



# **Que dois-je faire après l'restauration de mon cluster ?**

**ONTAP 9**

NetApp  
April 24, 2024

# Sommaire

- Que dois-je faire après l'restauration de mon cluster ? ..... 1
  - Vérification de l'état du cluster et du stockage après une restauration antérieure ..... 1
  - Basculement automatique pour les configurations MetroCluster. .... 3
  - Activez ou restaurez les LIF sur les ports de base après une restauration ..... 4
  - Activez les règles de copie Snapshot après le rétablissement ..... 6
  - Vérification de l'accès client (SMB et NFS) ..... 6
  - Vérifiez les entrées du pare-feu IPv6 ..... 6
  - Rétablit la fonction de hachage du mot de passe au type de cryptage pris en charge ..... 7
  - Facteurs à prendre en compte pour la mise à jour manuelle du firmware du processeur de service ..... 8
  - Modifier les comptes utilisateur pouvant accéder au Service Processor ..... 8

# Que dois-je faire après l'restauration de mon cluster ?

## Vérification de l'état du cluster et du stockage après une restauration antérieure

Une fois que vous avez déclassés ou repassé un cluster, vérifiez que les nœuds sont en bon état et peuvent participer au cluster, et que le cluster est au quorum. Vous devez également vérifier l'état de vos disques, agrégats et volumes.

### Vérification de l'état du cluster

1. Vérifiez que les nœuds du cluster sont en ligne et peuvent participer au cluster : `cluster show`

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0                true   true
node1                true   true
```

Si l'un des nœuds est défectueux ou non éligible, vérifiez la présence d'erreurs dans les journaux EMS et effectuez des actions correctives.

2. Définissez le niveau de privilège sur avancé :  
`set -privilege advanced`

Entrez `y` pour continuer.

3. Vérifier les détails de configuration pour chaque processus RDB
  - L'époque de la base de données relationnelle et les séries de tests de base de données doivent correspondre pour chaque nœud.
  - Le maître de quorum par anneau doit être le même pour tous les nœuds.

Notez que chaque anneau peut avoir un maître de quorum différent.

Pour afficher ce processus RDB...	Entrez cette commande...
Application de gestion	<code>cluster ring show -unitname mgmt</code>
Base de données d'emplacement de volume	<code>cluster ring show -unitname vl原因</code>
Gestionnaire d'interface virtuelle	<code>cluster ring show -unitname vifmgr</code>
Démon de gestion DU SAN	<code>cluster ring show -unitname bcomd</code>

Cet exemple représente le processus de la base de données d'emplacements de volumes :

```
cluster1::*> cluster ring show -unitname vldb
Node          UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0         vldb      154         154      14847  node0      master
node1         vldb      154         154      14847  node0      secondary
node2         vldb      154         154      14847  node0      secondary
node3         vldb      154         154      14847  node0      secondary
4 entries were displayed.
```

4. Retour au niveau de privilège admin : `set -privilege admin`
5. Si vous travaillez dans un environnement SAN, vérifiez que chaque nœud se trouve dans un quorum SAN : `event log show -severity informational -message-name scsiblade.*`

Le message d'événement scsiBlade le plus récent pour chaque nœud doit indiquer que le SCSI-Blade est quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
Time          Node      Severity      Event
-----
MM/DD/YYYY TIME node0      INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME node1      INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
```

## Informations associées

["Administration du système"](#)

## Vérification de l'état du stockage

Lorsque vous restaurez ou déclassés un cluster, vous devez vérifier l'état de vos disques, agrégats et volumes.

1. Vérification de l'état du disque :

Pour vérifier...	Procédez comme ça...
Disques cassés	<ol style="list-style-type: none"><li>a. Afficher les éventuels disques défectueux : <code>storage disk show -state broken</code></li><li>b. Retirez ou remplacez tout disque endommagé.</li></ol>

Pour vérifier...	Procédez comme ça...
Disques soumis à des opérations de maintenance ou de reconstruction	a. Afficher tous les disques en état de maintenance, en attente ou reconstruction : <code>`storage disk show -state maintenance`</code>
pending	reconstructing` .. Attendez la fin de l'opération de maintenance ou de reconstruction avant de poursuivre.

- Vérifiez que tous les agrégats sont en ligne en affichant l'état du stockage physique et logique, y compris les agrégats de stockage : `storage aggregate show -state !online`

Cette commande affiche les agrégats qui sont *not* online. Tous les agrégats doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Vérifiez que tous les volumes sont en ligne en affichant les volumes *NOT* online : `volume show -state !online`

Tous les volumes doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

- Vérifiez qu'il n'y a pas de volumes incohérents : `volume show -is-inconsistent true`

Consultez l'article de la base de connaissances "[Volume affichant des WAFL incohérentes](#)" sur la manière de traiter les volumes incohérents.

#### Informations associées

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

## Basculement automatique pour les configurations MetroCluster

Cette rubrique fournit des informations sur les tâches supplémentaires que vous devez effectuer après la reversion des configurations MetroCluster.

- Basculement automatique non planifié : `metrocluster modify -auto-switchover-failure -domain auto-on-cluster-disaster`
- Valider la configuration MetroCluster : `metrocluster check run`

# Activez ou restaurez les LIF sur les ports de base après une restauration

Au cours d'un redémarrage, certaines LIFs ont peut-être été migrées vers leurs ports de basculement qui leur sont attribués. Une fois que vous restaurez un cluster, vous devez activer et restaurer toutes les LIF qui ne se trouvent pas sur leur port de base.

La commande `network interface revert` restaure une LIF qui n'est pas actuellement sur son port home port vers son port home port, à condition que le port home port soit opérationnel. Le port de base d'une LIF est spécifié lors de sa création ; vous pouvez déterminer le port d'origine d'une LIF à l'aide de la commande `network interface show`.

- 1. Afficher le statut de toutes les LIFs : `network interface show`

Cet exemple affiche l'état de toutes les LIFs d'un Storage Virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
vs0					
	data001	down/down	192.0.2.120/24	node0	e0e
true					
	data002	down/down	192.0.2.121/24	node0	e0f
true					
	data003	down/down	192.0.2.122/24	node0	e2a
true					
	data004	down/down	192.0.2.123/24	node0	e2b
true					
	data005	down/down	192.0.2.124/24	node0	e0e
false					
	data006	down/down	192.0.2.125/24	node0	e0f
false					
	data007	down/down	192.0.2.126/24	node0	e2a
false					
	data008	down/down	192.0.2.127/24	node0	e2b
false					

8 entries were displayed.

Si des LIF dont le statut Status Admin est down ou avec un état is home est false, passez à l'étape suivante.

- 2. Activation des LIFs de données : `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

### 3. Rerestaurer les LIF sur leurs home ports : `network interface revert *`

Cette commande restaure toutes les LIF vers leur port de base.

```
cluster1::> network interface revert *
8 entries were acted on.
```

### 4. Vérifier que toutes les LIFs se trouvent sur leurs ports de type home : `network interface show`

Cet exemple montre que toutes les LIFs pour SVM vs0 sont sur leurs ports de base.

```
cluster1::> network interface show -vserver vs0
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
vs0					
true	data001	up/up	192.0.2.120/24	node0	e0e
true	data002	up/up	192.0.2.121/24	node0	e0f
true	data003	up/up	192.0.2.122/24	node0	e2a
true	data004	up/up	192.0.2.123/24	node0	e2b
true	data005	up/up	192.0.2.124/24	node1	e0e
true	data006	up/up	192.0.2.125/24	node1	e0f
true	data007	up/up	192.0.2.126/24	node1	e2a
true	data008	up/up	192.0.2.127/24	node1	e2b

```
8 entries were displayed.
```

# Activez les règles de copie Snapshot après le rétablissement

Après avoir restauré vers une version antérieure de ONTAP, vous devez activer les règles de copie Snapshot pour recommencer la création de copies Snapshot.

Vous réactivez les planifications Snapshot que vous avez désactivées avant de revenir à une version antérieure de ONTAP.

1. Activez les règles de copie Snapshot pour tous les SVM de données :

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Pour chaque nœud, activez la règle de copie Snapshot du volume racine à l'aide de la commande `run-nodenodenodaémaux optionsroot_vol_namenossip off`.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

## Vérification de l'accès client (SMB et NFS)

Pour les protocoles configurés, testez l'accès des clients SMB et NFS afin de vérifier que le cluster est accessible.

## Vérifiez les entrées du pare-feu IPv6

Une nouvelle version à partir de n'importe quelle version de ONTAP 9 peut entraîner l'absence d'entrées de pare-feu IPv6 par défaut pour certains services dans les politiques de pare-feu. Vous devez vérifier que les entrées de pare-feu requises ont été restaurées sur votre système.

1. Vérifiez que toutes les politiques de pare-feu sont correctes en les comparant aux politiques par défaut :

```
system services firewall policy show
```

L'exemple suivant montre les règles par défaut :



```
cluster1::*> system services firewall policy show
```

Policy	Service	Action	IP-List
-----			
cluster	dns	allow	0.0.0.0/0
	http	allow	0.0.0.0/0
	https	allow	0.0.0.0/0
	ndmp	allow	0.0.0.0/0
	ntp	allow	0.0.0.0/0
	rsh	allow	0.0.0.0/0
	snmp	allow	0.0.0.0/0
	ssh	allow	0.0.0.0/0
	telnet	allow	0.0.0.0/0
data	dns	allow	0.0.0.0/0, ::/0
	http	deny	0.0.0.0/0, ::/0
	https	deny	0.0.0.0/0, ::/0
	ndmp	allow	0.0.0.0/0, ::/0
	ntp	deny	0.0.0.0/0, ::/0
	rsh	deny	0.0.0.0/0, ::/0
.			
.			
.			

2. Ajoutez manuellement toutes les entrées de pare-feu IPv6 par défaut manquantes en créant une nouvelle politique de pare-feu : `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6  
-service ssh -action allow -ip-list ::/0
```

3. Appliquer la nouvelle policy à la LIF pour autoriser l'accès à un service réseau : `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1  
-firewall-policy newIPv6
```

## Rétablit la fonction de hachage du mot de passe au type de cryptage pris en charge

Si vous êtes ramené de ONTAP 9.1 ou ONTAP 9.0 à ONTAP 8.3.x, les utilisateurs de compte SHA-2 ne peuvent plus être authentifiés avec leurs mots de passe. Les mots de passe doivent être réinitialisés pour utiliser le type de cryptage MDS.

1. Définissez un mot de passe temporaire pour chaque compte utilisateur SHA-2 que vous [identifié avant le rétablissement](#): `security login password -username user_name -vserver vserver_name`
2. Communiquez le mot de passe temporaire aux utilisateurs concernés et demandez-leur de se connecter par le biais d'une console ou d'une session SSH pour modifier leur mot de passe comme le système l'invite.

## Facteurs à prendre en compte pour la mise à jour manuelle du firmware du processeur de service

Si la fonctionnalité de mise à jour automatique du processeur de service est activée (par défaut), la rétrogradation ou le rétablissement de ONTAP 8.3.x ne nécessite pas de mise à jour manuelle du micrologiciel du processeur de service. Le micrologiciel du processeur de service est automatiquement mis à jour vers la dernière version compatible prise en charge par la version ONTAP que vous avez rétablie ou rétrogradée.

Si la fonctionnalité de mise à jour automatique du processeur de service est désactivée (non recommandée), après ONTAP la fin du processus de restauration ou de mise à niveau vers une version antérieure du micrologiciel du processeur de service, vous devez mettre à jour manuellement la version prise en charge pour la version de ONTAP à laquelle vous avez rétabli ou déclassé.

["Matrice de prise en charge NetApp BIOS/ONTAP"](#)

["Téléchargements NetApp : firmware système et diagnostics"](#)

## Modifier les comptes utilisateur pouvant accéder au Service Processor

Si vous avez créé des comptes utilisateur sur ONTAP 9.8 ou une version antérieure, passez à ONTAP 9.9.1 ou une version ultérieure (lorsque l' `-role` paramètre est remplacé par `admin`), puis revient à ONTAP 9.8 ou antérieur, le `-role` le paramètre est restauré à sa valeur d'origine. Vous devez néanmoins vérifier que les valeurs modifiées sont acceptables.

Lors de la restauration, si le rôle d'un utilisateur SP a été supprimé, le message « `rbac.spuser.role.notfound` » EMS sera enregistré.

Pour plus d'informations, voir ["Comptes pouvant accéder au processeur de service"](#).

## 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 DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

## Informations sur les marques commerciales

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