Configuração NDMP

ONTAP 9

NetApp
January 17, 2025

Índice

Configuração NDMP

Visão geral da configuração NDMP

Você pode configurar rapidamente um cluster ONTAP 9 para usar o Protocolo de gerenciamento de dados de rede (NDMP) para fazer backup de dados diretamente em fita usando um aplicativo de backup de terceiros.

Se o aplicativo de backup oferecer suporte ao Cluster Aware Backup (CAB), você poderá configurar o NDMP como *SVM-scoped* ou *node-scoped*:

- O escopo do SVM no nível do cluster (admin SVM) permite fazer backup de todos os volumes hospedados em diferentes nós do cluster. NDMP com escopo SVM é recomendado, sempre que possível.
- O NDMP com escopo de nó permite fazer backup de todos os volumes hospedados nesse nó.

Se o aplicativo de backup não suportar CAB, você deve usar NDMP com escopo de nó.

NDMP com escopo SVM e escopo de nó são mutuamente exclusivos; eles não podem ser configurados no mesmo cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

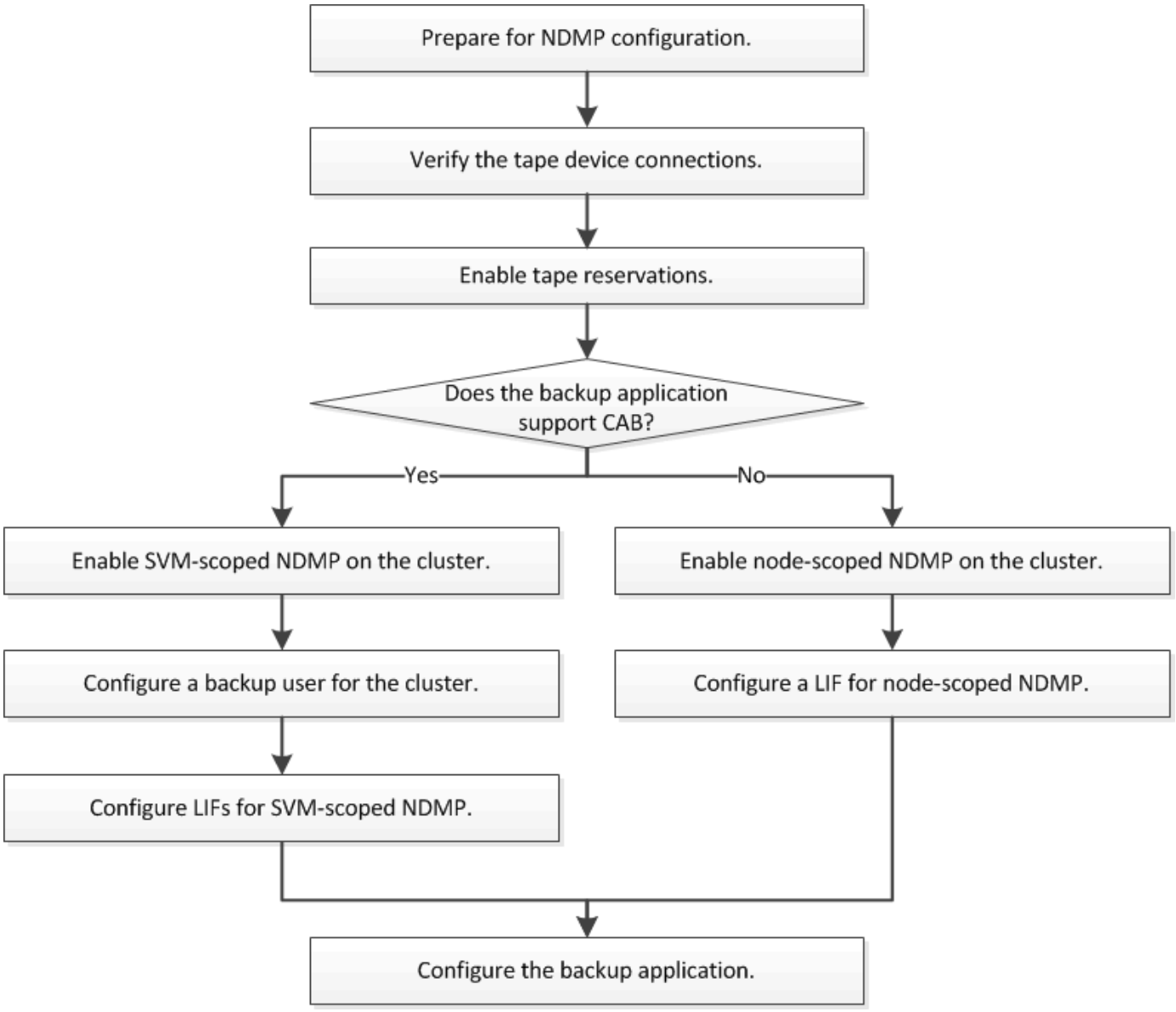
Saiba mais "Backup ciente de cluster (CAB)"sobre o .

Antes de configurar o NDMP, verifique o seguinte:

- Você tem um aplicativo de backup de terceiros (também chamado de aplicativo de gerenciamento de dados ou DMA).
- Você é um administrador de cluster.
- Dispositivos de fita e um servidor de Mídia opcional estão instalados.
- Os dispositivos de fita são conetados ao cluster por meio de um switch Fibre Channel (FC) ou conetados localmente.
- Pelo menos um dispositivo de fita tem um número de unidade lógica (LUN) de 0.

Fluxo de trabalho de configuração NDMP

A configuração do backup em fita no NDMP envolve a preparação para a configuração NDMP, a verificação das conexões do dispositivo de fita, a ativação de reservas de fita, a configuração do NDMP no nível do SVM ou nó, a ativação do NDMP no cluster, a configuração de um usuário de backup, a configuração de LIFs e a configuração do aplicativo de backup.



Prepare-se para a configuração NDMP

Antes de configurar o acesso de backup em fita pelo Network Data Management Protocol (NDMP), você deve verificar se a configuração planejada é suportada, verificar se suas unidades de fita estão listadas como unidades qualificadas em cada nó, verificar se todos os nós têm LIFs entre clusters e identificar se o aplicativo de backup suporta a extensão CAB (Cluster Aware Backup).

Passos

1. Consulte a matriz de compatibilidade do fornecedor do aplicativo de backup para obter suporte ao ONTAP (o NetApp não qualifica aplicativos de backup de terceiros com ONTAP ou NDMP).

   Você deve verificar se os seguintes componentes do NetApp são compatíveis:

   - A versão do ONTAP 9 que está sendo executada no cluster.
   - O fornecedor e a versão do aplicativo de backup: Por exemplo, Veritas NetBackup 8,2 ou CommVault.

- Os detalhes dos dispositivos de fita, como o fabricante, o modelo e a interface das unidades de fita: Por exemplo, IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- As plataformas dos nós no cluster: Por exemplo, FAS8700 ou A400.

> Você pode encontrar matrizes de suporte de compatibilidade legadas do ONTAP para aplicativos de backup no "Ferramenta de Matriz de interoperabilidade do NetApp".

2. Verifique se suas unidades de fita estão listadas como unidades qualificadas no arquivo de configuração de fita interno de cada nó:

   a. Na interface de linha de comando, visualize o arquivo de configuração de fita incorporado usando o `storage tape show-supported-status` comando.

```
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. Compare suas unidades de fita com a lista de unidades qualificadas na saída.

> Os nomes dos dispositivos de fita na saída podem variar ligeiramente dos nomes na etiqueta do dispositivo ou na Matriz de interoperabilidade. Por exemplo, o Digital DLT2000 também pode ser conhecido como DLT2k. Você pode ignorar essas pequenas diferenças de nomenclatura.

   c. Se um dispositivo não estiver listado como qualificado na saída, mesmo que o dispositivo esteja qualificado de acordo com a Matriz de interoperabilidade, baixe e instale um arquivo de configuração atualizado para o dispositivo usando as instruções no site de suporte da NetApp.

      "Downloads do NetApp: Arquivos de configuração do dispositivo de fita"

   Um dispositivo qualificado pode não estar listado no arquivo de configuração de fita incorporado se o dispositivo de fita tiver sido qualificado após o nó ser enviado.

3. Verifique se cada nó no cluster tem um LIF entre clusters:

   a. Visualize as LIFs entre clusters nos nós usando o `network interface show -role intercluster` comando.

```
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. Se um LIF entre clusters não existir em nenhum nó, crie um LIF entre clusters usando o `network interface create` comando.

```
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
```

"Gerenciamento de rede"

4. Identifique se o aplicativo de backup suporta Backup ciente de cluster (CAB) usando a documentação fornecida com o aplicativo de backup.

   O suporte DA CAB é um fator chave para determinar o tipo de backup que você pode executar.

Verifique as conexões do dispositivo de fita

Você deve garantir que todas as unidades e alteradores de Mídia estejam visíveis no

ONTAP como dispositivos.

Passos

1. Veja informações sobre todas as unidades e modificadores de Mídia usando o `storage tape show` comando.

```
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. Se uma unidade de fita não for exibida, solucione o problema.
3. Se um trocador de Mídia não for exibido, exiba informações sobre alteradores de Mídia usando o `storage tape show-media-changer` comando e solucione o problema.

```
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
...
```

Ative as reservas de fita

Você deve garantir que as unidades de fita sejam reservadas para uso por aplicativos de backup para operações de backup NDMP.

Sobre esta tarefa

As configurações de reserva variam em diferentes aplicativos de backup, e essas configurações devem corresponder ao aplicativo de backup e aos nós ou servidores que usam as mesmas unidades. Consulte a documentação do fornecedor do aplicativo de backup para obter as configurações corretas de reserva.

Passos

1. Ative as reservas usando o `options -option-name tape.reservations -option-value persistent` comando.

   O seguinte comando permite reservas com o `persistent` valor:

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

2. Verifique se as reservas estão ativadas em todos os nós usando o `options tape.reservations` comando e, em seguida, revise a saída.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

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

Configurar NDMP com escopo SVM

Habilite NDMP com escopo SVM no cluster

Se o DMA oferecer suporte à extensão CAB (Cluster Aware Backup), você poderá fazer backup de todos os volumes hospedados em diferentes nós em um cluster habilitando NDMP com escopo SVM, habilitando o serviço NDMP no cluster (admin SVM) e configurando LIFs para conexão de dados e controle.

O que você vai precisar

A extensão DA CABINA tem de ser suportada pelo DMA.

Sobre esta tarefa

Desativar o modo NDMP com escopo de nó ativa o modo NDMP com escopo SVM no cluster.

Passos

1. Ativar o modo NDMP com escopo SVM:

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

   O modo NDMP com escopo SVM está ativado.

2. Habilite o serviço NDMP no administrador SVM:

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

   O tipo de autenticação é definido como `challenge` por padrão e a autenticação de texto sem formatação é desativada.

   > Para uma comunicação segura, você deve manter a autenticação em texto simples desativada.

3. Verifique se o serviço NDMP está ativado:

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

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

Ative um usuário de backup para autenticação NDMP

Para autenticar NDMP com escopo SVM a partir do aplicativo de backup, deve haver um usuário administrativo com Privileges suficiente e uma senha NDMP.

Sobre esta tarefa

Você deve gerar uma senha NDMP para usuários de administração de backup. É possível habilitar usuários de administração de backup no nível de cluster ou SVM e, se necessário, criar um novo usuário. Por padrão, os usuários com as seguintes funções podem se autenticar para backup NDMP:

- Em todo o cluster: `admin` Ou `backup`
- SVMs individuais: `vsadmin` Ou `vsadmin-backup`

Se estiver a utilizar um utilizador NIS ou LDAP, o utilizador tem de existir no respetivo servidor. Você não pode usar um usuário do ative Directory.

Passos

1. Exibir os usuários e permissões de administrador atuais:

   ```
   security login show
   ```

2. Se necessário, crie um novo usuário de backup NDMP com o `security login create` comando e a função apropriada para o SVM Privileges individual ou em todo o cluster.

   Pode especificar um nome de utilizador de cópia de segurança local ou um nome de utilizador NIS ou LDAP para o `-user-or-group-name` parâmetro.

   O comando a seguir cria o usuário de backup `backup_admin1` com a `backup` função para todo o cluster:

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

   O comando a seguir cria o usuário de `vsbackup_admin1` backup com a `vsadmin-backup` função de um SVM individual:

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

   Introduza uma palavra-passe para o novo utilizador e confirme.

3. Gere uma senha para o administrador SVM usando o `vserver services ndmp generate password` comando.

   A senha gerada deve ser usada para autenticar a conexão NDMP pelo aplicativo de backup.

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

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

Configurar LIFs

Você precisa identificar os LIFs que serão usados para estabelecer uma conexão de dados entre os recursos de dados e fita, e para conexão de controle entre o SVM admin e o aplicativo de backup. Depois de identificar os LIFs, você deve verificar se as políticas de serviço e failover estão definidas.

A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Identifique o LIF de gerenciamento hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-management
   ```

3. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

4. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

   a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

      O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
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-  Default
                                                domain-wide
                                                        Failover
Targets:
                                                        .......
          IC1              cluster1-1:e0a   local-only  Default
                                                        Failover
Targets:
          IC2              cluster1-1:e0b   local-only  Default
                                                        Failover
Targets:
                                                        .......
cluster1-1 c1-1_mgmt1      cluster1-1:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
cluster1-2 c1-2_mgmt1      cluster1-2:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
```

a. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

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

5. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

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

6. Verifique se a função de interface preferida está definida para o cluster usando o `vserver`

`services ndmp show` comando.

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

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

ONTAP 9 1.9 ou anterior

Passos

1. Identifique os LIFs entre clusters, gerenciamento de cluster e gerenciamento de nós usando o `network interface show` comando com o `-role` parâmetro.

   O comando a seguir exibe as LIFs entre clusters:

```
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
```

   O comando a seguir exibe o LIF de gerenciamento de cluster:

```
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
```

   O comando a seguir exibe as LIFs de gerenciamento de nó:

```
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. Certifique-se de que a política de firewall está ativada para NDMP nos (`node-mgmt`LIFs entre clusters, gerenciamento de cluster (`cluster-mgmt`) e gerenciamento de nós):

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

      O comando a seguir exibe a política de firewall para o LIF de gerenciamento de cluster:

      ```
      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.
      ```

      O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
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.
```

O comando a seguir exibe a política de firewall para o LIF de gerenciamento de nós:

```
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. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

O seguinte comando ativa a política de firewall para o LIF entre clusters:

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

3. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

   O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
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. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

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

4. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

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

5. Verifique se a função de interface preferida está definida para o cluster usando o `vserver services ndmp show` comando.

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

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

Configurar NDMP com escopo de nó

Habilite NDMP com escopo de nó no cluster

Você pode fazer backup de volumes hospedados em um único nó habilitando NDMP com escopo de nó, habilitando o serviço NDMP e configurando um LIF para conexão de dados e controle. Isso pode ser feito para todos os nós do cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

Sobre esta tarefa

Ao usar NDMP no modo de escopo de nó, a autenticação deve ser configurada por nó. Para obter mais informações, "O artigo da base de dados de Conhecimento "como configurar a autenticação NDMP no modo 'nó-escopo'""consulte .

Passos

1. Ativar o modo NDMP com escopo de nó:

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

O modo de escopo do nó NDMP está ativado.

2. Habilite o serviço NDMP em todos os nós do cluster:

   O uso do curinga "'*" permite o serviço NDMP em todos os nós ao mesmo tempo.

   Você deve especificar uma senha para autenticação da conexão NDMP pelo aplicativo de backup.

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

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

3. Desative a `-clear-text` opção de comunicação segura da senha NDMP:

   Usando a opção curinga "'*" `disables the `-clear-text` em todos os nós ao mesmo tempo.

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

4. Verifique se o serviço NDMP está ativado e se a `-clear-text` opção está desativada:

```
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.
```

Configurar um LIF

Você deve identificar um LIF que será usado para estabelecer uma conexão de dados e controlar a conexão entre o nó e o aplicativo de backup. Depois de identificar o LIF, você deve verificar se as políticas de firewall e failover estão definidas para o LIF.

A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:

   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

   ```
   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. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

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

ONTAP 9 1.9 ou anterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-role` parâmetro.

```
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. Certifique-se de que a política de firewall está ativada para NDMP nos LIFs entre clusters:

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

   O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
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. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

   O seguinte comando ativa a política de firewall para o LIF entre clusters:

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

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:
   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

```
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. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

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

Configure a aplicação de cópia de segurança

Depois que o cluster é configurado para o acesso NDMP, você deve coletar informações da configuração do cluster e, em seguida, configurar o resto do processo de backup no aplicativo de backup.

Passos

1. Reúna as seguintes informações que você configurou anteriormente no ONTAP:
   - O nome de usuário e a senha que o aplicativo de backup requer para criar a conexão NDMP
   - Os endereços IP das LIFs entre clusters que o aplicativo de backup requer para se conetar ao cluster
2. No ONTAP, exiba os aliases atribuídos pelo ONTAP a cada dispositivo usando o `storage tape alias show` comando.

   Os aliases são muitas vezes úteis na configuração do aplicativo de backup.

```
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. No aplicativo de backup, configure o restante do processo de backup usando a documentação do aplicativo de backup.

Depois de terminar

Se ocorrer um evento de mobilidade de dados, como uma movimentação de volume ou migração de LIF, você deve estar preparado para reinicializar quaisquer operações de backup interrompidas.

Informações sobre direitos autorais

Informações sobre marcas comerciais