Configuración de NDMP

ONTAP 9

NetApp
September 12, 2024

Tabla de contenidos

Configuración de NDMP

Información general de la configuración de NDMP

Puede configurar rápidamente un clúster ONTAP 9 para utilizar el protocolo de gestión de datos de red (NDMP) con el fin de realizar backups de los datos directamente en cinta mediante una aplicación de backup de terceros.

Si la aplicación de backup admite Cluster Aware Backup (CAB), puede configurar NDMP como *SVM-scoped* o *node-scoped*:

- Con el ámbito de SVM en el nivel del clúster (SVM de administrador), puede realizar backup de todos los volúmenes alojados en diferentes nodos del clúster. Siempre que sea posible, se recomienda utilizar NDMP con ámbito SVM.
- NDMP de ámbito de nodo le permite realizar backup de todos los volúmenes alojados en ese nodo.

Si la aplicación de backup no admite CAB, debe utilizar NDMP de ámbito de nodo.

El protocolo NDMP de ámbito SVM y el de ámbito de nodo son mutuamente exclusivos; no se pueden configurar en el mismo clúster.

NDMP de ámbito del nodo está obsoleto en ONTAP 9.

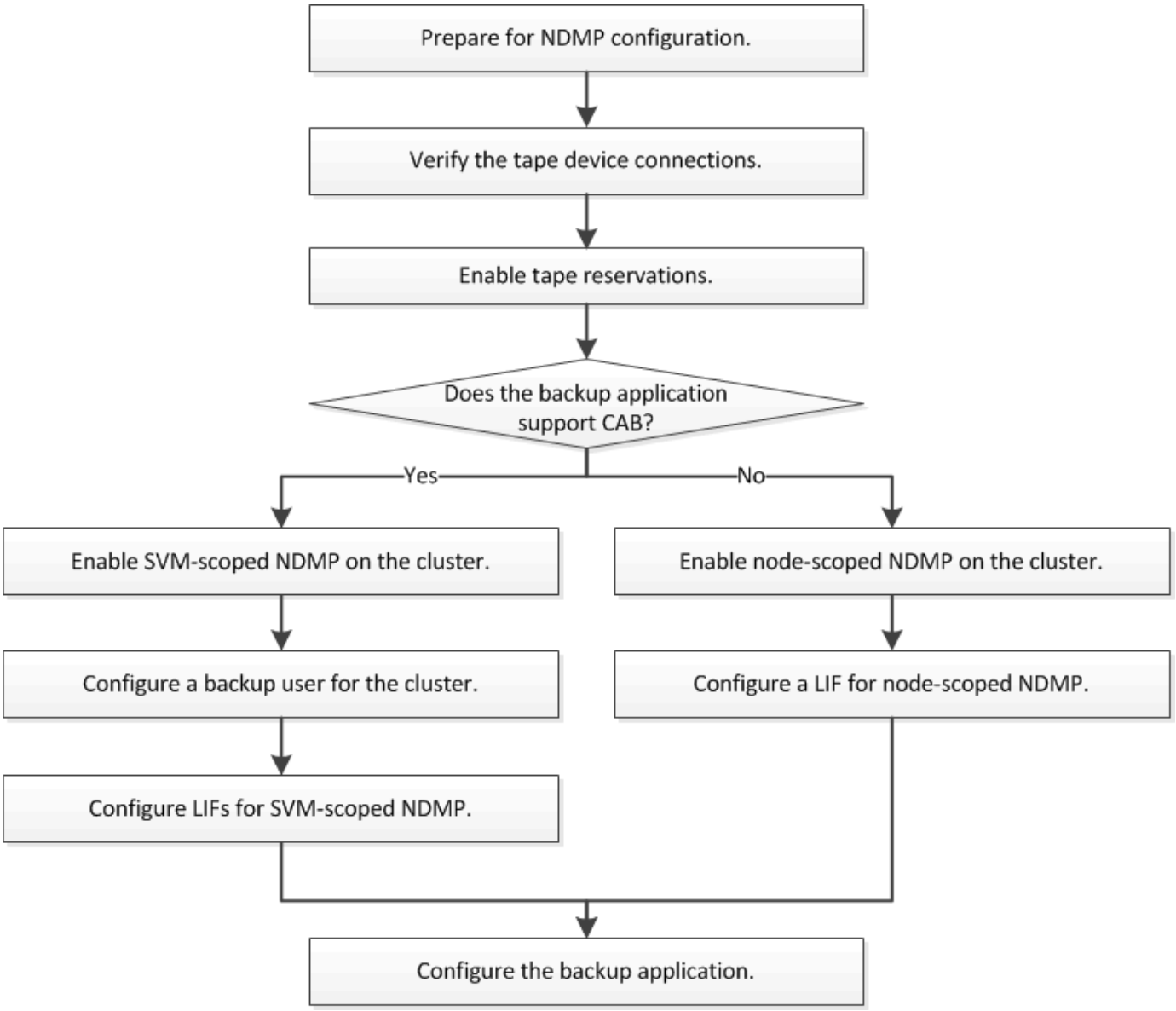
Más información sobre "Respaldo para clúster (CAB)".

Antes de configurar NDMP, compruebe lo siguiente:

- Tiene una aplicación de copia de seguridad de terceros (también llamada aplicación de administración de datos o DMA).
- Es un administrador de clúster.
- Se instalan dispositivos de cinta y un servidor multimedia opcional.
- Los dispositivos de cinta están conectados al clúster a través de un switch Fibre Channel (FC) y no están conectados directamente.
- Al menos un dispositivo de cinta tiene un número de unidad lógica (LUN) de 0.

Flujo de trabajo de configuración de NDMP

La configuración del backup en cinta mediante NDMP implica preparar la configuración NDMP, verificar las conexiones del dispositivo de cinta, habilitar las reservas en cinta, configurar NDMP en el nivel de SVM o nodo, habilitar NDMP en el clúster, configurar un usuario de backup, configurar LIF y configurar la aplicación de backup.



Prepárese para la configuración de NDMP

Antes de configurar el acceso al backup a cinta mediante el protocolo de gestión de datos de red (NDMP), debe comprobar que la configuración planificada es compatible y comprobar que las unidades de cinta aparecen como unidades adecuadas en cada nodo, verificar que todos los nodos tienen LIF de interconexión de clústeres. E identifique si la aplicación de backup es compatible con la extensión Cluster Aware Backup (CAB).

Pasos

1. Consulte la matriz de compatibilidad del proveedor de aplicaciones de backup para obtener información sobre la compatibilidad con ONTAP (NetApp no reúne los requisitos de aplicaciones de backup de terceros con ONTAP o NDMP).

   Debe verificar que los siguientes componentes de NetApp sean compatibles:

   - La versión de ONTAP 9 que se ejecuta en el clúster.

- El proveedor de aplicaciones de backup y la versión: Por ejemplo, Veritas NetBackup 8.2 o CommVault.
- Los detalles de los dispositivos de cinta, como el fabricante, el modelo y la interfaz de las unidades de cinta: Por ejemplo, IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Las plataformas de los nodos del clúster: Por ejemplo, FAS8700 o A400.

> Puede encontrar matrices de compatibilidad con ONTAP heredadas para aplicaciones de backup en la "Herramienta de matriz de interoperabilidad de NetApp".

2. Compruebe que las unidades de cinta aparecen como unidades cualificadas en el archivo de configuración de cinta incorporado de cada nodo:

   a. En la interfaz de línea de comandos, consulte el archivo de configuración de cinta incorporado mediante la `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 las unidades de cinta con la lista de unidades cualificadas de la salida.

> Los nombres de los dispositivos de cinta de la salida pueden variar ligeramente con respecto a los nombres de la etiqueta del dispositivo o de la matriz de interoperabilidad. Por ejemplo, Digital DLT2000 también se conoce como DLT2k. Puede ignorar estas pequeñas diferencias de nomenclatura.

   c. Si un dispositivo no aparece como cualificado en el resultado a pesar de que el dispositivo está cualificado según la matriz de interoperabilidad, descargue e instale un archivo de configuración actualizado para el dispositivo con las instrucciones en el sitio de soporte de NetApp.

      "Descargas de NetApp: Archivos de configuración de dispositivo de cinta"

   Es posible que un dispositivo cualificado no aparezca en el archivo de configuración de cinta integrado si el dispositivo de cinta fue cualificado después de enviar el nodo.

3. Compruebe que todos los nodos del clúster tienen una LIF de interconexión de clústeres:

   a. Consulte las LIF de interconexión de clústeres de los nodos mediante el `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. Si no hay ninguna LIF de interconexión de clústeres en ningún nodo, cree una LIF de interconexión de clústeres mediante la `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
```

"Gestión de redes"

4. Identifique si la aplicación de backup es compatible con Cluster Aware Backup (CAB) mediante la documentación proporcionada con la aplicación de backup.

   El soporte CAB es un factor clave a la hora de determinar el tipo de backup que se puede realizar.

Compruebe las conexiones del dispositivo de cinta

Debe asegurarse de que todas las unidades e intercambiadores de medios sean visibles en ONTAP como dispositivos.

Pasos

1. Ver información acerca de todas las unidades e intercambiadores de medios utilizando `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. Si no se muestra una unidad de cinta, solucione el problema.
3. Si no se muestra un cambiador de materiales, consulte la información sobre los intercambiadores de material utilizando `storage tape show-media-changer` y, a continuación, solucione el 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
...
```

Activar reservas de cinta

Debe asegurarse de que las unidades de cinta estén reservadas para que las aplicaciones de backup las operaciones de backup de NDMP.

Acerca de esta tarea

La configuración de las reservas varía en diferentes aplicaciones de backup, y esta configuración debe coincidir con la aplicación de backup y los nodos o servidores que utilizan las mismas unidades. Consulte la documentación del proveedor de la aplicación de backup para obtener los ajustes de reserva correctos.

Pasos

1. Habilite las reservas mediante el `options -option-name tape.reservations -option-value persistent` comando.

   El siguiente comando habilita las reservas con `persistent` valor:

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

2. Compruebe que las reservas estén habilitadas en todos los nodos mediante el `options tape.reservations` y, a continuación, revise el resultado.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                persistent

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

Configure NDMP con ámbito SVM

Habilite NDMP con ámbito de SVM en el clúster

Si el DMA admite la extensión Cluster Aware Backup (CAB), puede realizar un backup de todos los volúmenes alojados en diferentes nodos de un clúster mediante la habilitación de NDMP de ámbito SVM, la habilitación del servicio NDMP en el clúster (SVM de administrador) y la configuración de LIF para la conexión de datos y control.

Lo que necesitará

La extensión DE LA CABINA debe ser compatible con el DMA.

Acerca de esta tarea

Al desactivar el modo de NDMP con ámbito del nodo, es posible habilitar el modo NDMP con ámbito SVM en el clúster.

Pasos

1. Habilitar modo NDMP en ámbito de SVM:

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

   El modo NDMP en el ámbito de SVM está habilitado.

2. Habilite el servicio NDMP en la SVM de administrador:

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

   El tipo de autenticación se establece en `challenge` de forma predeterminada, la autenticación de texto sin formato está deshabilitada.

   > Para una comunicación segura, debe mantener la autenticación de texto sin formato deshabilitada.

3. Compruebe que el servicio NDMP está activado:

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

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

Habilitar un usuario de backup para la autenticación NDMP

Para autenticar NDMP de ámbito SVM desde la aplicación de backup, debe haber un usuario administrativo con suficientes privilegios y una contraseña NDMP.

Acerca de esta tarea

Debe generar una contraseña de NDMP para los usuarios administradores de backup. Puede habilitar los usuarios administradores de backup en el nivel del clúster o la SVM; si fuera necesario, puede crear un usuario nuevo. De forma predeterminada, los usuarios con los siguientes roles pueden autenticar para el backup NDMP:

- En todo el clúster: `admin` o. `backup`
- SVM individuales: `vsadmin` o. `vsadmin-backup`

Si utiliza un usuario NIS o LDAP, el usuario debe existir en el servidor correspondiente. No puede utilizar un

usuario de Active Directory.

Pasos

1. Mostrar los usuarios y permisos de administrador actuales:

   ```
   security login show
   ```

2. Si es necesario, cree un nuevo usuario de backup NDMP con el `security login create` Y el rol apropiado para privilegios de SVM individuales o en todo el clúster.

   Puede especificar un nombre de usuario de backup local o un nombre de usuario NIS o LDAP para el `-user-or-group-name` parámetro.

   El siguiente comando crea el usuario de backup `backup_admin1` con la `backup` rol para todo el clúster:

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

   El siguiente comando crea el usuario de backup `vsbackup_admin1` con la `vsadmin-backup` Rol para una SVM individual:

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

   Introduzca una contraseña para el nuevo usuario y confirme.

3. Genere una contraseña para la SVM de administrador con el `vserver services ndmp generate password` comando.

   La contraseña generada debe utilizarse para autenticar la conexión NDMP por parte de la aplicación de copia de seguridad.

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

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

Configure las LIF

Debe identificar las LIF que se usarán para establecer una conexión de datos entre los recursos de cinta y los de datos, y para controlar la conexión entre la SVM de administrador y la aplicación de backup. Tras identificar las LIF, debe verificar que las políticas de conmutación por error y firewall están establecidas para las LIF y especificar el rol de interfaz preferido.

A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Pasos

1. Identifique los LIF de interconexión de clústeres, gestión de clústeres y gestión de nodos mediante el `network interface show` con el `-role` parámetro.

   El siguiente comando muestra las LIF de interconexión de clústeres:

```
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
```

   El siguiente comando muestra la LIF de gestión del clúster:

```
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
```

   El siguiente comando muestra las LIF de gestión de nodos:

```
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. Compruebe que la política de firewall está habilitada para NDMP en las LIF de interconexión de clústeres, gestión de clústeres (gestión de clústeres) y gestión de nodos (gestión de nodos):

   a. Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

      El siguiente comando muestra la política de firewall para la LIF de administración de clústeres:

```
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.
```

      El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
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.
```

El siguiente comando muestra la política de firewall de la LIF de gestión de nodos:

```
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 directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

   El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

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

3. Asegurarse de que la política de conmutación por error esté establecida de forma adecuada para todos los LIF:

a. Compruebe que la política de conmutación por error para la LIF de administración del clúster está establecida en `broadcast-domain-wide`Y la directiva para las LIF de interconexión de clústeres y de gestión de nodos se establece en `local-only` mediante el uso de `network interface show -failover` comando.

   El siguiente comando muestra la política de conmutación por error para las LIF de gestión de clústeres, interconexión de clústeres y nodos:

```
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 las políticas de conmutación por error no están definidas de forma adecuada, modifique la política de conmutación por error mediante el `network interface modify` con el `-failover-policy` parámetro.

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

4. Especifique las LIF necesarias para la conexión de datos mediante el `vserver services ndmp modify` con el `preferred-interface-role` parámetro.

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

5. Compruebe que el rol de interfaz preferida esté establecido para el clúster mediante el `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
```

Configure el NDMP de ámbito del nodo

Habilite NDMP de ámbito del nodo en el clúster

Puede realizar backups de volúmenes alojados en un único nodo. Para ello, active el NDMP de ámbito del nodo, lo que habilita el servicio NDMP y configura una LIF para la conexión de datos y control. Esto puede hacerse para todos los nodos del clúster.

NDMP de ámbito del nodo está obsoleto en ONTAP 9.

Acerca de esta tarea

Cuando se utiliza NDMP en el modo de alcance del nodo, la autenticación debe configurarse por nodo. Para obtener más información, consulte "El artículo de la base de conocimientos "Cómo configurar la autenticación NDMP en el modo de alcance de nodo"".

Pasos

1. Habilitar modo NDMP de ámbito de nodo:

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

NDMP node-scope-mode está activado.

2. Habilite el servicio NDMP en todos los nodos del clúster:

   Si utiliza el comodín "'*'", se habilita el servicio NDMP en todos los nodos al mismo tiempo.

   Debe especificar una contraseña para la autenticación de la conexión NDMP mediante la aplicación de backup.

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

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

3. Deshabilite el `-clear-text` Opción de comunicación segura de la contraseña NDMP:

   Usando el comodín "'*" `disables the` `-clear-text` opción en todos los nodos al mismo tiempo.

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

4. Compruebe que el servicio NDMP esté habilitado y el `-clear-text` la opción está desactivada:

```
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.
```

Configure una LIF

Debe identificar una LIF que se utilizará para establecer una conexión de datos y controlar la conexión entre el nodo y la aplicación de backup. Tras identificar la LIF, debe verificar que las políticas de firewall y recuperación tras fallos están establecidas para la LIF.

> A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante el `network interface show` con el `-role` parámetro.

```
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. Compruebe que la política de firewall está activada para NDMP en las LIF de interconexión de clústeres:

   a. Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

      El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
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 directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

      El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

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

3. Asegúrese de que la normativa de recuperación tras fallos esté establecida de forma adecuada para las LIF de interconexión de clústeres:
   a. Compruebe que la política de recuperación tras fallos de las LIF de interconexión de clústeres está establecida en `local-only` mediante el uso de `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. Si la política de conmutación por error no está definida de forma adecuada, modifique la política de conmutación por error mediante el `network interface modify` con el `-failover-policy` parámetro.

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

Configure la aplicación de backup

Una vez que se configura el clúster para el acceso NDMP, debe recopilar información de la configuración del clúster y, a continuación, configurar el resto del proceso de backup en la aplicación de backup.

Pasos

1. Recopile la siguiente información configurada anteriormente en ONTAP:
   - El nombre de usuario y la contraseña que la aplicación de backup necesita para crear la conexión NDMP
   - Las direcciones IP de las LIF de interconexión de clústeres que necesita la aplicación de backup para conectarse al clúster

2. En ONTAP, muestre los alias que ONTAP asignó a cada dispositivo utilizando `storage tape alias show` comando.

   Los alias suelen ser útiles para configurar la aplicación de copia de seguridad.

```
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. En la aplicación de copia de seguridad, configure el resto del proceso de copia de seguridad utilizando la documentación de la aplicación de copia de seguridad.

Después de terminar

Si se produce un evento de movilidad de datos, como un movimiento de volúmenes o una migración LIF, debe estar preparado para reiniciar todas las operaciones de backup interrumpidas.