



NDMP-Konfiguration

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- NDMP-Konfiguration 1
 - NDMP-Konfiguration – Überblick 1
 - NDMP-Konfigurationsworkflow 1
 - Vorbereitung auf die NDMP-Konfiguration 2
 - Überprüfen Sie die Verbindungen des Bandgeräts 4
 - Aktivieren Sie Tape-Reservierungen 6
 - Konfigurieren Sie SVM-Scoped NDMP 7
 - Konfigurieren Sie NDMP mit Node-Umfang 14
 - Konfigurieren der Backup-Applikation 17

NDMP-Konfiguration

NDMP-Konfiguration – Überblick

ONTAP 9-Cluster können mithilfe des Network Data Management Protocol (NDMP) schnell und einfach konfiguriert werden, um Daten mithilfe einer Backup-Applikation eines Drittanbieters direkt auf Tape zu sichern.

Falls die Backup-Applikation Cluster Aware Backup (CAB) unterstützt, können Sie NDMP als *SVM-Scoped* oder *Node-Scoped* konfigurieren:

- Mit dem SVM-Umfang auf Cluster-Ebene (Admin SVM) können Sie alle Volumes sichern, die auf verschiedenen Nodes des Clusters gehostet werden. SVM-Scoped NDMP wird empfohlen, sofern möglich.
- Mit Node-Scoped NDMP können Sie ein Backup aller auf diesem Node gehosteten Volumes erstellen.

Falls die Backup-Anwendung CAB nicht unterstützt, müssen Sie den Node-Scoped NDMP verwenden.

SVM-Scoped und Node-Scoped NDMP schließen sich gegenseitig aus; sie können nicht auf demselben Cluster konfiguriert werden.



Node-Scoped NDMP ist veraltet in ONTAP 9.

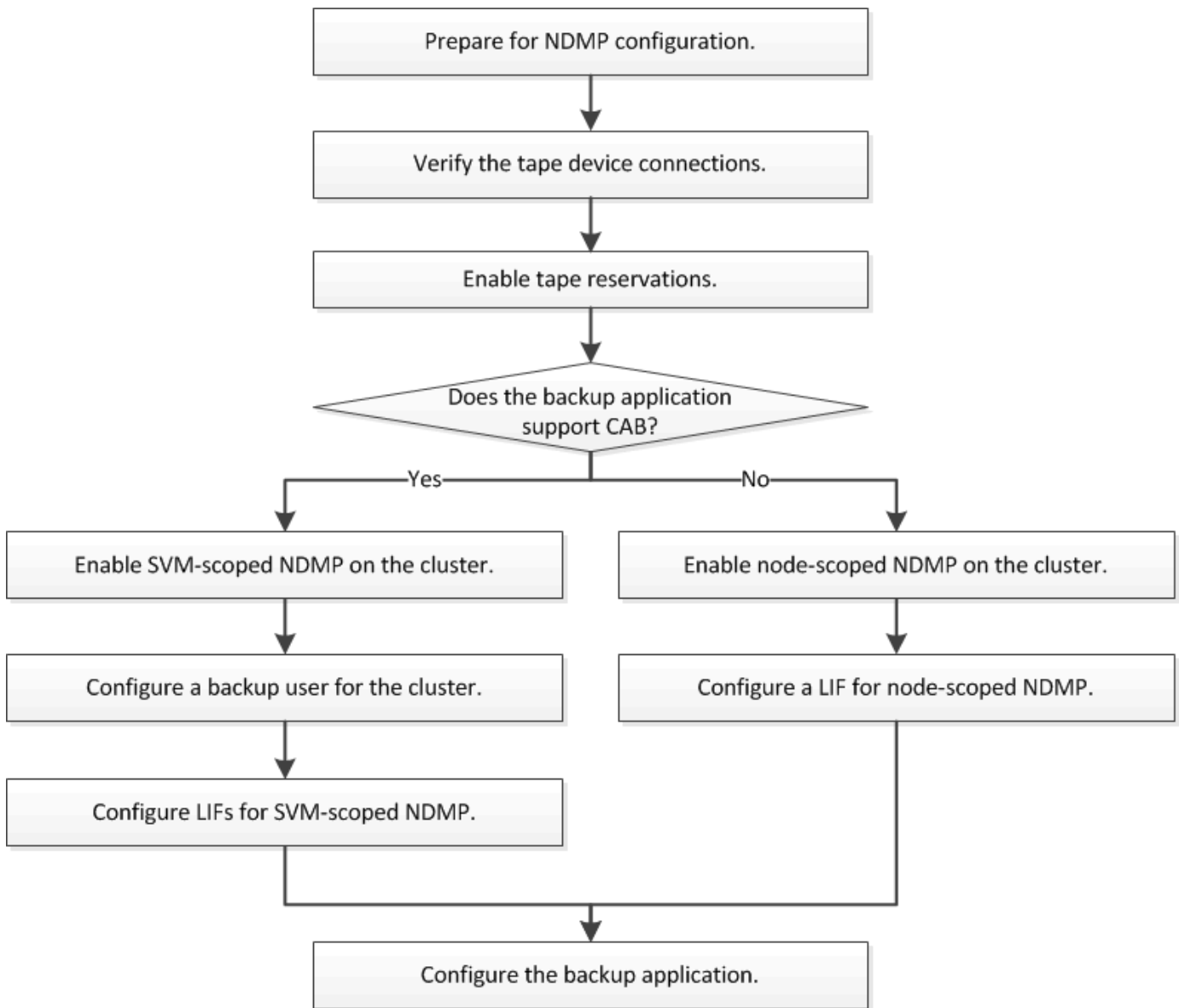
Weitere Informationen zu "[Cluster-sensibles Backup \(CAB\)](#)".

Überprüfen Sie vor dem Konfigurieren von NDMP Folgendes:

- Sie verfügen über eine Backup-Applikation eines Drittanbieters (auch als Datenmanagement-Applikation oder DMA bezeichnet).
- Sie sind ein Cluster-Administrator.
- Bandgeräte und ein optionaler Medienserver sind installiert.
- Tape-Geräte sind über einen FC-Switch (Fibre Channel) mit dem Cluster verbunden und nicht direkt verbunden.
- Mindestens ein Bandgerät verfügt über eine Logical Unit Number (LUN) von 0.

NDMP-Konfigurationsworkflow

Die Einrichtung von Tape Backups über NDMP umfasst die Vorbereitung der NDMP-Konfiguration, die Überprüfung der Verbindungen zwischen Tape-Geräten, Aktivierung von Tape-Reservierungen, Konfiguration von NDMP auf SVM- oder Node-Ebene, Aktivierung von NDMP auf dem Cluster, die Konfiguration eines Backup-Benutzers, die Konfiguration von LIFs sowie die Konfiguration der Backup-Applikation.



Vorbereitung auf die NDMP-Konfiguration

Bevor Sie den Zugriff auf Tape-Backups über das Network Data Management Protocol (NDMP) konfigurieren, müssen Sie überprüfen, ob die geplante Konfiguration unterstützt wird. Vergewissern Sie sich, dass Ihre Bandlaufwerke auf jedem Node als qualifizierte Laufwerke aufgeführt sind. Vergewissern Sie sich, dass alle Nodes über Intercluster LIFs verfügen. Und ermitteln, ob die Backup-Applikation die Cluster-Aware-Backup-Erweiterung (CAB) unterstützt.

Schritte

1. ONTAP-Unterstützung finden Sie in der Kompatibilitätstabelle des Providers Ihrer Backup-Applikation (NetApp ist nicht als Backup-Applikationen anderer Anbieter mit ONTAP oder NDMP qualifiziert).

Sie sollten überprüfen, ob die folgenden NetApp Komponenten kompatibel sind:

- Die Version von ONTAP 9, die auf dem Cluster ausgeführt wird.

- Anbieter und Version der Backup-Applikation, beispielsweise Veritas NetBackup 8.2 oder CommVault.
- Die Bandgeräte enthalten Details wie Hersteller, Modell und Schnittstelle der Bandlaufwerke, z. B. IBM Ultrium 8 oder HPE StoreEver Ultrium 30750 LTO-8.
- Die Plattformen der Nodes im Cluster, z. B. FAS8700 oder A400.



Im finden Sie Legacy-Supportmatrizen zur ONTAP-Kompatibilität für Backup-Anwendungen "[NetApp Interoperabilitäts-Matrix-Tool](#)".

2. Vergewissern Sie sich, dass Ihre Bandlaufwerke in der integrierten Tape-Konfigurationsdatei jedes Node als qualifizierte Laufwerke aufgeführt sind:

- a. Zeigen Sie auf der Befehlszeilenschnittstelle die integrierte Tape-Konfigurationsdatei mithilfe von an `storage tape show-supported-status` Befehl.

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

Node: cluster1-1

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

- b. Vergleichen Sie Ihre Bandlaufwerke mit der Liste der qualifizierten Laufwerke in der Ausgabe.



Die Namen der Bandgeräte in der Ausgabe können geringfügig von den Namen auf dem Geräteetikett oder in der Interoperabilitäts-Matrix abweichen. Beispielsweise kann Digital DLT2000 auch als DLT2K bezeichnet werden. Sie können diese geringfügigen Benennungsunterschiede ignorieren.

- c. Wenn ein Gerät in der Ausgabe nicht als qualifiziert aufgeführt wird, obwohl das Gerät gemäß der Interoperabilitäts-Matrix qualifiziert ist, können Sie eine aktualisierte Konfigurationsdatei für das Gerät herunterladen und mithilfe der Anweisungen auf der NetApp Support Site installieren.

["NetApp Downloads: Konfigurationsdateien für Bandgeräte"](#)

In der integrierten Bandkonfigurationsdatei wird möglicherweise kein qualifiziertes Gerät aufgeführt, wenn das Bandgerät nach dem Versand des Knotens qualifiziert war.

3. Überprüfen Sie, ob jeder Node im Cluster über eine Intercluster-LIF verfügt:

- a. Zeigen Sie die Intercluster-LIFs auf den Nodes mithilfe von an `network interface show -role intercluster` Befehl.

```
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. Wenn auf einem Node keine Intercluster-LIF vorhanden ist, erstellen Sie mithilfe der eine Intercluster-LIF network interface create Befehl.

```
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			

"Netzwerkmanagement"

4. Ermitteln Sie, ob die Backup-Applikation Cluster-Aware Backup (CAB) unterstützt, indem Sie die mit der Backup-Applikation bereitgestellte Dokumentation verwenden.

DIE CAB-Unterstützung ist ein entscheidender Faktor bei der Ermittlung der Art der Datensicherung, die Sie durchführen können.

Überprüfen Sie die Verbindungen des Bandgeräts

Sie müssen sicherstellen, dass alle Laufwerke und Medienwechsler in ONTAP als Geräte

sichtbar sind.

Schritte

1. Zeigen Sie Informationen zu allen Laufwerken und Medienschaltern an, indem Sie die verwenden `storage tape show` Befehl.

```
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. Wenn kein Bandlaufwerk angezeigt wird, beheben Sie das Problem.
3. Wenn kein Medienwechsler angezeigt wird, zeigen Sie Informationen über Medientauscher mithilfe des `storage tape show-media-changer` Befehl und dann Fehlerbehebung.

```
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
```

```
...
```

Aktivieren Sie Tape-Reservierungen

Sie müssen sicherstellen, dass Bandlaufwerke für Backup-Anwendungen für NDMP-Backup-Vorgänge reserviert sind.

Über diese Aufgabe

Die Reservierungseinstellungen variieren in unterschiedlichen Backup-Anwendungen, und diese Einstellungen müssen mit der Backup-Anwendung und den Nodes oder Servern übereinstimmen, die die gleichen Laufwerke verwenden. Die richtigen Reservierungseinstellungen finden Sie in der Anbieterdokumentation der Backup-Anwendung.

Schritte

1. Aktivieren Sie Reservierungen mithilfe des `options -option-name tape.reservations -option -value persistent` Befehl.

Mit dem folgenden Befehl werden Reservierungen mit aktiviert `persistent` Wert:

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

2. Überprüfen Sie mithilfe des, ob Reservierungen auf allen Knoten aktiviert sind `options tape.reservations` Befehl und dann überprüfen Sie die Ausgabe.


```
cluster1::> options tape.reservations

cluster1-1
  tape.reservations          persistent

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

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

          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
```

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
```

Konfigurieren Sie NDMP mit Node-Umfang

Aktivieren Sie NDMP mit Node-Umfang auf dem Cluster

Sie können Backups von Volumes, die auf einem einzelnen Node gehostet werden, durch die Aktivierung von NDMP mit Node-Umfang, die Aktivierung des NDMP-Service und die Konfiguration einer logischen Schnittstelle für die Daten- und Kontrollverbindung erstellen. Dies kann für alle Nodes des Clusters durchgeführt werden.



Node-Scoped NDMP ist veraltet in ONTAP 9.

Über diese Aufgabe

Bei Verwendung von NDMP im Node-Scope-Modus muss die Authentifizierung pro Node konfiguriert werden. Weitere Informationen finden Sie unter "[Der Knowledge Base-Artikel „How to configure NDMP Authentication in the 'Node-scope' Mode'“](#)".

Schritte

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

```
cluster1::> system services ndmp node-scope-mode on
NDMP node-scope-mode is enabled.
```

2. Aktivieren Sie den NDMP-Service auf allen Nodes im Cluster mithilfe von `system services ndmp on` Befehl.

Mit dem Platzhalter „*“ wird der NDMP-Service auf allen Nodes gleichzeitig aktiviert.

Sie müssen ein Passwort für die Authentifizierung der NDMP-Verbindung durch die Backup-Anwendung

angeben.

```
cluster1::> system services ndmp on -node *  
  
Please enter password:  
Confirm password:  
2 entries were modified.
```

3. Deaktivieren Sie das `-clear-text` Möglichkeit zur sicheren Kommunikation des NDMP-Passworts mithilfe der `system services ndmp modify` Befehl.

Verwenden des Platzhalters „*“ disables the `-clear-text` Auf allen Nodes gleichzeitig möglich.

```
cluster1::> system services ndmp modify -node * -clear-text false  
2 entries were modified.
```

4. Vergewissern Sie sich, dass der NDMP-Service aktiviert ist und der `-clear-text` Die Option ist mit der deaktiviert `system services ndmp show` Befehl.

```
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.
```

Konfigurieren Sie ein LIF

Sie müssen ein LIF angeben, das zur Einrichtung einer Datenverbindung und zur Steuerung der Verbindung zwischen dem Node und der Backup-Applikation verwendet wird. Nach der Identifizierung der LIF müssen Sie überprüfen, ob für die LIF Firewall- und Failover-Richtlinien festgelegt sind.



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

Schritte

1. Identifizieren Sie die auf den Nodes gehostete Intercluster-LIF mithilfe des `network interface show` Befehl mit dem `-role` Parameter.

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

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

2. Vergewissern Sie sich, dass die Firewallrichtlinie für NDMP auf den intercluster LIFs aktiviert ist:

- 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 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.

- 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 die Intercluster LIFs ordnungsgemäß festgelegt ist:

- a. Vergewissern Sie sich, dass die Failover-Richtlinie für die Intercluster LIFs auf festgelegt ist `local-only` Durch Verwendung des `network interface show -failover` Befehl.

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

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

Konfigurieren der Backup-Applikation

Nachdem das Cluster für den NDMP-Zugriff konfiguriert ist, müssen Sie Informationen aus der Cluster-Konfiguration erfassen und dann den Rest des Backup-Prozesses in der Backup-Applikation konfigurieren.

Schritte

1. Stellen Sie die folgenden Informationen zusammen, die Sie zuvor in ONTAP konfiguriert haben:
 - Der Benutzername und das Passwort, den die Backup-Anwendung zum Erstellen der NDMP-Verbindung benötigt
 - Die IP-Adressen der Intercluster LIFs, die die Backup-Applikation zur Verbindung mit dem Cluster benötigt
2. Zeigen Sie in ONTAP die Aliase an, die ONTAP jedem Gerät zugewiesen hat, indem Sie das `storage tape alias show` Befehl.

Die Aliase sind oft nützlich bei der Konfiguration der Backup-Anwendung.

```
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. Konfigurieren Sie in der Backup-Applikation den Rest des Backup-Prozesses mithilfe der Dokumentation der Backup-Applikation.

Nachdem Sie fertig sind

Falls ein Ereignis der Datenmobilität eintritt, wie z. B. eine Volume-Verschiebung oder LIF-Migration, müssen Sie bereit sein, alle unterbrochenen Backup-Vorgänge erneut zu initialisieren.

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.