Configuration NDMP

ONTAP 9

NetApp
September 12, 2024

Sommaire

Configuration NDMP

Présentation de la configuration NDMP

Vous pouvez rapidement configurer un cluster ONTAP 9 de sorte qu'il utilise le protocole NDMP (Network Data Management Protocol) pour sauvegarder les données directement sur bande à l'aide d'une application de sauvegarde tierce.

Si l'application de backup supporte Cluster Aware Backup (CAB), vous pouvez configurer NDMP sous la forme *SVM-scoped* ou *node-scoped* :

- SVM-scoped au niveau du cluster (admin SVM) permet de sauvegarder tous les volumes hébergés sur différents nœuds du cluster. SVM-scoped NDMP est recommandé si possible.
- Node-scoped NDMP vous permet de sauvegarder tous les volumes hébergés sur ce nœud.

Si l'application de backup ne prend pas en charge CAB, il faut utiliser node-scoped NDMP.

SVM-scoped et node-scoped NDMP sont mutuellement exclusifs ; ils ne peuvent pas être configurés sur le même cluster.

> Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

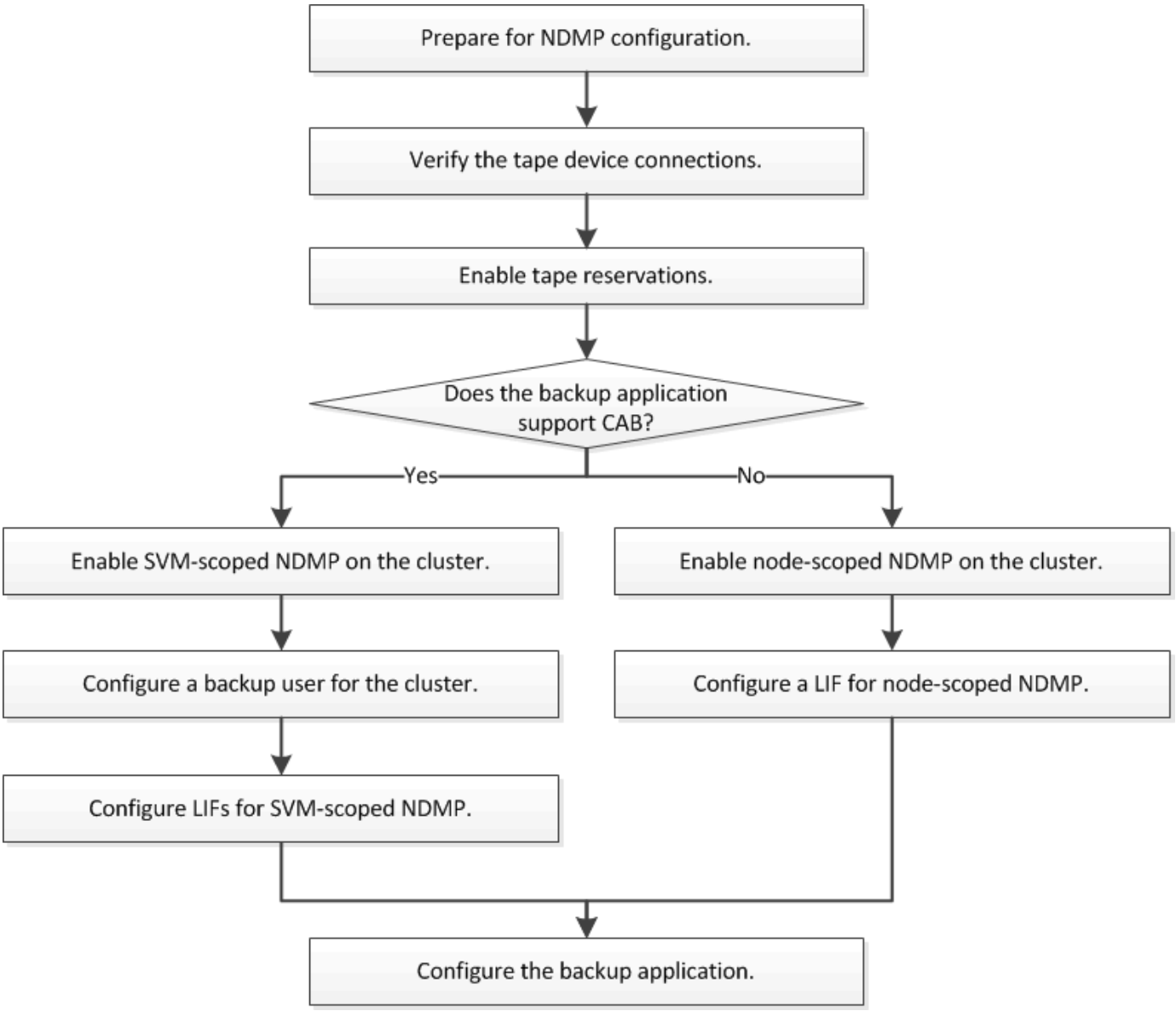
En savoir plus sur "Sauvegarde « cluster Aware Backup » (CAB)".

Avant de configurer NDMP, vérifiez les points suivants :

- Vous disposez d'une application de sauvegarde tierce (également appelée Data Management application ou DMA).
- Vous êtes un administrateur de cluster.
- Les périphériques de bande et un serveur multimédia en option sont installés.
- Les périphériques de bande sont connectés au cluster via un commutateur Fibre Channel (FC) et ne sont pas directement connectés.
- Au moins une unité de bande a un numéro d'unité logique (LUN) de 0.

Workflow de configuration NDMP

La configuration de la sauvegarde sur bande sur NDMP implique la préparation de la configuration NDMP, la vérification des connexions du périphérique de bande, l'activation des réservations sur bande, la configuration de NDMP au niveau SVM ou node, l'activation de NDMP sur le cluster, la configuration d'un utilisateur de sauvegarde, la configuration des LIFs et la configuration de l'application de sauvegarde.



Préparation à la configuration NDMP

Avant de configurer l'accès de sauvegarde sur bande via le protocole NDMP (Network Data Management Protocol), vous devez vérifier que la configuration planifiée est prise en charge. Vérifier que vos lecteurs de bande sont répertoriés comme disques qualifiés sur chaque nœud, vérifier que tous les nœuds disposent des LIF intercluster, Et déterminer si l'application de sauvegarde prend en charge l'extension CLUSTER Aware Backup (CAB).

Étapes

1. Consultez le tableau de compatibilité de votre fournisseur d'applications de sauvegarde pour la prise en charge du protocole ONTAP (NetApp ne qualifier pas les applications de sauvegarde tierces avec ONTAP ou NDMP).

   Vérifiez que les composants NetApp suivants sont compatibles :

   - Version de ONTAP 9 qui s'exécute sur le cluster.

- Le fournisseur et la version de l'application de sauvegarde, par exemple Veritas NetBackup 8.2 ou CommVault.
- Les lecteurs de bande décrivent en détail le fabricant, le modèle et l'interface des lecteurs de bande, par exemple IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- Plateformes des nœuds du cluster : par exemple, FAS8700 ou A400

> Vous trouverez des matrices de support de compatibilité ONTAP existantes pour les applications de sauvegarde dans le "Matrice d'interopérabilité NetApp".

2. Vérifiez que vos lecteurs de bande sont répertoriés comme lecteurs qualifiés dans le fichier de configuration de bande intégré de chaque nœud :

   a. Sur l'interface de ligne de commande, affichez le fichier de configuration de bande intégré à l'aide du `storage tape show-supported-status` commande.

   ```
   cluster1::> storage tape show-supported-status

   Node: cluster1-1
                                   Is
   Tape Drives                     Supported  Support Status
   -------------------------------  ---------
   -------------------------------
   Certance Ultrium 2              true       Dynamically Qualified
   Certance Ultrium 3              true       Dynamically Qualified
   Digital DLT2000                 true       Qualified
   ```

   b. Comparez vos lecteurs de bande à la liste des lecteurs qualifiés dans la sortie.

   > Les noms des périphériques de bande dans la sortie peuvent varier légèrement par rapport aux noms figurant sur l'étiquette du périphérique ou dans la matrice d'interopérabilité. Par exemple, le DLT2000 numérique peut également être appelé DL2k. Vous pouvez ignorer ces différences mineures de dénomination.

   c. Si un périphérique ne figure pas dans la liste comme indiqué dans le résultat, même si celui-ci est qualifié conformément à la matrice d'interopérabilité, téléchargez et installez un fichier de configuration mis à jour pour le périphérique, en suivant les instructions du site du support NetApp.

   "Téléchargements NetApp : fichiers de configuration des lecteurs de bande"

   Il se peut qu'un périphérique qualifié ne figure pas dans le fichier de configuration de bande intégré si le périphérique de bande a été qualifié après l'expédition du nœud.

3. Vérifier que chaque nœud du cluster dispose d'un LIF intercluster :

   a. Afficher les LIFs intercluster sur les nœuds en utilisant le `network interface show -role intercluster` commande.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Si aucune LIF intercluster n'existe sur un nœud, créer une LIF intercluster en utilisant le `network interface create` commande.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gestion du réseau"

4. Déterminez si l'application de sauvegarde prend en charge Cluster Aware Backup (CAB) à l'aide de la documentation fournie avec l'application de sauvegarde.

   Le support CAB est un facteur clé pour déterminer le type de sauvegarde que vous pouvez effectuer.

Vérifiez les connexions du lecteur de bande

Vous devez vous assurer que tous les lecteurs et changeurs de supports sont visibles

dans ONTAP en tant que périphériques.

Étapes

1. Affichez des informations sur tous les lecteurs et changeurs de supports à l'aide du `storage tape show` commande.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11                tape drive      HP LTO-3
normal
0b.125L1                 media changer   HP MSL G3 Series
normal
0d.4                     tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                   media changer   IBM 3573-TL
normal
...
```

2. Si aucun lecteur de bande n'est affiché, résolvez le problème.
3. Si un changeur de supports n'est pas affiché, affichez les informations relatives aux changeurs de supports à l'aide du `storage tape show-media-changer` commande, puis résolution du problème.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Activer les réservations sur bande

Vous devez vous assurer que les lecteurs de bande sont réservés à l'utilisation par les applications de sauvegarde pour les opérations de sauvegarde NDMP.

Description de la tâche

Les paramètres de réservation varient selon les applications de sauvegarde et ces paramètres doivent correspondre à l'application de sauvegarde et aux nœuds ou serveurs utilisant les mêmes lecteurs. Consultez la documentation fournisseur de l'application de sauvegarde pour connaître les paramètres de réservation corrects.

Étapes

1. Activer les réservations à l'aide de `options -option-name tape.reservations -option-value persistent` commande.

   La commande suivante active les réservations avec le `persistent` valeur :

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Vérifiez que les réservations sont activées sur tous les nœuds à l'aide de l' `options tape.reservations` commande, puis vérifiez la sortie.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

cluster1-2
    tape.reservations                persistent
2 entries were displayed.
```

Configurer SVM-scoped NDMP

Activer SVM-scoped NDMP sur le cluster

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

Ce dont vous avez besoin

L'extension CAB doit être prise en charge par le DMA.

Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

1. Activer le mode NDMP SVM-scoped :

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   Le mode NDMP SVM-scoped est activé.

2. Activer le service NDMP sur le SVM d'admin:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   Le type d'authentification est défini sur `challenge` par défaut, l'authentification en texte brut est désactivée.

   > Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

3. Vérifier que le service NDMP est activé :

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Activez un utilisateur de sauvegarde pour l'authentification NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : `admin` ou `backup`
- SVM individuels : `vsadmin` ou `vsadmin-backup`

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.

Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

   ```
   security login show
   ```

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec le `security login create` Commande et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

   Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l' `-user-or-group-name` paramètre.

   La commande suivante crée l'utilisateur de sauvegarde `backup_admin1` avec le `backup` rôle pour l'ensemble du cluster :

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   La commande suivante crée l'utilisateur de sauvegarde `vsbackup_admin1` avec le `vsadmin-backup` Rôle d'un SVM individuel :

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Entrez un mot de passe pour le nouvel utilisateur et confirmez.

3. Générer un mot de passe pour la SVM d'admin via le `vserver services ndmp generate password` commande.

   Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configurez les LIF

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Une fois les LIF définies, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour les LIF et spécifier le rôle d'interface privilégié.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Étapes

1. Identifier les LIF intercluster, cluster-management et node-management en utilisant le `network interface show` commande avec `-role` paramètre.

   La commande suivante affiche les LIFs intercluster :

```
cluster1::> network interface show -role intercluster

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    IC1               up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2               up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   La commande suivante affiche la LIF cluster-management :

```
cluster1::> network interface show -role cluster-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M     true
```

La commande suivante affiche les LIFs de node-management :

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------ ------------
------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24      cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24      cluster1-2
e0M     true
```

2. S’assurer que la politique de pare-feu est activée pour NDMP sur les LIF intercluster, cluster-management (cluster-mgmt) et node-management (node-mgmt) :

   a. Vérifiez que la politique de pare-feu est activée pour NDMP à l’aide de `system services firewall policy show` commande.

      La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                        ** ndmp       0.0.0.0/0**
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

   La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

   a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-domain-wide`, Et la policy pour les LIFs intercluster et node-management est définie sur `local-only` à l'aide du `network interface show -failover` commande.

      La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ----------------- --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover Targets:
                                                     .......

**cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-wide
Default**
                                                     Failover Targets:
                                                     .......
           **IC1                 cluster1-1:e0a    local-only
Default**
                                                     Failover Targets:
           **IC2                 cluster1-1:e0b    local-only
Default**
                                                     Failover Targets:
                                                     .......
**cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
**cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
```

a. Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
             Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

Configurer node-scoped NDMP

Activez NDMP node-scoped sur le cluster

Vous pouvez sauvegarder des volumes hébergés sur un seul nœud en activant NDMP node-scoped, en activant le service NDMP et en configurant une LIF pour la connexion data et contrôle. Cela peut être effectué pour tous les nœuds du cluster.

> Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

Description de la tâche

Si vous utilisez NDMP en mode node-scope, l'authentification doit être configurée sur la base de chaque nœud. Pour plus d'informations, voir "L'article de la base de connaissances "Comment configurer l'authentification NDMP en mode 'node-scope'"".

Étapes

1. Activer le mode NDMP node-scoped :

```
cluster1::> system services ndmp node-scope-mode on
```

   NDMP node-scope-mode est activé.

2. Activer le service NDMP sur tous les nœuds du cluster :

   L'utilisation du caractère générique "*" permet le service NDMP sur tous les nœuds en même temps.

   Vous devez spécifier un mot de passe pour l'authentification de la connexion NDMP par l'application de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Désactivez le `-clear-text` Option pour la communication sécurisée du mot de passe NDMP :

   Utilisation du caractère générique “*” disables the `-clear-text` option sur tous les nœuds simultanément.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Vérifiez que le service NDMP est activé et que `-clear-text` l’option est désactivée :

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurer une LIF

Vous devez identifier une LIF qui sera utilisée pour établir une connexion de données et une connexion de contrôle entre le nœud et l’application de sauvegarde. Après avoir identifié le LIF, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour le LIF.

> Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d’informations, voir "Configuration des politiques de pare-feu pour les LIF".

Étapes

1. Identifier le LIF intercluster hébergé sur les nœuds en utilisant le `network interface show` commande avec `-role` paramètre.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a
true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b
true
```

2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIFs intercluster :

   a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

      La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

      La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la politique de basculement est correctement définie pour les LIFs intercluster :

a. Vérifier que la policy de basculement pour les LIFs intercluster est définie sur `local-only` à l'aide du `network interface show -failover` commande.

```
cluster1::> network interface show -failover
            Logical          Home               Failover     Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  ----------------- ------------ --------
cluster1    **IC1               cluster1-1:e0a    local-only
Default**
                                                    Failover Targets:
                                                    .......
            **IC2               cluster1-2:e0b    local-only
Default**
                                                    Failover Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only    Default
                                                    Failover Targets:
                                                    .......
```

b. Si la stratégie de basculement n'est pas définie de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configurez l'application de sauvegarde

Une fois le cluster configuré pour l'accès NDMP, vous devez collecter les informations de la configuration du cluster, puis configurer le reste du processus de sauvegarde dans l'application de sauvegarde.

Étapes

1. Collectez les informations suivantes que vous avez configurées précédemment dans ONTAP :
   - Nom d'utilisateur et mot de passe requis par l'application de sauvegarde pour créer la connexion NDMP
   - Les adresses IP des LIFs intercluster que l'application de sauvegarde nécessite pour se connecter au cluster
2. Dans ONTAP, affichez les alias attribués par ONTAP à chaque périphérique en utilisant le `storage tape alias show` commande.

   Les alias sont souvent utiles pour configurer l'application de sauvegarde.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                        Alias     Mapping
--------------------------- --------- -------------------------------
stsw-3220-4a-4b-02          st2       SN[HU19497WVR]
...
```

3. Dans l'application de sauvegarde, configurez le reste du processus de sauvegarde à l'aide de la documentation de l'application de sauvegarde.

Une fois que vous avez terminé

En cas de mobilité des données, comme un déplacement de volume ou une migration LIF, vous devez être prêt à réinitialiser les opérations de sauvegarde interrompues.