



Konfigurieren Sie SVM-Scoped NDMP

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- Konfigurieren Sie SVM-Scoped NDMP 1
 - Aktivieren Sie NDMP mit SVM-Umfang auf dem Cluster 1
 - Aktivieren Sie einen Backup-Benutzer für die NDMP-Authentifizierung 2
 - Konfigurieren Sie LIFs 3

Konfigurieren Sie SVM-Scoped NDMP

Aktivieren Sie NDMP mit SVM-Umfang auf dem Cluster

Wenn der DMA die Erweiterung Cluster-Aware Backup (CAB) unterstützt, können Sie alle Volumes, die auf verschiedenen Nodes in einem Cluster gehostet werden, sichern, indem Sie SVM-Scoped NDMP aktivieren, den NDMP-Service auf dem Cluster aktivieren (admin SVM) und LIFs für die Daten- und Kontrollverbindung konfigurieren.

Was Sie benötigen

Die CAB-Erweiterung muss vom DMA unterstützt werden.

Über diese Aufgabe

Durch die Aktivierung des Node-Scoped NDMP-Modus wird der SVM-Scoped NDMP-Modus auf dem Cluster aktiviert.

Schritte

1. Aktivieren Sie den NDMP-Modus mit SVM-Umfang mithilfe der `system services ndmp` Befehl mit dem `node-scope-mode` Parameter.

```
cluster1::> system services ndmp node-scope-mode off
NDMP node-scope-mode is disabled.
```

2. Aktivieren Sie den NDMP-Service für die SVM-Admin mit `vserver services ndmp on` Befehl.

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

Der Authentifizierungstyp ist auf festgelegt `challenge` Standardmäßig ist die Klartext-Authentifizierung deaktiviert.



Für eine sichere Kommunikation sollten Sie die Klartext-Authentifizierung deaktivieren.

3. Vergewissern Sie sich, dass der NDMP-Dienst mit aktiviert ist `vserver services ndmp show` Befehl.

```
cluster1::> vserver services ndmp show

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

Aktivieren Sie einen Backup-Benutzer für die NDMP-Authentifizierung

Zur Authentifizierung von SVM-Scoped NDMP aus der Backup-Applikation muss ein administrativer Benutzer mit ausreichenden Berechtigungen und einem NDMP-Passwort eingerichtet werden.

Über diese Aufgabe

Sie müssen ein NDMP-Passwort für Backup-Admin-Benutzer generieren. Sie können Backup-Admin-Benutzer auf Cluster- oder SVM-Ebene aktivieren und bei Bedarf einen neuen Benutzer erstellen. Standardmäßig können sich Benutzer mit den folgenden Rollen beim NDMP-Backup authentifizieren:

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

Wenn Sie einen NIS- oder LDAP-Benutzer verwenden, muss der Benutzer auf dem jeweiligen Server vorhanden sein. Sie können keinen Active Directory-Benutzer verwenden.

Schritte

1. Aktuelle Admin-Benutzer und -Berechtigungen anzeigen:

```
security login show
```

2. Erstellen Sie bei Bedarf einen neuen NDMP-Backup-Benutzer mit dem `security login create` Befehl und die entsprechende Rolle für Cluster-weite oder einzelne SVM-Berechtigungen.

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

Mit dem folgenden Befehl wird der Backup-Benutzer erstellt `backup_admin1` Mit dem `backup` Rolle für den gesamten Cluster:

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

Mit dem folgenden Befehl wird der Backup-Benutzer erstellt `vsbackup_admin1` Mit dem `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.

3. Generieren Sie mit ein Passwort für die Admin-SVM `vserver services ndmp generate password` Befehl.

Das generierte Passwort muss verwendet werden, um die NDMP-Verbindung durch die Backup-Anwendung zu authentifizieren.

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

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

Konfigurieren Sie LIFs

Sie müssen die LIFs identifizieren, die für die Einrichtung einer Datenverbindung zwischen den Daten- und Tape-Ressourcen verwendet werden, und für die Kontrollverbindung zwischen der Admin-SVM und der Backup-Applikation. Nachdem Sie die LIFs identifiziert haben, müssen Sie überprüfen, ob Firewall- und Failover-Richtlinien für die LIFs festgelegt wurden, und geben Sie die bevorzugte Schnittstellenrolle an.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Service-Richtlinien ersetzt. Weitere Informationen finden Sie unter ["LIFs und Service-Richtlinien in ONTAP 9.6 und höher"](#).

Schritte

1. Ermitteln Sie mithilfe des die Intercluster-, Cluster-Management- und Node-Management-LIFs `network interface show` Befehl mit dem `-role` Parameter.

Mit dem folgenden Befehl werden die Intercluster-LIFs angezeigt:

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

Current Is	Logical	Status	Network	Current
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			

Mit dem folgenden Befehl wird die Cluster-Management-LIF angezeigt:

```

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

```

Mit dem folgenden Befehl werden die Node-Management-LIFs angezeigt:

```

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. Vergewissern Sie sich, dass die Firewallrichtlinie für NDMP im Intercluster, Cluster-Management (Cluster-Management) und Node-Management-LIFs aktiviert ist:

- a. Überprüfen Sie mithilfe der, ob die Firewallrichtlinie für NDMP aktiviert ist `system services firewall policy show` Befehl.

Mit dem folgenden Befehl wird die Firewallrichtlinie für die Cluster-Management-LIF angezeigt:

```
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.

Mit dem folgenden Befehl wird die Firewallrichtlinie für die Intercluster-LIF angezeigt:

```
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.

Mit dem folgenden Befehl wird die Firewallrichtlinie für die Node-Management-LIF angezeigt:

```
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. Wenn die Firewallrichtlinie nicht aktiviert ist, aktivieren Sie die Firewallrichtlinie unter `system services firewall policy modify` Befehl mit dem `-service` Parameter.

Mit dem folgenden Befehl wird eine Firewall-Richtlinie für die Intercluster LIF aktiviert:

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

3. Vergewissern Sie sich, dass die Failover-Richtlinie für alle LIFs ordnungsgemäß festgelegt ist:

- a. Überprüfen Sie, ob die Failover-Richtlinie für die Cluster-Management-LIF auf festgelegt ist `broadcast-domain-wide` und die Richtlinie für die Schnittstellen zwischen Clustern und Nodes-Management ist auf festgelegt `local-only` Durch Verwendung des `network interface show -failover` Befehl.

Mit dem folgenden Befehl wird die Failover-Richtlinie für die LIFs für das Cluster-Management, die Intercluster und die Node-Management angezeigt:


```

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. Wenn die Failover-Richtlinien nicht entsprechend festgelegt sind, ändern Sie die Failover-Richtlinie mithilfe der `network interface modify` Befehl mit dem `-failover-policy` Parameter.

```

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

```

4. Geben Sie die LIFs an, die mithilfe von für die Datenverbindung erforderlich sind `vserver services ndmp modify` Befehl mit dem `preferred-interface-role` Parameter.

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

5. Vergewissern Sie sich, dass die bevorzugte Schnittstellenrolle für das Cluster mithilfe von festgelegt wird
vserver services ndmp show **Befehl**.

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

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

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.