SVM-bezogenes NDMP konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/ndmp/enable-svm-scoped-ndmp-cluster-task.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

SVM-bezogenes NDMP konfigurieren 1
SVM-bezogenes NDMP auf dem ONTAP Cluster aktivieren 1
Backup-Benutzer für ONTAP NDMP Authentifizierung aktivieren 2
ONTAP LIFs für SVM-bezogenes NDMP konfigurieren 3

SVM-bezogenes NDMP konfigurieren

SVM-bezogenes NDMP auf dem ONTAP Cluster aktivieren

Wenn der DMA die Cluster Aware Backup (CAB) Erweiterung unterstützt, ist das Sichern aller Volumes, die auf verschiedenen Knoten in einem Cluster gehostet werden, möglich, indem SVM-scoped NDMP aktiviert wird, der NDMP-Service auf dem Cluster (admin SVM) aktiviert wird und LIFs für die Daten- und Steuerverbindung konfiguriert werden.

Bevor Sie beginnen

Die CAB-Erweiterung muss vom DMA unterstützt werden.

Über diese Aufgabe

Durch das Deaktivieren des knotenbezogenen NDMP-Modus wird der SVM-bezogene NDMP-Modus auf dem Cluster aktiviert.

Schritte

1. SVM-bezogener NDMP-Modus:

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

   Der SVM-basierte NDMP-Modus ist aktiviert.

2. NDMP-Service auf der Administrator-SVM aktivieren:

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

   Der Authentifizierungstyp ist standardmäßig auf `challenge` gesetzt und die Authentifizierung im Klartext ist deaktiviert.

   ⓘ Für eine sichere Kommunikation sollte die Authentifizierung im Klartext deaktiviert bleiben.

3. Es sollte überprüft werden, ob der NDMP-Service aktiviert ist:

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

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

Backup-Benutzer für ONTAP NDMP Authentifizierung aktivieren

Zur Authentifizierung von SVM-scoped NDMP aus der Backup-Anwendung muss ein Administratorbenutzer mit ausreichenden Berechtigungen und ein NDMP-Passwort vorhanden sein.

Über diese Aufgabe

Sie müssen ein NDMP-Passwort für Backup-Admin-Benutzer generieren. Backup-Admin-Benutzer können auf Cluster- oder SVM-Ebene aktiviert werden, und falls erforderlich, kann ein neuer Benutzer erstellt werden. Standardmäßig können sich Benutzer mit den folgenden Rollen für NDMP-Backup authentifizieren:

- Cluster-weit: `admin` oder `backup`
- Einzelne SVMs: `vsadmin` oder `vsadmin-backup`

Wenn Sie einen NIS- oder LDAP-Benutzer verwenden, muss dieser Benutzer auf dem jeweiligen Server existieren. Ein Active Directory-Benutzer kann nicht verwendet werden.

Schritte

1. Die aktuellen Administratorbenutzer und Berechtigungen werden angezeigt:

   ```
   security login show
   ```

   Weitere Informationen zu `security login show` finden sich in der "ONTAP-Befehlsreferenz".

2. Falls erforderlich kann ein neuer NDMP-Backup-Benutzer mit dem `security login create` Befehl und der passenden Rolle für clusterweite oder individuelle SVM-Berechtigungen erstellt werden.

   Sie können einen lokalen Backup-Benutzernamen oder einen NIS- oder LDAP-Benutzernamen für den `-user-or-group-name` Parameter angeben.

   Der folgende Befehl erstellt den Backup-Benutzer `backup_admin1` mit der `backup` Rolle für den gesamten Cluster:

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

   Der folgende Befehl erstellt den Backup-Benutzer `vsbackup_admin1` mit der `vsadmin-backup` Rolle für eine einzelne SVM:

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

   Geben Sie ein Passwort für den neuen Benutzer ein und bestätigen Sie es.

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

3. Ein Passwort für die Admin-SVM wird mithilfe des `vserver services ndmp generate password` Befehls generiert.

   Das generierte Passwort muss zur Authentifizierung der NDMP-Verbindung durch die Backup-Anwendung

verwendet werden.

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

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

ONTAP LIFs für SVM-bezogenes NDMP konfigurieren

Sie müssen die LIFs identifizieren, die für die Herstellung einer Datenverbindung zwischen den Daten- und Tape-Ressourcen sowie für die Steuerungsverbindung zwischen der Admin-SVM und der Backup-Anwendung verwendet werden. Nach der Identifizierung der LIFs ist zu überprüfen, ob die Service- und Failover-Richtlinien festgelegt sind.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Unterstützten Datenverkehr verwalten".

ONTAP 9.10.1 oder höher

Schritte

1. Die auf den Knoten gehostete Intercluster-LIF wird mit dem `network interface show` Befehl und dem `-service-policy` Parameter identifiziert.

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

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Die auf den Knoten gehostete Management-LIF wird mit dem `network interface show` Befehl und dem `-service-policy` Parameter identifiziert.

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

3. Stellen Sie sicher, dass der Intercluster-LIF den `backup-ndmp-control` Dienst enthält:

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

   Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

4. Stellen Sie sicher, dass die Failover-Richtlinie für alle LIFs entsprechend festgelegt ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Cluster-Management-LIF auf `broadcast-domain-wide` gesetzt ist und die Richtlinie für die Intercluster- sowie Node-Management-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

Der folgende Befehl zeigt die Failover-Richtlinie für die Cluster-Management-, Intercluster- und Node-Management-LIFs an:

```
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. Falls die Failover-Richtlinien nicht ordnungsgemäß eingestellt sind, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

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

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

5. Die für die Datenverbindung erforderlichen LIFs werden mit dem `vserver services ndmp modify` Befehl und dem `preferred-interface-role` Parameter angegeben.

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

6. Es sollte überprüft werden, ob die bevorzugte Schnittstellenrolle für den Cluster mit dem `vserver services ndmp show` Befehl festgelegt ist.

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

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

ONTAP 9.9 oder früher

Schritte

1. Die Intercluster-, Cluster-Management- und Node-Management-LIFs lassen sich mit dem `network interface show` Befehl und dem `-role` Parameter identifizieren.

   Der folgende Befehl zeigt die Intercluster-LIFs an:

```
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
```

   Der folgende Befehl zeigt die Cluster-Management-LIF an:

```
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
```

Der folgende Befehl zeigt die Node-Management-LIFs an:

```
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
```

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Es muss sichergestellt sein, dass die Firewall-Richtlinie für NDMP auf den Intercluster-, Cluster-Management (`cluster-mgmt` und Node-Management (`node-mgmt` LIFs aktiviert ist:

   a. Es sollte überprüft werden, ob die Firewall-Richtlinie für NDMP mit dem `system services firewall policy show` Befehl aktiviert ist.

      Der folgende Befehl zeigt die Firewall-Richtlinie für die Cluster Management LIF an:

```
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.
```

Der folgende Befehl zeigt die Firewall-Richtlinie für die Intercluster LIF an:

```
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.
```

Der folgende Befehl zeigt die Firewall-Richtlinie für die Node Management-LIF an:

```
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. Falls die Firewall-Richtlinie nicht aktiviert ist, kann die Firewall-Richtlinie mit dem `system services firewall policy modify` Befehl mit dem `-service` Parameter aktiviert werden.

Der folgende Befehl aktiviert die Firewall-Richtlinie für die Intercluster-LIF:

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

3. Stellen Sie sicher, dass die Failover-Richtlinie für alle LIFs entsprechend festgelegt ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Cluster-Management-LIF auf `broadcast-domain-wide` gesetzt ist und die Richtlinie für die Intercluster- sowie Node-Management-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

      Der folgende Befehl zeigt die Failover-Richtlinie für die Cluster-Management-, Intercluster- und Node-Management-LIFs an:

```
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. Falls die Failover-Richtlinien nicht ordnungsgemäß eingestellt sind, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

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

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Die für die Datenverbindung erforderlichen LIFs werden mit dem `vserver services ndmp modify` Befehl und dem `preferred-interface-role` Parameter angegeben.

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

5. Es sollte überprüft werden, ob die bevorzugte Schnittstellenrolle für den Cluster mit dem `vserver services ndmp show` Befehl festgelegt ist.

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

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.