-10
      192.168.10.101 192.168.10.200 HA Partner
completed
      Home Port: e0a-10
      192.168.10.101 192.168.11.151 DR Partner
completed
      Home Port: e0a-10
      192.168.10.101 192.168.11.250 DR Auxiliary
completed
      Home Port: e0b-20
      192.168.20.100 192.168.20.200 HA Partner
completed
      Home Port: e0b-20
      192.168.20.100 192.168.21.150 DR Partner
completed
      Home Port: e0b-20
      192.168.20.100 192.168.21.250 DR Auxiliary
completed

```

# Maintenance et remplacement du commutateur IP

## Remplacez un commutateur IP ou modifiez l'utilisation des commutateurs IP MetroCluster existants

Vous devrez peut-être remplacer un commutateur défectueux, mettre à niveau ou rétrograder un commutateur, ou modifier l'utilisation des commutateurs IP MetroCluster existants.

### Description de la tâche

Cette procédure s'applique lorsque vous utilisez des commutateurs validés par NetApp. Si vous utilisez des switchs conformes à MetroCluster, reportez-vous au fournisseur du commutateur.

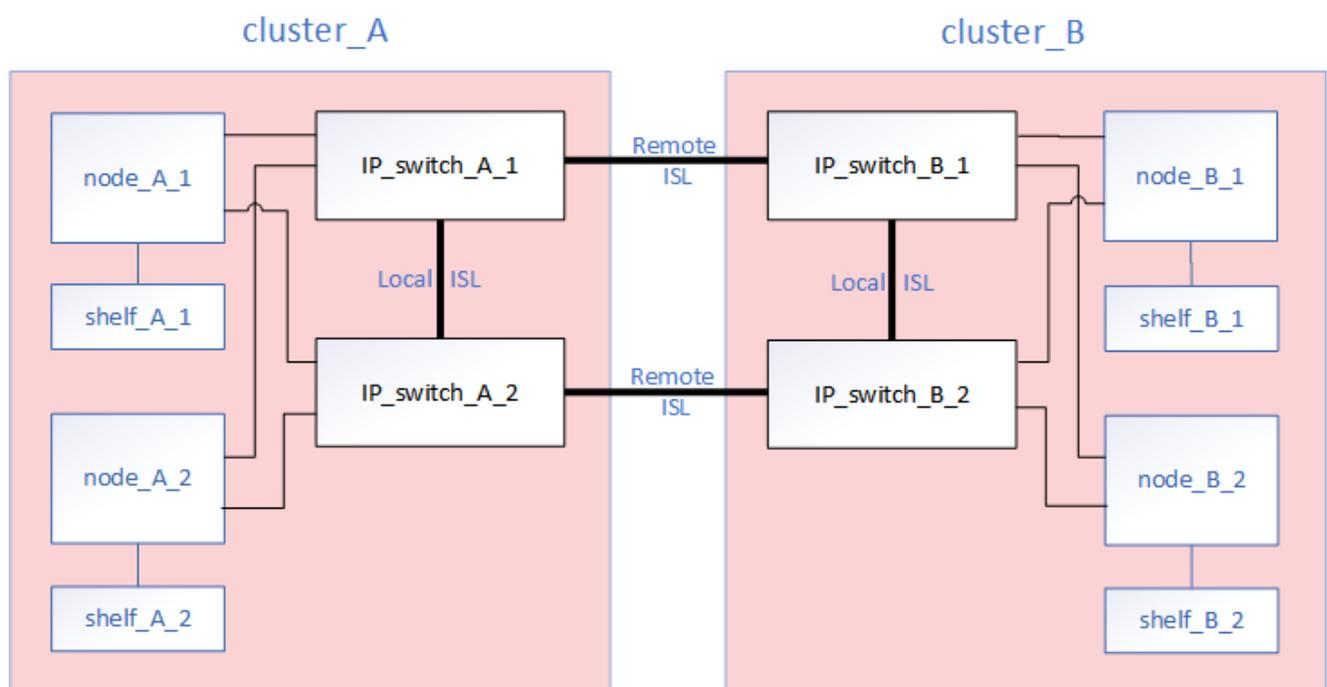
["Activer la journalisation de la console"](#) avant d'effectuer cette tâche.

Cette procédure prend en charge les conversions suivantes :

- Modification du fournisseur, du type ou des deux commutateurs. Le nouveau commutateur peut être identique à l'ancien commutateur en cas de défaillance d'un commutateur ou vous pouvez modifier le type de commutateur (mettre à niveau ou rétrograder le commutateur).

Par exemple, pour étendre une configuration IP MetroCluster d'une configuration unique à quatre nœuds à l'aide de contrôleurs AFF A400 et de commutateurs BES-53248 à une configuration à huit nœuds à l'aide de contrôleurs AFF A400, vous devez remplacer les commutateurs par un type pris en charge pour la configuration, car les commutateurs BES-53248 ne sont pas pris en charge dans la nouvelle configuration.

Si vous souhaitez remplacer un commutateur défectueux par le même type de commutateur, vous devez remplacer uniquement le commutateur défectueux. Si vous souhaitez mettre à niveau ou rétrograder un commutateur, vous devez régler deux commutateurs situés sur le même réseau. Deux commutateurs se trouvent sur le même réseau lorsqu'ils sont connectés via une liaison ISL et non sur le même site. Par exemple, le réseau 1 inclut IP\_switch\_A\_1 et IP\_switch\_B\_1, et le réseau 2 inclut IP\_switch\_A\_2 et IP\_switch\_B\_2, comme indiqué dans le schéma ci-dessous :





Si vous remplacez un switch ou effectuez une mise à niveau vers d'autres switches, vous pouvez préconfigurer les switches en installant le firmware du switch et le fichier RCF.

- Convertissez une configuration IP MetroCluster en configuration IP MetroCluster à l'aide de commutateurs MetroCluster de stockage partagé.

Par exemple, si vous disposez d'une configuration IP MetroCluster standard avec les contrôleurs AFF A700 et que vous souhaitez reconfigurer le MetroCluster pour connecter les tiroirs NS224 aux mêmes switches.



- Si vous ajoutez ou supprimez des tiroirs dans une configuration MetroCluster IP à l'aide de commutateurs MetroCluster IP de stockage partagé, suivez les étapes de la section ["Ajout de tiroirs à une adresse IP MetroCluster à l'aide de commutateurs MetroCluster de stockage partagé"](#)
- Votre configuration IP MetroCluster peut déjà se connecter directement aux tiroirs NS224 ou aux commutateurs de stockage dédiés.

### Fiche technique d'utilisation des ports

Voici un exemple de feuille de calcul pour la conversion d'une configuration MetroCluster IP en une configuration de stockage partagé qui connecte deux tiroirs NS224 à l'aide des commutateurs existants.

Définitions de feuille de calcul :

- Configuration existante : câblage de la configuration MetroCluster existante.
- Nouvelle configuration avec les tiroirs NS224 : configuration cible dans laquelle les switches sont partagés entre le stockage et le MetroCluster.

Les champs mis en surbrillance dans cette feuille de calcul indiquent les éléments suivants :

- Vert : vous n'avez pas besoin de changer le câblage.
- Jaune : vous devez déplacer des ports avec une configuration identique ou différente.
- Bleu : ports qui sont de nouvelles connexions.

PORT USAGE OVERVIEW

Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G

Switch port	Existing configuration			New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2	Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'		Cluster Port 'A'	Cluster Port 'B'
3						
4						
5				Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6					NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8						
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'		Port 'A'	Port 'B'
11						
12						
13				ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14						
15						
16						
17				MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18					Storage Port 'A'	Storage Port 'B'
19						
20						
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G	Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22					NSM-B, e0a	NSM-B, e0b
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						

## Étapes

1. Vérifiez l'état de santé de la configuration.
  - a. Vérifier que la MetroCluster est configurée et en mode normal sur chaque cluster : **metrocluster show**

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

- b. Vérifier que la mise en miroir est activée sur chaque nœud : **metrocluster node show**

```
cluster_A::> metrocluster node show
DR                                     Configuration  DR
Group Cluster Node                    State          Mirroring Mode
-----
-----
1      cluster_A
      node_A_1      configured     enabled      normal
      cluster_B
      node_B_1      configured     enabled      normal
2 entries were displayed.
```

- c. Vérifier que les composants MetroCluster sont sains : **metrocluster check run**

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

```
Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
4 entries were displayed.
```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

d. Vérifier qu'il n'y a pas d'alerte de santé : **system health alert show**

2. Configurer le nouveau commutateur avant l'installation.

Si vous réutilisez des commutateurs existants, passez à l' [Étape 4](#).



Si vous mettez à niveau ou déclarez les commutateurs, vous devez configurer tous les commutateurs du réseau.

Suivez les étapes de la section *Configuration des commutateurs IP* dans "[Installation et configuration de MetroCluster IP](#)."

Assurez-vous d'appliquer le fichier RCF approprié pour le commutateur `_A_1`, `_A_2`, `_B_1` ou `_B_2`. Si le nouveau switch est identique à l'ancien switch, vous devez appliquer le même fichier RCF.

Si vous mettez à niveau ou déclasser un commutateur, appliquez le fichier RCF le plus récent pris en charge pour le nouveau commutateur.

3. Lancer la commande `port show` pour afficher des informations sur les ports réseau :

**network port show**

a. Modifier toutes les LIFs de cluster pour désactiver auto-revert :

```
network interface modify -vserver <vserver_name> -lif <lif_name>
-auto-revert false
```

4. déconnectez les connexions de l'ancien commutateur.



Vous ne déconnectez que les connexions qui n'utilisent pas le même port dans les anciennes et les nouvelles configurations. Si vous utilisez de nouveaux commutateurs, vous devez déconnecter toutes les connexions.

Déposer les connexions dans l'ordre suivant :

- a. Déconnectez les interfaces locales du cluster
- b. Déconnectez les liens ISL locaux du cluster
- c. Déconnectez les interfaces IP MetroCluster
- d. Déconnectez les liens ISL MetroCluster

Dans l'exemple [\[port\\_usage\\_worksheet\]](#), les commutateurs ne changent pas. Les liens ISL de MetroCluster sont déplacés et doivent être déconnectés. Vous n'avez pas besoin de déconnecter les connexions marquées en vert sur la feuille de travail.

5. Si vous utilisez de nouveaux commutateurs, mettez l'ancien commutateur hors tension, retirez les câbles et retirez physiquement l'ancien commutateur.

Si vous réutilisez des commutateurs existants, passez à l' [Étape 6](#).



Ne câblez **pas** les nouveaux commutateurs à l'exception de l'interface de gestion (le cas échéant).

6. configurez les commutateurs existants.

Si vous avez déjà préconfiguré les commutateurs, vous pouvez ignorer cette étape.

Pour configurer les switches existants, suivez la procédure d'installation et de mise à niveau des fichiers du micrologiciel et des fichiers RCF :

- ["Mise à niveau du micrologiciel sur les commutateurs IP MetroCluster"](#)
- ["Mettre à niveau les fichiers RCF sur les commutateurs IP MetroCluster"](#)

7. Câbler les commutateurs.

Vous pouvez suivre les étapes de la section *câblage des commutateurs IP* de la section ["Installation et configuration de MetroCluster IP"](#).

Câblez les interrupteurs dans l'ordre suivant (si nécessaire) :

- a. Reliez les liens ISL au site distant.
- b. Reliez les interfaces IP MetroCluster.
- c. Reliez les interfaces locales du cluster.



- Les ports utilisés peuvent être différents de ceux de l'ancien commutateur si le type de commutateur est différent. Si vous effectuez une mise à niveau ou une rétrogradation des commutateurs, procédez à **PAS** de câble reliant les liens ISL locaux. Connectez les liens ISL locaux uniquement si vous mettez à niveau ou rétrogradez les switchs du second réseau, et que les deux commutateurs d'un site présentent le même type et le même câblage.
- Si vous mettez à niveau les commutateurs A1 et B1, vous devez effectuer les étapes 1 à 6 pour les commutateurs A2 et B2.

#### 8. Finalisez le câblage local du cluster.

- a. Si les interfaces de cluster locales sont connectées à un commutateur :
  - i. Reliez les liens ISL du cluster local.
- b. Si les interfaces de cluster locales sont **non** connectées à un commutateur :
  - i. Utilisez le "[Migrer vers un environnement de cluster NetApp commuté](#)" procédure de conversion d'un cluster sans commutateur en cluster avec commutateur. Utilisez les orifices indiqués dans "[Installation et configuration de MetroCluster IP](#)" Ou les fichiers de câblage RCF pour connecter l'interface de cluster locale.

#### 9. Mettez le ou les commutateurs sous tension.

Si le nouveau commutateur est le même, mettez le nouveau commutateur sous tension. Si vous effectuez une mise à niveau ou une rétrogradation des commutateurs, mettez les deux commutateurs sous tension. La configuration peut fonctionner avec deux commutateurs différents sur chaque site jusqu'à la mise à jour du second réseau.

#### 10. Vérifiez que la configuration MetroCluster fonctionne correctement en répétant cette procédure [Étape 1](#).

Si vous effectuez une mise à niveau ou une rétrogradation des commutateurs du premier réseau, vous pouvez voir certaines alertes relatives à la mise en grappe locale.



Si vous mettez à niveau ou déclarez les réseaux, répétez toutes les étapes pour le second réseau.

#### 11. Modifier toutes les LIFs de cluster pour réactiver auto-revert :

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

#### 12. Vous pouvez également déplacer les tiroirs NS224.

Si vous reconfigurez une configuration IP MetroCluster qui ne connecte pas les tiroirs NS224 aux commutateurs IP MetroCluster, suivez la procédure appropriée pour ajouter ou déplacer les tiroirs NS224 :

- "[Ajout de tiroirs à une adresse IP MetroCluster à l'aide de commutateurs MetroCluster de stockage partagé](#)"
- "[Migrez depuis un cluster sans commutateur avec du stockage DAS](#)"
- "[Migrer d'une configuration sans commutateur vers un système de stockage FAS par commutateur en réutilisant les commutateurs de stockage](#)"

## Ports d'interface IP MetroCluster en ligne ou hors ligne

Lorsque vous effectuez des tâches de maintenance, vous devrez peut-être mettre un port d'interface IP MetroCluster hors ligne ou en ligne.

### Description de la tâche

"[Activer la journalisation de la console](#)" avant d'effectuer cette tâche.

### Étapes

Vous pouvez procéder comme suit pour mettre en ligne ou mettre hors ligne un port d'interface IP MetroCluster.

1. Définissez le niveau de privilège sur avancé.

```
set -privilege advanced
```

### Exemple de sortie

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
           directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. Mettre le port d'interface IP MetroCluster hors ligne.

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

### Exemple de sortie

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

- a. Vérifiez que l'interface IP de MetroCluster est hors ligne.

```
Cluster_A1::*> system ha interconnect port show
```

### Exemple de sortie

```
Cluster_A1::*> system ha interconnect port show
```

Active	Link	Physical	Link	Physical	Physical	
Node	Monitor	Port	Layer	Layer	Link Up	Link Down
Link			State	State		
-----	-----	----	-----	-----	-----	-----
node-a1	off		disabled	down	4	3
false		0	linkup	active	4	2
true		1	linkup	active	4	2
node-a2	off		linkup	active	4	2
true		0	linkup	active	4	2
true		1	linkup	active	4	2

2 entries were displayed.

### 3. Mettez le port d'interface IP MetroCluster en ligne.

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or 1>
```

#### Exemple de sortie

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

#### a. Vérifiez que le port de l'interface IP MetroCluster est en ligne.

```
Cluster_A1::*> system ha interconnect port show
```

#### Exemple de sortie

```

Cluster_A1::*> system ha interconnect port show
                Physical  Link
                Layer    Layer    Physical  Physical
Active
Node           Monitor  Port  State  State  Link Up  Link Down
Link
-----
node-a1        off
                0  linkup  active  5      3
true
                1  linkup  active  4      2
true
node-a2        off
                0  linkup  active  4      2
true
                1  linkup  active  4      2
true
2 entries were displayed.

```

## Mise à niveau du micrologiciel sur les commutateurs IP MetroCluster

Vous devrez peut-être mettre à niveau le micrologiciel d'un commutateur IP MetroCluster.

### Description de la tâche

Vous devez répéter cette tâche sur chacun des commutateurs successivement.

"[Activer la journalisation de la console](#)" avant d'effectuer cette tâche.

### Étapes

1. Vérifier l'état de santé de la configuration.
  - a. Vérifier que la MetroCluster est configurée et en mode normal sur chaque cluster :

```
metrocluster show
```

```

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

```

b. Vérifier que la mise en miroir est activée sur chaque nœud :

```
metrocluster node show
```

```

cluster_A::> metrocluster node show
DR                Configuration DR
Group Cluster Node      State           Mirroring Mode
-----
-----
1      cluster_A
           node_A_1      configured      enabled      normal
           cluster_B
           node_B_1      configured      enabled      normal
2 entries were displayed.

```

c. Vérifier que les composants MetroCluster sont sains :

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results. To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

a. Vérifier qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Installer le logiciel sur le premier commutateur.



Vous devez installer le logiciel du commutateur sur les commutateurs dans l'ordre suivant : switch\_A\_1, switch\_B\_1, switch\_A\_2, switch\_B\_2.

Suivez les étapes d'installation du logiciel du commutateur dans la rubrique correspondante selon que le type de commutateur est Broadcom, Cisco ou NVIDIA :

- ["Téléchargez et installez le logiciel EFOS du commutateur Broadcom"](#)
- ["Téléchargez et installez le logiciel Cisco switch NX-OS"](#)
- ["Téléchargez et installez le logiciel Cumulus du commutateur NVIDIA SN2100"](#)

3. Répéter l'étape précédente pour chacun des commutateurs.

4. Recommencez [Étape 1](#) pour vérifier l'état de santé de la configuration.

## Mettre à niveau les fichiers RCF sur les commutateurs IP MetroCluster

Il peut être nécessaire de mettre à niveau un fichier RCF sur un commutateur IP MetroCluster. Par exemple, si la version du fichier RCF exécutée sur les switches n'est pas prise en charge par la version ONTAP, la version du firmware du switch ou les deux.

### Vérifiez que le fichier RCF est pris en charge

Si vous modifiez la version de ONTAP ou la version du firmware du commutateur, vérifiez que vous disposez d'un fichier RCF pris en charge par cette version. Si vous utilisez le générateur FCR, le fichier RCF approprié sera généré pour vous.

## Étapes

1. Utiliser les commandes suivantes des commutateurs pour vérifier la version du fichier RCF :

À partir de ce commutateur...	Exécutez cette commande...
Commutateur Broadcom	(IP_switch_A_1) # show clibanner
Commutateur Cisco	IP_switch_A_1# show banner motd

Pour l'un ou l'autre commutateur, recherchez la ligne du résultat indiquant la version du fichier RCF. Par exemple, le résultat suivant provient d'un commutateur Cisco, qui indique que la version du fichier RCF est « v1.80 ».

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Pour vérifier quels fichiers sont pris en charge pour une version, un commutateur et une plate-forme ONTAP spécifiques, utilisez le générateur de fichiers RcfFileGenerator. Si vous pouvez générer le fichier RCF pour la configuration dont vous disposez ou vers laquelle vous souhaitez procéder à la mise à niveau, ce fichier est pris en charge.
3. Pour vérifier que le micrologiciel du commutateur est pris en charge, reportez-vous aux sections suivantes :
  - ["Hardware Universe"](#)
  - ["Matrice d'interopérabilité NetApp"](#)

## Mettre à niveau les fichiers RCF

Si vous installez un nouveau firmware du commutateur, vous devez installer le micrologiciel du commutateur avant de mettre à niveau le fichier RCF.

### Description de la tâche

- Cette procédure perturbe le trafic sur le commutateur où le fichier RCF est mis à niveau. Le trafic reprend lorsque le nouveau fichier RCF est appliqué.
- Effectuer les étapes sur un commutateur à la fois, dans l'ordre suivant : Switch\_A\_1, Switch\_B\_1, Switch\_A\_2, Switch\_B\_2.
- ["Activer la journalisation de la console"](#) avant d'effectuer cette tâche.

## Étapes

1. Vérification de l'état de santé de la configuration.
  - a. Vérifiez que les composants MetroCluster sont sains :

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

L'opération s'exécute en arrière-plan.

- b. Après le `metrocluster check run` opération terminée, exécutez `metrocluster check show` pour afficher les résultats.

Après environ cinq minutes, les résultats suivants s'affichent :

```
-----
::*> metrocluster check show

Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
clusters           ok
connections        not-applicable
volumes            ok
7 entries were displayed.
```

- a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id 38
```

- b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

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

Suivez les étapes pour votre fournisseur de commutateur :

- "Réinitialisez les paramètres par défaut du commutateur IP Broadcom"
- "Réinitialisez le commutateur IP Cisco sur les paramètres d'usine par défaut"
- "Réinitialisez les paramètres par défaut du commutateur NVIDIA IP SN2100"

## 3. Téléchargez et installez le fichier RCF IP, selon votre fournisseur de commutateur.

- "Téléchargez et installez les fichiers RCF IP Broadcom"
- "Téléchargez et installez les fichiers RCF IP Cisco"
- "Téléchargez et installez les fichiers RCF IP de NVIDIA"



Si vous disposez d'une configuration réseau L2 partagée ou L3, il se peut que vous deviez ajuster les ports ISL sur les commutateurs intermédiaire/client. Le mode de port de commutateur peut passer du mode « accès » au mode « réseau ». Ne procédez à la mise à niveau de la deuxième paire de commutateurs (A\_2, B\_2) que si la connectivité réseau entre les commutateurs A\_1 et B\_1 est pleinement opérationnelle et que le réseau fonctionne correctement.

## Mettre à niveau les fichiers RCF sur les commutateurs IP Cisco à l'aide de CleanUpFiles

La mise à niveau d'un fichier RCF peut être nécessaire sur un commutateur IP Cisco. Par exemple, une mise à niveau de ONTAP ou une mise à niveau du firmware du switch nécessite tous deux un nouveau fichier RCF.

### Description de la tâche

- À partir de la version 1.4a de RcfFileGenerator, il existe une nouvelle option permettant de modifier (mise à niveau, rétrogradation ou remplacement) la configuration du commutateur sur les commutateurs IP Cisco sans avoir à effectuer de « effacement d'écriture ».
- "[Activer la journalisation de la console](#)" avant d'effectuer cette tâche.
- Le switch Cisco 9336C-FX2 possède deux types de stockage de switch distincts dont le nom est différent dans le RCF. Utilisez le tableau suivant pour déterminer le type de stockage Cisco 9336C-FX2 adapté à votre configuration :

Si vous connectez le stockage suivant...	Choisissez le type de stockage Cisco 9336C-FX2...	Exemple de bannière/MOTD du fichier RCF
<ul style="list-style-type: none"><li>• Tiroirs SAS directement connectés</li><li>• Tiroirs NVMe directement connectés</li><li>• Tiroirs NVMe connectés à des switchs de stockage dédiés</li></ul>	9336C-FX2 – stockage direct uniquement	* Switch : NX9336C (direct storage, L2 Networks, direct ISL)
<ul style="list-style-type: none"><li>• Tiroirs SAS directement connectés</li><li>• Tiroirs NVMe connectés aux switchs IP MetroCluster</li></ul> <p> Au moins un tiroir NVMe connecté Ethernet est requis</p>	9336C-FX2 : stockage SAS et Ethernet	* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)

### Avant de commencer

Vous pouvez utiliser cette méthode si votre configuration répond aux exigences suivantes :

- La configuration FCR standard est appliquée.
- Le "[RcfFileGenerator](#)" doit pouvoir créer le même fichier RCF appliqué avec la même version et la même configuration (plateformes ou VLAN).
- Le fichier RCF appliqué n'a pas été fourni par NetApp pour une configuration spéciale.
- Le fichier RCF n'a pas été modifié avant son application.
- Les étapes permettant de réinitialiser les paramètres d'usine du commutateur ont été suivies avant d'appliquer le fichier RCF actuel.
- Aucune modification n'a été apportée à la configuration du switch(port) après l'application de la FCR.

Si vous ne répondez pas à ces exigences, vous ne pouvez pas utiliser les fichiers CleanUpFiles créés lors de la génération des fichiers RCF. Cependant, vous pouvez utiliser la fonction pour créer des CleanUpFiles génériques — le nettoyage à l'aide de cette méthode est dérivé de la sortie de `show running-config` et il s'agit des meilleures pratiques.



Vous devez mettre à jour les commutateurs dans l'ordre suivant : `switch_A_1`, `Switch_B_1`, `Switch_A_2`, `Switch_B_2`. Vous pouvez également mettre à jour les commutateurs `Switch_A_1` et `Switch_B_1` en même temps, puis les commutateurs `Switch_A_2` et `Switch_B_2`.

## Étapes

1. Déterminez la version actuelle du fichier RCF, ainsi que les ports et les VLAN utilisés : `IP_switch_A_1# show banner motd`



Vous devez obtenir ces informations à partir des quatre commutateurs et remplir le tableau d'information suivant.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*
#
IP_switch_A_1#
```

À partir de cette sortie, vous devez collecter les informations présentées dans les deux tableaux suivants.

Informations génériques	MetroCluster	Les données
Version du fichier RCF		1.81
Type de commutateur		NX9336
Typologie de réseau		Réseaux L2, liens ISL directs
Type de stockage		Stockage SAS
Plateformes	1	AFF A400
	2	FAS9000

Informations VLAN	Le réseau	Configuration MetroCluster	Ports de commutation	Site A	Site B
Cluster local VLAN	Réseau 1	1	1, 2	111	222
		2	3 février 4	151	251
	Réseau 2	1	1, 2	111	222
		2	3 février 4	151	251
VLAN MetroCluster	Réseau 1	1	9 février 10	119	119
		2	11 février 12	159	159
	Réseau 2	1	9 février 10	219	219
		2	11 février 12	259	259

2. ] Créez les fichiers RCF et CleanUpFiles ou créez des CleanUpFiles génériques pour la configuration actuelle.

Si votre configuration répond aux exigences décrites dans les conditions préalables, sélectionnez **option 1**. Si votre configuration ne répond pas \* aux exigences décrites dans les conditions préalables, sélectionnez **option 2**.

### Option 1 : créez les fichiers RCF et CleanUpFiles

Utiliser cette procédure si la configuration répond aux exigences.

#### Étapes

- a. Utilisez le RcfFileGenerator 1.4a (ou version ultérieure) pour créer les fichiers RCF avec les informations récupérées à l'étape 1. La nouvelle version de RcfFileGenerator crée un jeu supplémentaire de CleanUpFiles que vous pouvez utiliser pour rétablir une certaine configuration et préparer le commutateur pour appliquer une nouvelle configuration RCF.
- b. Comparez la bannière motd avec les fichiers FCR actuellement appliqués. Les types de plate-forme, le type de commutateur, le port et le VLAN doivent être identiques.



Vous devez utiliser les CleanUpFiles de la même version que le fichier RCF et pour la même configuration. L'utilisation d'un CleanUpFile ne fonctionnera pas et peut nécessiter une réinitialisation complète du commutateur.



La version ONTAP pour laquelle le fichier RCF est créé n'est pas pertinente. Seule la version du fichier RCF est importante.



Le fichier RCF (même si sa version est identique) peut lister un nombre inférieur ou supérieur à celui-ci. Assurez-vous que votre plate-forme est répertoriée.

### Option 2 : création de fichiers génériques CleanUpFiles

Utilisez cette procédure si la configuration ne répond pas \* à toutes les exigences.

#### Étapes

- a. Récupérer la sortie de `show running-config` de chaque commutateur.
- b. Ouvrez l'outil RcfFileGenerator et cliquez sur 'Create generic CleanUpFiles' en bas de la fenêtre
- c. Copiez le résultat que vous avez récupéré à l'étape 1 à partir du commutateur 'un' dans la fenêtre supérieure. Vous pouvez supprimer ou conserver la sortie par défaut.
- d. Cliquez sur 'Créer des fichiers CUF'.
- e. Copiez la sortie de la fenêtre inférieure dans un fichier texte (ce fichier est le CleanUpFile).
- f. Répétez les étapes c, d et e pour tous les commutateurs de la configuration.

À la fin de cette procédure, vous devez avoir quatre fichiers texte, un pour chaque commutateur. Vous pouvez utiliser ces fichiers de la même manière que les fichiers CleanUpFiles que vous pouvez créer à l'aide de l'option 1.

3. Créez les fichiers RCF « nouveaux » pour la nouvelle configuration. Créez ces fichiers de la même manière que vous avez créé les fichiers à l'étape précédente, à l'exception de choisir la version respective des fichiers ONTAP et RCF.

Une fois cette étape terminée, vous devez avoir deux jeux de fichiers RCF, chacun composé de douze fichiers.

4. Téléchargez les fichiers sur le bootflash.

- a. Téléchargez les CleanUpFiles que vous avez créés dans [Créez les fichiers RCF et les fichiers CleanUpFiles](#) ou [créez des fichiers CleanUpFiles génériques pour la configuration actuelle](#)



Ce fichier CleanUpFile est destiné au fichier FCR en cours qui est appliqué et **NON** pour la nouvelle FCR vers laquelle vous souhaitez effectuer la mise à niveau.

Exemple de fichier CleanUpFile pour Switch-A1 : Cleanup\_NX9336\_v1.81\_Switch-A1.txt

- b. Téléchargez les « nouveaux » fichiers RCF que vous avez créés dans [Créez les fichiers RCF « nouveaux » pour la nouvelle configuration](#).

Exemple de fichier RCF pour Switch-A1 : NX9336\_v1.90\_Switch-A1.txt

- c. Téléchargez les CleanUpFiles que vous avez créés dans [Créez les fichiers RCF « nouveaux » pour la nouvelle configuration](#). Cette étape est facultative — vous pouvez utiliser le fichier ultérieurement pour mettre à jour la configuration du commutateur. Elle correspond à la configuration actuellement appliquée.

Exemple de fichier CleanUpFile pour Switch-A1 : Cleanup\_NX9336\_v1.90\_Switch-A1.txt



Vous devez utiliser CleanUpFile pour la version FCR correcte (correspondante). Si vous utilisez un CleanUpFile pour une version FCR différente, ou une configuration différente, le nettoyage de la configuration risque de ne pas fonctionner correctement.

L'exemple suivant copie les trois fichiers dans le bootflash :

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_XXX_XXX_XXX_XXX/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+



Vous êtes invité à spécifier le routage et le transfert virtuels (VRF).

5. Appliquez le CleanUpFile ou le CleanUpFile générique.

Une partie de la configuration est rétablie et les ports de commutation sont « hors ligne ».

- a. Vérifiez qu'aucune modification n'est en attente de la configuration de démarrage : `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Si vous voyez la sortie du système, enregistrez la configuration en cours d'exécution dans la configuration de démarrage : `copy running-config startup-config`



Le résultat du système indique que la configuration de démarrage et la configuration en cours d'exécution sont différentes et en attente de modifications. Si vous n'enregistrez pas les modifications en attente, vous ne pouvez pas revenir en arrière à l'aide d'un rechargement du commutateur.

- a. Appliquer le fichier CleanUpFile :

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```



Le script peut prendre un certain temps pour revenir à l'invite du commutateur. Aucune sortie n'est attendue.

7. Afficher la configuration en cours d'exécution pour vérifier que la configuration est effacée : `show running-config`

La configuration actuelle doit indiquer :

- Aucun mappage de classe et aucune liste d'accès IP n'est configuré
- Aucun mappage de stratégie n'est configuré
- Aucune stratégie de services n'est configurée
- Aucun profil de port n'est configuré
- Toutes les interfaces Ethernet (à l'exception de mgmt0 qui ne doivent pas afficher de configuration, et seul le VLAN 1 doit être configuré).

Si l'un des éléments ci-dessus est configuré, il est possible que vous ne puissiez pas appliquer une nouvelle configuration de fichier RCF. Cependant, vous pouvez revenir à la configuration précédente en rechargeant le commutateur **sans** enregistrer la configuration en cours d'exécution dans la configuration de démarrage. Le commutateur s'active avec la configuration précédente.

8. Appliquer le fichier RCF et vérifier que les ports sont en ligne.

- a. Appliquez les fichiers RCF.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```



Certains messages d'avertissement s'affichent lors de l'application de la configuration. Les messages d'erreur ne sont généralement pas attendus. Toutefois, si vous êtes connecté à l'aide de SSH, vous pouvez recevoir l'erreur suivante : `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

- b. Une fois la configuration appliquée, vérifiez que le cluster et les ports MetroCluster sont mis en ligne à l'aide de l'une des commandes suivantes, `show interface brief`, `show cdp neighbors`, ou `show lldp neighbors`



Si vous avez modifié le VLAN pour le cluster local et que vous avez mis à niveau le premier commutateur du site, la surveillance de l'état du cluster risque de ne pas indiquer qu'il est « sain », car les VLAN de l'ancienne et des nouvelles configurations ne correspondent pas. Après la mise à jour du second commutateur, l'état doit revenir à l'état sain.

Si la configuration n'est pas correctement appliquée ou si vous ne souhaitez pas conserver la configuration, vous pouvez revenir à la configuration précédente en rechargeant le commutateur **sans** enregistrer la configuration en cours dans la configuration de démarrage. Le commutateur s'active avec la configuration précédente.

9. Enregistrer la configuration et recharger le commutateur.

```
IP_switch_A_1# copy running-config startup-config  
  
IP_switch_A_1# reload
```

## Modification du nom d'un commutateur IP Cisco

Vous devrez peut-être renommer un commutateur IP Cisco pour fournir une dénomination cohérente dans toute votre configuration.

### Description de la tâche

- Dans les exemples de cette tâche, le nom du commutateur est modifié de `myswitch` à `IP_switch_A_1`.
- "[Activer la journalisation de la console](#)" avant d'effectuer cette tâche.

### Étapes

1. Passer en mode de configuration globale :

#### **configure terminal**

L'exemple suivant montre l'invite du mode de configuration. Les deux invites indiquent le nom du commutateur de `myswitch`.

```
myswitch# configure terminal  
myswitch(config)#
```

2. Renommez le commutateur :

```
switchname new-switch-name
```

Si vous renommez les deux commutateurs dans la structure, utilisez la même commande sur chaque switch.

L'invite de l'interface de ligne de commandes prend en compte le nouveau nom :

```
myswitch(config)# switchname IP_switch_A_1  
IP_switch_A_1(config)#
```

3. Quitter le mode de configuration :

```
exit
```

L'invite du commutateur de niveau supérieur s'affiche :

```
IP_switch_A_1(config)# exit  
IP_switch_A_1#
```

4. Copier la configuration en cours d'exécution dans le fichier de configuration de démarrage :

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

5. Vérifiez que la modification du nom du commutateur est visible depuis l'invite du cluster ONTAP.

Notez que le nouveau nom du commutateur est affiché et que l'ancien nom du commutateur (*myswitch*) n'apparaît pas.

a. Passez en mode privilège avancé, puis appuyez sur **y** lorsque vous y êtes invité :

```
set -privilege advanced
```

b. Afficher les périphériques connectés :

```
network device-discovery show
```

c. Revenir en mode de privilège admin:

```
set -privilege admin
```

L'exemple suivant montre que le commutateur apparaît avec le nouveau nom, *IP\_switch\_A\_1*:

```
cluster_A::storage show> set advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster_A::storage show*> network device-discovery show
```

Node/ Protocol	Local Port	Discovered Device	Interface	Platform
-----				
node_A_2/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/28	N9K-
C9372PX				
	e1a	IP_switch_A_1 (FOC21211RBU)	Ethernet1/2	N3K-
C3232C				
	e1b	IP_switch_A_1 (FOC21211RBU)	Ethernet1/10	N3K-
C3232C				
.				
.			Ethernet1/18	N9K-
C9372PX				
node_A_1/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/26	N9K-
C9372PX				
	e0a	IP_switch_A_2 (FOC21211RB5)	Ethernet1/1	N3K-
C3232C				
	e0b	IP_switch_A_2 (FOC21211RB5)	Ethernet1/9	N3K-
C3232C				
	e1a	IP_switch_A_1 (FOC21211RBU)		
.				
.				
.				

16 entries were displayed.

## Ajoutez, supprimez ou modifiez des ports ISL sans interrompre l'activité sur les commutateurs IP Cisco

Vous devrez peut-être ajouter, supprimer ou modifier des ports ISL sur des commutateurs IP Cisco. Vous pouvez convertir des ports ISL dédiés en ports ISL partagés ou modifier la vitesse des ports ISL sur un commutateur IP Cisco.

### Description de la tâche

Si vous convertissez des ports ISL dédiés en ports ISL partagés, assurez-vous que les nouveaux ports respectent le ["Exigences relatives aux ports ISL partagés"](#).

Vous devez effectuer toutes les étapes des deux commutateurs pour assurer la connectivité ISL.

La procédure suivante suppose que vous remplacez un ISL de 10 Go connecté au port du commutateur eth1/24/1 par deux liens ISL de 100 Go connectés aux ports de commutation 17 et 18.



Si vous utilisez un commutateur Cisco 9336C-FX2 dans une configuration partagée qui connecte des tiroirs NS224, la modification des liens ISL peut nécessiter un nouveau fichier RCF. Vous n'avez pas besoin d'un nouveau fichier RCF si la vitesse ISL actuelle et la nouvelle vitesse sont de 40 Gbit/s et de 100 Gbit/s. Toute autre modification de la vitesse ISL requiert un nouveau fichier RCF. Par exemple, changer la vitesse des liens ISL de 40 Gbits/s à 100 Gbits/s ne nécessite pas de nouveau fichier RCF. En revanche, pour passer de 10 Gbits/s à 40 Gbits/s, la vitesse des liens ISL nécessite la création d'un nouveau fichier RCF.

### Avant de commencer

Reportez-vous à la section **commutateurs** du ["NetApp Hardware Universe"](#) pour vérifier les émetteurs-récepteurs pris en charge.

["Activer la journalisation de la console"](#) avant d'effectuer cette tâche.

### Étapes

1. Désactivez les ports ISL des deux commutateurs dans la structure que vous souhaitez modifier.



Vous n'avez besoin de désactiver les ports ISL actuels que si vous les déplacez vers un autre port, ou si la vitesse de l'ISL change. Si vous ajoutez un port ISL avec la même vitesse que les liens ISL existants, passez à l'étape 3.

Vous ne devez entrer qu'une seule commande de configuration pour chaque ligne et appuyer sur Ctrl-Z après avoir saisi toutes les commandes, comme illustré dans l'exemple suivant :

```

switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#

```

2. Retirez les câbles et émetteurs-récepteurs existants.
3. Modifiez le port ISL si nécessaire.



Si vous utilisez des switchs Cisco 9336C-FX2 dans une configuration partagée qui connecte des tiroirs NS224, et que vous devez mettre à niveau le fichier RCF et appliquer la nouvelle configuration pour les nouveaux ports ISL, suivez les étapes à ["Mettez à niveau les fichiers RCF sur les switchs IP MetroCluster."](#)

Option	Étape
Pour modifier la vitesse d'un port ISL...	Reliez les nouveaux liens ISL aux ports désignés, selon leur vitesse. Vous devez vous assurer que ces ports ISL pour votre commutateur sont répertoriés dans la section <i>MetroCluster IP installation and Configuration</i> .
Pour ajouter un ISL...	Insérez les QFSP dans les ports que vous ajoutez en tant que ports ISL. Assurez-vous qu'ils sont répertoriés dans la section <i>MetroCluster IP installation and Configuration</i> et reliez-les en conséquence.

4. Activez tous les ports ISL (si non activés) sur les deux commutateurs dans la structure, en commençant par la commande suivante :

```
switch_A_1# conf t
```

Vous ne devez entrer qu'une seule commande de configuration par ligne et appuyer sur Ctrl-Z après avoir saisi toutes les commandes :

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Vérifiez que les liens ISL et les canaux de port pour les liens ISL sont établis entre les deux commutateurs :

```
switch_A_1# show int brief
```

Vous devez voir les interfaces ISL dans la sortie de la commande, comme dans l'exemple suivant :

```

Switch_A_1# show interface brief
-----
-----
Ethernet          VLAN    Type Mode   Status Reason          Speed
Port
Interface
Ch #
-----
-----
Eth1/17           1       eth  access down  XCVR not inserted
auto(D) --
Eth1/18           1       eth  access down  XCVR not inserted
auto(D) --
-----
-----
Port-channel      VLAN    Type Mode   Status Reason
Speed  Protocol
Interface
-----
-----
Po10              1       eth  trunk  up     none
a-100G(D) lacp
Po11              1       eth  trunk  up     none
a-100G(D) lacp

```

6. Répéter la procédure pour le tissu 2.

## Identification du stockage dans une configuration MetroCluster IP

Si vous devez remplacer un disque ou un module de tiroir, vous devez d'abord identifier l'emplacement.

### Identification des tablettes locales et distantes

Lorsque vous affichez les informations relatives aux tiroirs à partir d'un site MetroCluster, tous les disques distants sont sur 0m, la carte hôte iSCSI virtuelle. Cela signifie que les disques sont accessibles via les interfaces IP de MetroCluster. Tous les autres lecteurs sont locaux.

Après avoir identifié si un tiroir est distant (sur 0 m), vous pouvez davantage identifier le disque ou le tiroir par le numéro de série ou, en fonction des attributions d'ID de tiroir dans votre configuration, par ID de tiroir.



Dans les configurations IP MetroCluster exécutant ONTAP 9.4, l'ID de tiroir n'est pas requis d'être unique entre les sites MetroCluster. Cela inclut les tiroirs internes (0) et externes. Le numéro de série est cohérent lorsqu'il est affiché depuis un nœud sur un site MetroCluster.

Ils doivent être uniques dans le groupe de reprise après incident, à l'exception du tiroir interne.

Un fois le module de disque ou de tiroir identifié, vous pouvez remplacer le composant en suivant la procédure adéquate.

## "Maintenance des tiroirs disques DS460C DS224C et DS212C"

### Exemple de sortie sysconfig -a

L'exemple suivant utilise le `sysconfig -a` Commande permettant d'afficher les périphériques d'un nœud dans la configuration IP de MetroCluster. Ce nœud est associé aux tiroirs et périphériques suivants :

- Logement 0 : disques internes (disques locaux)
- Slot 3 : ID de tiroir externe 75 et 76 (disques locaux)
- Logement 0 : adaptateur hôte iSCSI virtuel 0m (lecteurs distants)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
          0      : NETAPP  X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
          1      : NETAPP  X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
          2      : NETAPP  X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:  Microsemi Corp. 110-03801 rev. A0
Part number:      111-03801+A0
Serial number:    7A1063AF14B
Date Code:        20170320
Firmware rev:     03.08.09.00
Base WWN:         5:0000d1:702e69e:80
Phy State:        [12] Enabled, 12.0 Gb/s
                  [13] Enabled, 12.0 Gb/s
                  [14] Enabled, 12.0 Gb/s
                  [15] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor:      Molex Inc.
Mini-SAS HD Part Number: 112-00436+A0
```

```
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
      75.0 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
      75.1 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
      75.2 : NETAPP      X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
      75.3 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
      75.4 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
```

.  
.
.  
.

```
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
```

```
slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
```

```
MFG Part Number:      Microsemi Corp. 110-03801 rev. A0
```

```
Part number:          111-03801+A0
```

```
Serial number:        7A1063AF14B
```

```
Date Code:            20170320
```

```
Firmware rev:         03.08.09.00
```

```
Base WWN:              5:0000d1:702e69e:88
```

```
Phy State:            [0] Enabled, 12.0 Gb/s
                      [1] Enabled, 12.0 Gb/s
                      [2] Enabled, 12.0 Gb/s
                      [3] Enabled, 12.0 Gb/s
```

```
Mini-SAS HD Vendor:   Molex Inc.
```

```
Mini-SAS HD Part Number: 112-00436+A0
```

```
Mini-SAS HD Type:     Passive Copper (unequalized) 0.5m ID:00
```

```
Mini-SAS HD Serial Number: 614130691
```

```
      75.0 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
      75.1 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
      75.2 : NETAPP      X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
      75.3 : NETAPP      X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
```

.  
.
.  
.

```
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
```

Shelf 76: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)

MFG Part Number: Microsemi Corp. 110-03801 rev. A0

Part number: 111-03801+A0

Serial number: 7A1063AF14B

Date Code: 20170320

Firmware rev: 03.08.09.00

Base WWN: 5:0000d1:702e69e:8c

Phy State: [4] Enabled, 12.0 Gb/s

[5] Enabled, 12.0 Gb/s

[6] Enabled, 12.0 Gb/s

[7] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor: Molex Inc.

Mini-SAS HD Part Number: 112-00436+A0

Mini-SAS HD Type: Passive Copper (unequalized) 0.5m ID:01

Mini-SAS HD Serial Number: 614130690

75.0 : NETAPP X438\_S1633400AMD NA04 381.3GB 520B/sect  
(S20KNYAG501805)

75.1 : NETAPP X438\_S1633400AMD NA04 381.3GB 520B/sect  
(S20KNYAG502050)

75.2 : NETAPP X438\_PHM2400MCTO NA04 381.3GB 520B/sect  
(25M0A03WT2KA)

.  
. .

Shelf 75: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

Shelf 76: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+

.  
. .

slot 0: Virtual iSCSI Host Adapter 0m

0.0 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500690)

0.1 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500571)

0.2 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500323)

0.3 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500724)

0.4 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500734)

0.5 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect  
(S3NBNX0J500598)

```
0.12 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
0.13 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E Firmware rev. PSM3E A: 0103 PSM3E B: 0103
Shelf 35: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220
Shelf 36: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

node_A_1::>
```

## Ajout de tiroirs à un IP MetroCluster à l'aide des commutateurs MetroCluster de stockage partagé

Vous devrez peut-être ajouter des tiroirs NS224 à un MetroCluster à l'aide de commutateurs MetroCluster de stockage partagé.

À partir de ONTAP 9.10.1, vous pouvez ajouter des tiroirs NS224 à partir d'un MetroCluster à l'aide des commutateurs MetroCluster/stockage partagé. Vous pouvez ajouter plusieurs tiroirs à la fois.

### Avant de commencer

- Les nœuds doivent exécuter ONTAP 9.9.1 ou version ultérieure.
- Tous les tiroirs NS224 actuellement connectés doivent être connectés aux mêmes commutateurs que MetroCluster (configuration du stockage partagé / commutateur MetroCluster).
- Cette procédure ne peut pas être utilisée pour convertir une configuration avec des tiroirs NS224 directement connectés ou des tiroirs NS224 reliés à des commutateurs Ethernet dédiés à une configuration à l'aide de commutateurs MetroCluster/stockage partagé.
- ["Activer la journalisation de la console"](#) avant d'effectuer cette tâche.

### Envoi d'un message AutoSupport personnalisé avant la maintenance

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

#### Description de la tâche

Cette tâche doit être effectuée sur chaque site MetroCluster.

#### Étapes

1. Pour éviter la génération automatique de dossiers de demande de support, envoyez un message AutoSupport pour indiquer que la mise à niveau est en cours.
  - a. Exécutez la commande suivante :

```
system node autosupport invoke -node * -type all -message "Maint=10h Adding
or Removing NS224 shelves" _
```

Cet exemple spécifie une fenêtre de maintenance de 10 heures. Selon votre plan, il est possible que vous souhaitiez accorder plus de temps.

Si la maintenance est terminée avant le temps écoulé, vous pouvez appeler un message AutoSupport indiquant la fin de la période de maintenance :

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

- a. Répétez la commande sur le cluster partenaire.

## Vérification de l'état de santé de la configuration MetroCluster

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

### Étapes

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

- a. Vérifier si le système est multipathed :

```
node run -node node-name sysconfig -a
```

- b. Vérifier si des alertes d'intégrité sont disponibles sur les deux clusters :

```
system health alert show
```

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

```
metrocluster show
```

- d. Effectuer une vérification MetroCluster :

```
metrocluster check run
```

- e. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

- f. Exécutez Config Advisor.

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

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

2. Vérifiez que le cluster fonctionne correctement :

```
cluster show -vserver Cluster
```

```

cluster_A::> cluster show -vserver Cluster
Node           Health Eligibility  Epsilon
-----
node_A_1      true   true         false
node_A_2      true   true         false

cluster_A::>

```

### 3. Vérifier que tous les ports du cluster sont bien :

```
network port show -ipSPACE cluster
```

```

cluster_A::> network port show -ipSPACE cluster

Node: node_A_1-old

Port           IPspace      Broadcast Domain Link MTU      Speed(Mbps) Health
-----
e0a            Cluster      Cluster      up   9000    auto/10000 healthy
e0b            Cluster      Cluster      up   9000    auto/10000 healthy

Node: node_A_2-old

Port           IPspace      Broadcast Domain Link MTU      Speed(Mbps) Health
-----
e0a            Cluster      Cluster      up   9000    auto/10000 healthy
e0b            Cluster      Cluster      up   9000    auto/10000 healthy

4 entries were displayed.

cluster_A::>

```

### 4. Vérifier que toutes les LIFs de cluster sont opérationnelles :

```
network interface show -vserver Cluster
```

Chaque LIF de cluster doit afficher « true » pour is Home et avoir un Status Admin/Oper of up/up »

```
cluster_A::> network interface show -vserver cluster
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
-----	-----				
Cluster					
	node_A_1-old_clus1	up/up	169.254.209.69/16	node_A_1	e0a
true					
	node_A_1-old_clus2	up/up	169.254.49.125/16	node_A_1	e0b
true					
	node_A_2-old_clus1	up/up	169.254.47.194/16	node_A_2	e0a
true					
	node_A_2-old_clus2	up/up	169.254.19.183/16	node_A_2	e0b
true					

```
4 entries were displayed.
```

```
cluster_A::>
```

5. Vérifiez que la fonction de restauration automatique est activée sur l'ensemble des LIFs du cluster :

```
network interface show -vserver Cluster -fields auto-revert
```

```

cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver  Interface      Auto-revert
-----  -
Cluster
          node_A_1-old_clus1
                        true
          node_A_1-old_clus2
                        true
          node_A_2-old_clus1
                        true
          node_A_2-old_clus2
                        true

          4 entries were displayed.

cluster_A::>

```

## Application du nouveau fichier RCF aux commutateurs



Si votre commutateur est déjà configuré correctement, vous pouvez passer directement à ces sections suivantes [Configuration du cryptage MACsec sur les commutateurs Cisco 9336C](#), si applicable ou à [Connexion de la nouvelle étagère NS224](#).

- Vous devez modifier la configuration de commutateurs pour ajouter des tiroirs.
- Consultez les détails de câblage à l'adresse "[Affectations des ports de plate-forme](#)".
- Vous devez utiliser l'outil **RcfFileGenerator** pour créer le fichier RCF correspondant à votre configuration. Le "**RcfFileGenerator**" fournit également un aperçu du câblage par port pour chaque commutateur. Assurez-vous de choisir le nombre correct d'étagères. Des fichiers supplémentaires sont créés avec le fichier RCF, afin de fournir une disposition de câblage détaillée correspondant à vos options spécifiques. Utilisez cette présentation pour vérifier le câblage des nouveaux tiroirs.

### Mise à niveau des fichiers RCF sur des commutateurs IP MetroCluster

Si vous installez un nouveau firmware du commutateur, vous devez installer le micrologiciel du commutateur avant de mettre à niveau le fichier RCF.

Cette procédure perturbe le trafic sur le commutateur où le fichier RCF est mis à niveau. Le trafic reprend lorsque le nouveau fichier RCF est appliqué.

#### Étapes

1. Vérification de l'état de santé de la configuration.
  - a. Vérifiez que les composants MetroCluster sont sains :

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

L'opération s'exécute en arrière-plan.

- b. Après le `metrocluster check run` opération terminée, exécution `metrocluster check show` pour afficher les résultats.

Après environ cinq minutes, les résultats suivants s'affichent :

```
-----  
::*> metrocluster check show  
  
Component                Result  
-----  
nodes                    ok  
lifs                     ok  
config-replication      ok  
aggregates              ok  
clusters                ok  
connections             not-applicable  
volumes                 ok  
7 entries were displayed.
```

- a. Pour vérifier le statut de l'opération MetroCluster check en cours d'exécution, utiliser la commande :  
**metrocluster operation history show -job-id 38**
- b. Vérifiez qu'il n'y a pas d'alerte d'intégrité :  
**system health alert show**

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

### Réinitialisation des paramètres d'usine du commutateur IP Cisco

Avant d'installer une nouvelle version du logiciel et des RCFs, vous devez effacer la configuration du commutateur Cisco et effectuer la configuration de base.

Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.

1. Rétablir les paramètres d'usine du commutateur :
  - a. Effacez la configuration existante : `write erase`
  - b. Recharger le logiciel du commutateur : `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)[n]`, vous devez répondre `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.



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.

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"

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

#### "Téléchargement de logiciels Cisco"

2. Copier le logiciel du commutateur sur le commutateur : `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

Dans cet exemple, le fichier `nxos.7.0.3.I4.6.bin` est copié 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)...
```

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

## Configuration du cryptage MACsec sur les commutateurs Cisco 9336C

Si vous le souhaitez, vous pouvez 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.



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

## 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"](#)

## Activation des liens ISL de Cisco MACsec dans des 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.

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
```

## Désactivation du cryptage Cisco MACsec

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.



Si vous désactivez le cryptage, vous devez également supprimer vos clés.

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 `no` 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, la règle et le trousseau de secours configurés sur l'interface pour supprimer la configuration MACsec :`no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

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
```

### Configuration d'une chaîne de clés MACsec et de clés

Pour plus de détails sur la configuration d'une chaîne de clés MACsec, reportez-vous à la documentation Cisco de votre commutateur.

## Connexion de la nouvelle étagère NS224

### Étapes

1. Installez le kit de montage sur rail fourni avec votre shelf en utilisant la Flyer d'installation fourni avec le kit.
2. Installez et fixez le shelf sur les supports et le rack ou armoire en utilisant la brochure d'installation.
3. Branchez les cordons d'alimentation au tiroir, fixez-les à l'aide de la pièce de retenue du cordon d'alimentation, puis branchez les câbles d'alimentation à différentes sources d'alimentation pour assurer la résilience.

Une étagère se met sous tension lorsqu'elle est connectée à une source d'alimentation ; elle n'a pas de commutateurs d'alimentation. Lorsqu'elle fonctionne correctement, la LED bicolore d'un bloc d'alimentation s'allume en vert.

4. Définissez l'ID du tiroir sur un nombre unique dans la paire HA et dans la configuration.
5. Connecter les ports shelf dans l'ordre suivant :
  - a. Connecter le NSM-A, e0a au commutateur (Switch-A1 ou Switch-B1)
  - b. Connecter le NSM-B, e0a au commutateur (commutateur-A2 ou commutateur-B2)
  - c. Connectez le NSM-A, e0b au commutateur (Switch-A1 ou Switch-B1)
  - d. Connectez le NSM-B, e0b au commutateur (commutateur A2 ou commutateur B2)

6. Utilisez la disposition des câbles générée à partir de l'outil **RcfFileGenerator** pour raccorder le shelf aux ports appropriés.

Une fois le nouveau tiroir correctement câblé, ONTAP le détecte automatiquement sur le réseau.

## Configurer le chiffrement de bout en bout dans une configuration MetroCluster IP

À partir de ONTAP 9.15.1, vous pouvez configurer le chiffrement de bout en bout afin de chiffrer le trafic back-end, tel que NVlog et les données de réplication du stockage, entre les sites d'une configuration IP MetroCluster.

### Description de la tâche

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Avant de pouvoir configurer le chiffrement de bout en bout, vous devez "[Configurer la gestion externe des clés](#)".
- Vérifiez les systèmes pris en charge et la version minimale de ONTAP requise pour configurer le chiffrement de bout en bout dans une configuration MetroCluster IP :

Version minimale de ONTAP	Systèmes pris en charge
ONTAP 9.15.1	<ul style="list-style-type: none"><li>• AFF A400</li><li>• FAS8300</li><li>• FAS8700</li></ul>

### Chiffrez vos données de bout en bout

Procédez comme suit pour activer le chiffrement de bout en bout.

#### Étapes

1. Vérifier l'état de santé de la configuration MetroCluster.
  - a. Vérifiez que les composants MetroCluster sont sains :

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

L'opération s'exécute en arrière-plan.

- b. Après le `metrocluster check run` l'opération se termine, exécutez :

```
metrocluster check show
```

Après environ cinq minutes, les résultats suivants s'affichent :

```
cluster_A:::*> metrocluster check show
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	not-applicable
volumes	ok

7 entries were displayed.

a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id <id>
```

b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Vérifier que la gestion externe des clés est configurée sur les deux clusters :

```
security key-manager external show-status
```

3. Chiffrement de bout en bout pour chaque groupe de reprise d'activité :

```
metrocluster modify -is-encryption-enabled true -dr-group-id  
<dr_group_id>
```

### Exemple

```

cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
        replication data sent between MetroCluster nodes and have an
impact on
        performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.

```

Répétez cette étape pour chaque groupe DR de la configuration.

#### 4. Vérifiez que le chiffrement de bout en bout est activé :

```
metrocluster node show -fields is-encryption-enabled
```

#### Exemple

```

cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster      node      configuration-state is-encryption-
enabled
-----
1           cluster_A    node_A_1  configured         true
1           cluster_A    node_A_2  configured         true
1           cluster_B    node_B_1  configured         true
1           cluster_B    node_B_2  configured         true
4 entries were displayed.

```

## Désactivez le chiffrement de bout en bout

Procédez comme suit pour désactiver le chiffrement de bout en bout.

### Étapes

1. Vérifier l'état de santé de la configuration MetroCluster.
  - a. Vérifiez que les composants MetroCluster sont sains :

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

L'opération s'exécute en arrière-plan.

b. Après le `metrocluster check run` l'opération se termine, exécutez :

```
metrocluster check show
```

Après environ cinq minutes, les résultats suivants s'affichent :

```
cluster_A:::*> metrocluster check show

Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
clusters           ok
connections        not-applicable
volumes            ok
7 entries were displayed.
```

a. Vérifier l'état de l'opération de vérification MetroCluster en cours :

```
metrocluster operation history show -job-id <id>
```

b. Vérifiez qu'il n'y a pas d'alerte de santé :

```
system health alert show
```

2. Vérifier que la gestion externe des clés est configurée sur les deux clusters :

```
security key-manager external show-status
```

3. Désactivez le chiffrement de bout en bout sur chaque groupe de reprise après incident :

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

### Exemple

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Répétez cette étape pour chaque groupe DR de la configuration.

4. Vérifiez que le chiffrement de bout en bout est désactivé :

```
metrocluster node show -fields is-encryption-enabled
```

### Exemple

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled
```

dr-group-id	cluster	node	configuration-state	is-encryption-enabled
1	cluster_A	node_A_1	configured	false
1	cluster_A	node_A_2	configured	false
1	cluster_B	node_B_1	configured	false
1	cluster_B	node_B_2	configured	false

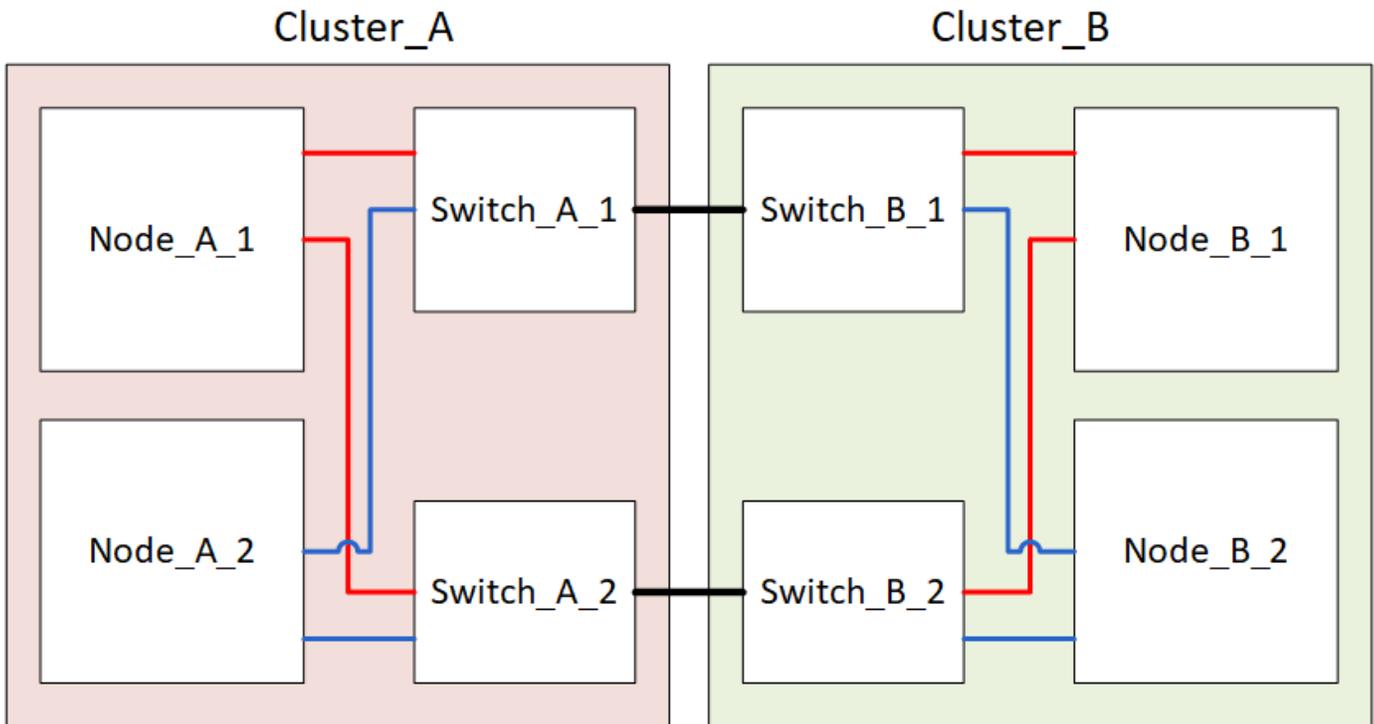
4 entries were displayed.

## Mettez le système hors tension et sous tension sur un seul site dans une configuration MetroCluster IP

Si vous avez besoin d'effectuer des opérations de maintenance sur site ou de déplacer un site unique dans une configuration MetroCluster IP, vous devez savoir comment mettre le site hors tension et sous tension.

Si vous devez déplacer et reconfigurer un site (par exemple, si vous devez passer d'un cluster à quatre nœuds à un cluster à huit nœuds), vous ne pouvez pas effectuer ces tâches en même temps. Cette procédure couvre uniquement les étapes nécessaires à la maintenance du site ou au transfert d'un site sans modifier sa configuration.

Le schéma suivant présente une configuration MetroCluster. Cluster\_B est hors tension pour des raisons de maintenance.



## Mettez un site MetroCluster hors tension

Vous devez mettre hors tension un site et tous les équipements avant le début de la maintenance ou du transfert du site.

### Description de la tâche

Toutes les commandes des étapes suivantes sont émises à partir du site qui reste sous tension.

### Étapes

1. Avant de commencer, vérifiez que tous les agrégats non mis en miroir sur le site sont hors ligne.
2. Vérifier le fonctionnement de la configuration MetroCluster dans ONTAP :
  - a. Vérifier si le système est multipathed :

```
node run -node node-name sysconfig -a
```

- b. Vérifier si des alertes d'intégrité sont disponibles sur les deux clusters :

```
system health alert show
```

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

```
metrocluster show
```

- d. Effectuer une vérification MetroCluster :

```
metrocluster check run
```

- e. Afficher les résultats de la vérification MetroCluster :

```
metrocluster check show
```

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

```
storage switch show
```

g. Exécutez Config Advisor.

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

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

3. Depuis le site que vous souhaitez rester à la hauteur, implémentez le basculement :

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

L'opération peut prendre plusieurs minutes.

4. Surveiller et vérifier la fin du basculement :

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
Operation: Switchover
Start time: 10/4/2012 19:04:13
State: in-progress
End time: -
Errors:

cluster_A::*> metrocluster operation show
Operation: Switchover
Start time: 10/4/2012 19:04:13
State: successful
End time: 10/4/2012 19:04:22
Errors: -
```

5. Si vous disposez d'une configuration IP MetroCluster exécutant ONTAP 9.6 ou une version ultérieure, attendez que les plexes du site d'incident soient en ligne et que les opérations de réparation s'effectuent automatiquement.

Dans les configurations MetroCluster IP exécutant ONTAP 9.5 ou une version antérieure, les nœuds du site d'incident ne démarrent pas automatiquement vers ONTAP et les plexes restent hors ligne.

6. Mettez hors ligne tout volume et toute LUN appartenant à des agrégats non mis en miroir.

a. Déplacez les volumes hors ligne.

```
cluster_A::* volume offline <volume name>
```

b. Mettez les LUN hors ligne.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Déplacez les agrégats non mis en miroir hors ligne : `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. Selon la configuration et la version de ONTAP, identifiez et déplacez les plexes affectés hors ligne situés sur le site de reprise sur incident (Cluster\_B).

Vous devez déplacer les plexes suivants hors ligne :

- Les plexes non mis en miroir se trouvent sur les disques situés sur le site de reprise après incident.  
Si vous ne déplacez pas les plexes non mis en miroir hors ligne sur le site d'incident, celui-ci risque d'être interrompu par la suite.
- Les plexes en miroir situés sur les disques situés sur le site de reprise après incident pour la mise en miroir des agrégats. Une fois déplacés hors ligne, les plexes sont inaccessibles.

a. Identifier les plexes affectés.

Les plexes qui appartiennent aux nœuds du site survivant se composent de disques Pool1. Les plexes qui appartiennent aux nœuds sur le site de secours se composent de disques de pool0.

```

Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate      plex  status          is-online pool
-----
Node_B_1_aggr0 plex0 normal,active true      0
Node_B_1_aggr0 plex1 normal,active true      1

Node_B_2_aggr0 plex0 normal,active true      0
Node_B_2_aggr0 plex5 normal,active true      1

Node_B_1_aggr1 plex0 normal,active true      0
Node_B_1_aggr1 plex3 normal,active true      1

Node_B_2_aggr1 plex0 normal,active true      0
Node_B_2_aggr1 plex1 normal,active true      1

Node_A_1_aggr0 plex0 normal,active true      0
Node_A_1_aggr0 plex4 normal,active true      1

Node_A_1_aggr1 plex0 normal,active true      0
Node_A_1_aggr1 plex1 normal,active true      1

Node_A_2_aggr0 plex0 normal,active true      0
Node_A_2_aggr0 plex4 normal,active true      1

Node_A_2_aggr1 plex0 normal,active true      0
Node_A_2_aggr1 plex1 normal,active true      1
14 entries were displayed.

Cluster_A::>

```

Les plexes affectés sont ceux qui sont distants vers le cluster A. Le tableau suivant indique si les disques sont locaux ou distants par rapport au cluster A :

Noeud	Disques au pool	Les disques doivent-ils être mis hors ligne ?	Exemple de plexes à déplacer hors ligne
Noeud_A_1 et noeud_A_2	Disques dans le pool 0	Non Les disques sont locaux au cluster A.	-
Disques dans le pool 1	Oui. Les disques sont distants du cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Noeud_B_1 et noeud_B_2

Disques dans le pool 0	Oui. Les disques sont distants du cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Disques dans le pool 1
------------------------	--	--	------------------------

b. Déplacer les plexes affectés hors ligne :

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+



Effectuez cette étape pour tous les plexes dont les disques sont distants sur le cluster\_A.

9. De manière persistante hors ligne les ports de commutateur ISL en fonction du type de commutateur.

10. Arrêtez les nœuds en exécutant la commande suivante sur chaque nœud :

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Mettez l'équipement hors tension sur le site de secours.

Vous devez mettre l'équipement suivant hors tension dans l'ordre indiqué :

- Contrôleurs de stockage : les contrôleurs de stockage doivent se trouver actuellement au niveau du LOADER vous devez les éteindre complètement.
- Commutateurs IP MetroCluster
- Tiroirs de stockage

## Déplacement du site hors tension du MetroCluster

Une fois le site hors tension, vous pouvez commencer les travaux de maintenance. La procédure est la même que si les composants MetroCluster sont déplacés au sein du même data Center ou vers un autre data Center.

- Le matériel doit être câblé de la même manière que le site précédent.
- Si la vitesse, la longueur ou le numéro de la liaison inter-commutateurs (ISL) ont changé, ils doivent tous être reconfigurés.

### Étapes

1. Vérifiez que le câblage de tous les composants est soigneusement enregistré afin de pouvoir le reconnecter correctement au nouvel emplacement.
2. Déplacez physiquement l'ensemble du matériel, des contrôleurs de stockage, des commutateurs IP, des FibreBridges et des tiroirs de stockage.
3. Configurez les ports ISL et vérifiez la connectivité entre les sites.

a. Mettez les commutateurs IP sous tension.



Ne pas mettre d'autres équipements sous tension.

4. Utilisez les outils sur les commutateurs (lorsqu'ils sont disponibles) pour vérifier la connectivité entre les sites.



Vous ne devez continuer que si les liens sont correctement configurés et stables.

5. Désactivez à nouveau les liens s'ils sont stables.

## Mise sous tension de la configuration MetroCluster et retour au fonctionnement normal

Une fois la maintenance effectuée ou le site déplacé, vous devez mettre le site sous tension et rétablir la configuration MetroCluster.

### Description de la tâche

Toutes les commandes des étapes suivantes sont émises à partir du site que vous mettez sous tension.

### Étapes

1. Mettez les commutateurs sous tension.

Vous devez d'abord mettre les commutateurs sous tension. Si le site a été déplacé, il se peut qu'il ait été mis sous tension lors de l'étape précédente.

- a. Reconfigurez le lien ISL (Inter-Switch Link) si nécessaire ou si cela n'a pas été effectué dans le cadre du déplacement.
- b. Activez l'ISL si l'escrime a été terminé.
- c. Vérifiez le lien ISL.

2. Mettez les contrôleurs de stockage sous tension et attendez que le s'affiche `LOADER` à l'invite. Les contrôleurs ne doivent pas être entièrement démarrés.

Si le démarrage automatique est activé, appuyez sur `Ctrl+C` pour empêcher les contrôleurs de démarrer automatiquement.

3. Mettez les tiroirs sous tension, en leur laissant suffisamment de temps pour pouvoir les mettre complètement sous tension.

4. Vérifiez que le stockage est visible.

- a. Vérifiez que le stockage est visible depuis le site survivant. Remettez les plexes hors ligne en ligne pour redémarrer l'opération de resynchronisation et rétablir la SyncMirror.
- b. Vérifiez que le stockage local est visible depuis le nœud en mode Maintenance :

```
disk show -v
```

5. Rétablir la configuration MetroCluster.

Suivez les instructions de la section "[Vérifier que votre système est prêt pour le rétablissement](#)" Afin d'effectuer des opérations de rétablissement et de rétablissement en fonction de votre configuration MetroCluster.

# Mise hors tension de l'intégralité d'une configuration MetroCluster IP

Vous devez mettre hors tension la totalité de la configuration IP d'MetroCluster et de tout l'équipement avant le début des opérations de maintenance ou de relocalisation.



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

1. Vérifier la configuration MetroCluster des deux sites de la configuration MetroCluster.
  - a. Vérifier que la configuration MetroCluster et le mode opérationnel sont normaux.  
**metrocluster show**
  - b. Exécuter la commande suivante :  
**metrocluster interconnect show**
  - c. Vérifier la connectivité sur les disques en saisissant la commande suivante sur l'un des nœuds MetroCluster :  
**run local sysconfig -v**
  - d. Exécuter la commande suivante :  
**storage port show**
  - e. Exécuter la commande suivante :  
**storage switch show**
  - f. Exécuter la commande suivante :  
**network interface show**
  - g. Exécuter la commande suivante :  
**network port show**
  - h. Exécuter la commande suivante :  
**network device-discovery show**
  - i. Effectuer une vérification MetroCluster :  
**metrocluster check run**
  - j. Afficher les résultats de la vérification MetroCluster :  
**metrocluster check show**
  - k. Exécuter la commande suivante :  
**metrocluster configuration-settings interface show**

2. Si nécessaire, désactivez AUSO en modifiant le domaine de défaillance AUSO sur

**auso-disabled**

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain  
auso-disabled
```



Dans une configuration MetroCluster IP, le domaine de défaillance AUSO est déjà défini sur 'auso-Disabled' à moins que la configuration ne soit configurée avec le médiateur ONTAP.

### 3. Vérifiez la modification à l'aide de la commande

#### **metrocluster operation show**

```
cluster_A_site_A::*> metrocluster operation show
  Operation: modify
    State: successful
  Start Time: 4/25/2020 20:20:36
  End Time: 4/25/2020 20:20:36
  Errors: -
```

### 4. Arrêter les nœuds :

#### **halt**

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

### 5. Mettez hors tension l'équipement suivant sur le site :

- Contrôleurs de stockage
- Commutateurs IP MetroCluster
- Tiroirs de stockage

### 6. Attendez trente minutes, puis mettez tous les tiroirs de stockage, les commutateurs IP MetroCluster et les contrôleurs de stockage sous tension.

### 7. Une fois les contrôleurs mis sous tension, vérifiez la configuration MetroCluster des deux sites.

Pour vérifier la configuration, répétez l'étape 1.

### 8. Effectuer des vérifications de cycle d'alimentation.

#### a. Vérifier que tous les SVM source sont en ligne :

**vserver show**

#### b. Démarrez tous les SVM source de synchronisation qui ne sont pas en ligne :

**vserver start**

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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