Was muss ich nach meinem Upgrade tun?

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

Was muss ich nach meinem Upgrade tun?

Worauf nach dem Upgrade zu tun ist

Nach dem Upgrade der ONTAP Software sollten Sie verschiedene Aufgaben durchführen, um die Cluster-Bereitschaft zu verifizieren.

Überprüfung des Clusters nach dem Upgrade

Nach dem Upgrade von sollten Sie die Cluster-Version, den Cluster-Zustand und den Storage-Zustand überprüfen.

Bevor Sie beginnen

Bei Nutzung einer MetroCluster FC-Konfiguration müssen Sie auch sicherstellen, dass das Cluster für die automatische ungeplante Umschaltung aktiviert ist.

Überprüfen der Cluster-Version

Nachdem alle HA-Paare aktualisiert wurden, müssen Sie den Versionsbefehl verwenden, um zu überprüfen, ob auf allen Nodes der Zielversion ausgeführt wird.

Die Cluster-Version ist die niedrigste Version von ONTAP, die auf einem beliebigen Node im Cluster ausgeführt wird. Wenn die Cluster-Version nicht die ONTAP-Zielversion ist, können Sie ein Cluster-Upgrade durchführen.

1. Vergewissern Sie sich, dass die Cluster-Version die ONTAP-Zielversion ist:

   ```
   version
   ```

2. Wenn die Cluster-Version nicht die ONTAP-Zielversion ist, können Sie den Upgrade-Status aller Nodes überprüfen:

   ```
   system node upgrade-revert show
   ```

Überprüfen des Cluster-Systemzustands

Nach dem Upgrade eines Clusters sollten Sie überprüfen, ob die Nodes ordnungsgemäß sind und berechtigt sind, am Cluster teilzunehmen, und dass sich das Cluster in einem Quorum befindet.

1. Vergewissern Sie sich, dass die Nodes im Cluster online sind und am Cluster teilnehmen können:

   ```
   cluster show
   ```

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

Wenn ein Knoten fehlerhaft oder nicht geeignet ist, überprüfen Sie die EMS-Protokolle auf Fehler und ergreifen Sie Korrekturmaßnahmen.

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

   Geben Sie „y“ ein, um fortzufahren.

3. Überprüfen Sie die Konfigurationsdetails für jeden RDB-Prozess.

   - Die Epochen der relationalen Datenbank und Datenbank-Epochen sollten für jeden Node übereinstimmen.
   - Der Quorum-Master pro Ring sollte für alle Knoten gleich sein.

     Beachten Sie, dass für jeden Ring möglicherweise ein anderer Quorum-Master vorhanden ist.

So zeigen Sie diesen RDB-Prozess an:	Diesen Befehl eingeben…
Managementapplikation	`cluster ring show -unitname mgmt`
Volume-Standortdatenbank	`cluster ring show -unitname vldb`
Virtual Interface Manager	`cluster ring show -unitname vifmgr`
SAN Management-Daemon	`cluster ring show -unitname bcomd`

   Dieses Beispiel zeigt den Datenbankprozess für den Speicherort des Volumes:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Wenn Sie in einer SAN-Umgebung arbeiten, vergewissern Sie sich, dass sich jeder Knoten in einem SAN-Quorum befindet: `event log show -severity informational -message-name scsiblade.*`

   Die letzte scsiblade-Ereignismeldung für jeden Knoten sollte darauf hinweisen, dass sich das scsi-Blade im Quorum befindet.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- --------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Verwandte Informationen

"Systemadministration"

Vergewissern Sie sich, dass die automatische ungeplante Umschaltung aktiviert ist

Nach einem Cluster-Upgrade sollten Sie überprüfen, ob die automatische ungeplante Umschaltung aktiviert ist.

Über diese Aufgabe

Dieses Verfahren wird nur für MetroCluster FC-Konfigurationen durchgeführt. Wenn Sie eine MetroCluster IP-Konfiguration verwenden, überspringen Sie diesen Vorgang.

Schritte

1. Prüfen, ob die automatische ungeplante Umschaltung aktiviert ist:

   `metrocluster show`

   Wenn die automatische ungeplante Umschaltung aktiviert ist, wird die folgende Anweisung in der Befehlsausgabe angezeigt:

   ```
   AUSO Failure Domain  auso-on-cluster-disaster
   ```

2. Wenn die Anweisung nicht angezeigt wird, aktivieren Sie eine automatische ungeplante Umschaltung:

   `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster`

3. Überprüfen Sie, ob eine automatische ungeplante Umschaltung durch Wiederholung von Schritt 1 aktiviert wurde.

Überprüfung des Storage-Zustands

Nach dem Upgrade eines Clusters sollten Sie den Status Ihrer Festplatten, Aggregate und Volumes überprüfen.

1. Überprüfen des Festplattenstatus:

Um zu prüfen, ob…	Tun Sie das…

Fehlerhafte Festplatten	a. Fehlerhafte Festplatten anzeigen: `storage disk show -state broken` b. Entfernen oder ersetzen Sie alle defekten Festplatten.
Festplatten werden gewartet oder rekonstruiert	a. Anzeigen aller Datenträger in Wartungs-, Ausstehend- oder Rekonstruktionstatus: `storage disk show -state maintenance
pending	reconstructing` .. Warten Sie, bis die Wartung oder Rekonstruktion abgeschlossen ist, bevor Sie fortfahren.

2. Überprüfen Sie, ob alle Aggregate online sind, indem Sie den Status des physischen und logischen Storage anzeigen, einschließlich Storage-Aggregate:

   `storage aggregate show -state !online`

   Mit diesem Befehl werden die Aggregate angezeigt, die *Not* online sind. Alle Aggregate müssen vor und nach einem größeren Upgrade oder einer erneuten Version online sein.

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

3. Überprüfen Sie, ob alle Volumes online sind, indem Sie alle Volumes anzeigen, die *Not* online sind:

   `volume show -state !online`

   Alle Volumes müssen vor und nach einem größeren Upgrade oder einer erneuten Version online sein.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Vergewissern Sie sich, dass es keine inkonsistenten Volumes gibt:

   `volume show -is-inconsistent true`

   Weitere Informationen finden Sie im Knowledge Base-Artikel "Volume zeigt WAFL inkonsistent an" Die Vorgehensweise für inkonsistente Volumes

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Stellen Sie nach dem Upgrade sicher, dass alle LIFS sich auf Home-Ports befinden

Während eines Neubootens wurden möglicherweise einige LIFs zu ihren zugewiesenen Failover-Ports migriert. Nach dem Upgrade eines Clusters müssen Sie alle LIFs aktivieren bzw. zurücksetzen, die sich nicht auf den Home-Ports befinden.

Mit dem Befehl zur Zurücksetzung der Netzwerkschnittstelle wird eine logische Schnittstelle, die sich derzeit nicht auf ihrem Home Port befindet, zurück auf ihren Home Port zurückgesetzt, vorausgesetzt, der Home Port ist funktionsfähig. Der Home Port einer LIF wird angegeben, wenn das LIF erstellt wird. Sie können den Home Port für eine LIF mithilfe des Befehls „Network Interface show“ bestimmen.

1. Zeigt den Status aller LIFs an: `network interface show -fields home-port,curr-port`

   Dieses Beispiel zeigt den Status aller LIFs für eine Storage Virtual Machine (SVM) an.

```
cluster1::> network interface show -fields home-port,curr-port
vserver                          lif       home-port curr-port
-------------------------------- --------- --------- ---------
C1_sti96-vsim-ucs539g_1622463615 clus_mgmt e0d       e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1_inet6 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1_inet6 e0c e0c
Cluster                          sti96-vsim-ucs539g_clus1 e0a e0a
Cluster                          sti96-vsim-ucs539g_clus2 e0b e0b
Cluster                          sti96-vsim-ucs539h_clus1 e0a e0a
Cluster                          sti96-vsim-ucs539h_clus2 e0b e0b
vs0                              sti96-vsim-ucs539g_data1 e0d e0d
vs0                              sti96-vsim-ucs539g_data1_inet6 e0d e0d
vs0                              sti96-vsim-ucs539g_data2 e0e e0e
vs0                              sti96-vsim-ucs539g_data2_inet6 e0e e0e
vs0                              sti96-vsim-ucs539g_data3 e0f e0f
vs0                              sti96-vsim-ucs539g_data3_inet6 e0f e0f
vs0                              sti96-vsim-ucs539g_data4 e0d e0d
vs0                              sti96-vsim-ucs539g_data4_inet6 e0d e0d
vs0                              sti96-vsim-ucs539g_data5 e0e e0e
vs0                              sti96-vsim-ucs539g_data5_inet6 e0e e0e
vs0                              sti96-vsim-ucs539g_data6 e0f e0f
vs0                              sti96-vsim-ucs539g_data6_inet6 e0f e0f
vs0                              sti96-vsim-ucs539h_data1 e0d e0d
vs0                              sti96-vsim-ucs539h_data1_inet6 e0d e0d
vs0                              sti96-vsim-ucs539h_data2 e0e e0e
vs0                              sti96-vsim-ucs539h_data2_inet6 e0e e0e
vs0                              sti96-vsim-ucs539h_data3 e0f e0f
vs0                              sti96-vsim-ucs539h_data3_inet6 e0f e0f
vs0                              sti96-vsim-ucs539h_data4 e0d e0d
vs0                              sti96-vsim-ucs539h_data4_inet6 e0d e0d
vs0                              sti96-vsim-ucs539h_data5 e0e e0e
vs0                              sti96-vsim-ucs539h_data5_inet6 e0e e0e
vs0                              sti96-vsim-ucs539h_data6 e0f e0f
vs0                              sti96-vsim-ucs539h_data6_inet6 e0f e0f
35 entries were displayed.
```

Wenn irgendwelche LIFs mit dem Status-Admin-Status von „down“ oder mit dem ist-Startstatus von „false“ angezeigt werden, fahren Sie mit dem nächsten Schritt fort.

2. Aktivieren der Daten-LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Zurücksetzen von LIFs auf ihre Home Ports: `network interface revert *`

   Mit diesem Befehl werden alle LIFs zurück zu ihren Home-Ports zurückgesetzt.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Vergewissern Sie sich, dass sich alle LIFs in ihren Home-Ports befinden: `network interface show`

   Dieses Beispiel zeigt, dass alle LIFs für SVM vs0 sich auf ihren Home-Ports befinden.

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network         Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask    Node     Port    Home
-------- ---------- ---------- --------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24  node0    e0e     true
         data002    up/up      192.0.2.121/24  node0    e0f     true
         data003    up/up      192.0.2.122/24  node0    e2a     true
         data004    up/up      192.0.2.123/24  node0    e2b     true
         data005    up/up      192.0.2.124/24  node1    e0e     true
         data006    up/up      192.0.2.125/24  node1    e0f     true
         data007    up/up      192.0.2.126/24  node1    e2a     true
         data008    up/up      192.0.2.127/24  node1    e2b     true
8 entries were displayed.
```

Spezielle Konfigurationen überprüfen

Nach dem Upgrade werden Prüfungen für spezielle Konfigurationen durchgeführt

Wenn Ihr Cluster mit einer der folgenden Funktionen konfiguriert ist, müssen Sie nach einem Upgrade möglicherweise weitere Schritte durchführen.

Fragen Sie sich…	Wenn Ihre Antwort ja lautet, dann tun Sie das…
Habe ich ein Upgrade auf ONTAP 9.8 oder höher von ONTAP 9.7 oder früher durchgeführt	Überprüfen Sie die Netzwerkkonfiguration Entfernen Sie den EMS-LIF-Dienst aus den Netzwerkdienstpolices, die dem EMS-Ziel keine Erreichbarkeit bieten
Habe ich eine MetroCluster Konfiguration?	Überprüfen Sie den Netzwerk- und Storage-Status
Habe ich eine SAN-Konfiguration?	Überprüfen Sie Ihre SAN-Konfiguration
Verwende ich NetApp Storage Encryption und habe ein Upgrade auf ONTAP 9.3 oder höher?	Neukonfigurieren der KMIP-Serververbindungen
Gibt es Spiegelungen zur Lastverteilung?	Verschiebung von Quell-Volumes mit verschobenen Load-Sharing-Spiegeln
Verwende ich SnapMirror?	Setzen Sie den SnapMirror Betrieb fort
Habe ich ein Upgrade von ONTAP 8.3 durchgeführt?	Legen Sie die Anzeigeebene für die gewünschten NT ACL-Berechtigungen für NFS-Clients fest
Gibt es Administratorkonten, die vor ONTAP 9.0 erstellt wurden?	Durchsetzen von SHA-2 für Administratorpasswörter
Habe ich Benutzerkonten für den Zugriff auf den Service Processor (SP), der vor ONTAP 9.9 erstellt wurde?	Überprüfen Sie die Änderungen an Konten, die auf den Service Processor zugreifen können

Überprüfen der Netzwerkkonfiguration nach einem Upgrade

ONTAP 9.8 und höher überwacht automatisch die Reachability der Ebene 2. Nach dem Upgrade von ONTAP 9.0x oder früher auf ONTAP 9.8 oder höher sollten Sie überprüfen, ob jeder .Netzwerk-Port seine erwartete Broadcast-Domain wiederverwerten kann.

1. Überprüfen Sie, ob jeder Port seine erwartete Domäne besitzt:`network port reachability show -detail`

   Ein Status der Erreichbarkeit von OK zeigt an, dass der Port über eine Reachability der Ebene 2 zur zugewiesenen Domäne verfügt.

Überprüfen des Netzwerk- und Storage-Status für MetroCluster Konfigurationen

Nachdem Sie in einer MetroCluster Konfiguration ein Update durchgeführt haben, sollten Sie den Status der LIFs, Aggregate und Volumes für jedes Cluster überprüfen.

1. Überprüfen Sie den LIF-Status: `network interface show`

   Im normalen Betrieb müssen LIFs für Quell-SVMs einen Administratorstatus von „up“ aufweisen und sich auf ihren Home-Nodes befinden. LIFs für Ziel-SVMs müssen nicht auf ihren Home-Nodes up-to-located sein. Durch die Umschaltung verfügen alle LIFs über einen Administratorstatus von oben, müssen sich aber nicht auf ihren Home-Nodes befinden.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. Überprüfen Sie den Status der Aggregate: `storage aggregate show -state !online`

   Mit diesem Befehl werden alle Aggregate angezeigt, die *Not* online sind. Im normalen Betrieb müssen alle Aggregate am lokalen Standort online sein. Wenn die MetroCluster-Konfiguration jedoch um den Switch geht, können Root-Aggregate am Disaster-Recovery-Standort offline sein.

   Dieses Beispiel zeigt ein Cluster im normalen Betrieb:

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

   Dieses Beispiel zeigt ein Cluster in Switchover, in dem die Root-Aggregate am Disaster-Recovery-Standort offline sind:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Überprüfen Sie den Status der Volumes: `volume show -state !online`

   Dieser Befehl zeigt alle Volumes an, die *Not* online sind.

   Wenn die MetroCluster-Konfiguration sich im normalen Betrieb befindet (sie befindet sich nicht im Switchover-Status), sollte die Ausgabe alle Volumes anzeigen, die zu den sekundären SVMs des Clusters gehören (diejenigen mit dem SVM-Namen, angehängt mit „-mc“).

   Diese Volumes sind nur bei einem Switchover online verfügbar.

   Dieses Beispiel zeigt einen Cluster im normalen Betrieb, bei dem die Volumes am Disaster-Recovery-Standort nicht online sind.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. Vergewissern Sie sich, dass es keine inkonsistenten Volumes gibt: `volume show -is-inconsistent true`

   Weitere Informationen finden Sie im Knowledge Base-Artikel "Volume zeigt WAFL inkonsistent an" Die Vorgehensweise für inkonsistente Volumes

Überprüfen Sie die SAN-Konfiguration nach einem Upgrade

Wenn Sie in einer SAN-Umgebung Upgrades durchführen, sollten Sie nach dem Upgrade überprüfen, ob jeder Initiator, der mit einem LIF verbunden war, bevor das Upgrade erfolgreich wieder mit der LIF verbunden wurde.

1. Vergewissern Sie sich, dass jeder Initiator mit dem richtigen LIF verbunden ist.

   Sie sollten die Liste der Initiatoren mit der Liste vergleichen, die Sie während der Upgrade-Vorbereitung erstellt haben.

Für…	Eingeben…
ISCSI	`iscsi initiator show -fields igroup,initiator-name,tpgroup`
FC	`fcp initiator show -fields igroup,wwpn,lif`

Neukonfigurieren von KMIP-Serververbindungen nach dem Upgrade auf ONTAP 9.3 oder höher

Nach einem Upgrade auf ONTAP 9.3 oder höher müssen Sie Ihre KMIP-Serververbindungen (External Key Management) neu konfigurieren.

1. Konfiguration der Schlüsselmanager-Konnektivität:`security key-manager setup`
2. Fügen Sie Ihre KMIP-Server hinzu: `security key-manager add -address key_management_server_ip_address`
3. Vergewissern Sie sich, dass KMIP-Server verbunden sind: `security key-manager show -status`
4. Abfrage der Schlüsselserver: `security key-manager query`
5. Neuen Authentifizierungsschlüssel und neue Passphrase erstellen: `security key-manager create-key -prompt-for-key true`

   Die Passphrase muss mindestens 32 Zeichen lang sein.
6. Abfrage des neuen Authentifizierungsschlüssels: `security key-manager query`
7. Weisen Sie Ihren Self-Encrypting Disks (SEDs) den neuen Authentifizierungsschlüssel zu: `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   > Stellen Sie sicher, dass Sie den neuen Authentifizierungsschlüssel aus Ihrer Abfrage verwenden.
8. Weisen Sie den SEDs bei Bedarf einen FIPS-Schlüssel zu: `storage encryption disk modify -disk disk_id -fips-key-id fips_authentication_key_id`

   Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

Verlagern von verschobenen Load-Sharing-Mirror-Quell-Volumes

Nach erfolgreichem Upgrade eines unterbrechungsfreien Upgrades können Sie Quell-Volumes, die die Last gemeinsam nutzen, vor dem Upgrade wieder an die ursprünglichen Speicherorte verschieben.

1. Ermitteln Sie den Speicherort, an den Sie das Load-Sharing-Mirror-Quellvolume verschieben, indem Sie den Datensatz verwenden, den Sie erstellt haben, bevor Sie das Load-Sharing-Spiegelquellvolume verschieben.
2. Verschieben Sie das Quell-Volume der Lastverteilung-Spiegelung zurück an den ursprünglichen Speicherort, indem Sie den Befehl „Start“ der Volume-Verschiebung verwenden.

Wiederaufnahme des SnapMirror Betriebs

Nach Abschluss eines unterbrechungsfreien Upgrades müssen Sie alle unterbrochenen SnapMirror Beziehungen wieder aufnehmen.

Vorhandene SnapMirror Beziehungen müssen mithilfe des Befehls snapmirror Quiesce ausgesetzt worden sein, und der Cluster muss unterbrechungsfrei aktualisiert worden sein.

1. Wiederaufnahme der Transfers für jede SnapMirror Beziehung, die zuvor stillgelegt wurde: `snapmirror resume *`

   Mit diesem Befehl wird der Transfer für alle stillgelegten SnapMirror Beziehungen fortgesetzt.

2. Vergewissern Sie sich, dass die SnapMirror Vorgänge wieder aufgenommen wurden: `snapmirror show`

```
cluster1::> snapmirror show

Source            Destination  Mirror  Relationship  Total
Last
Path        Type  Path         State   Status        Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
cluster1-vs1:dp_src1
            DP   cluster1-vs2:dp_dst1
                              Snapmirrored
                                      Idle           -         true    -
cluster1-vs1:xdp_src1
            XDP  cluster1-vs2:xdp_dst1
                              Snapmirrored
                                      Idle           -         true    -
cluster1://cluster1-vs1/ls_src1
            LS   cluster1://cluster1-vs1/ls_mr1
                              Snapmirrored
                                      Idle           -         true    -
                 cluster1://cluster1-vs1/ls_mr2
                              Snapmirrored
                                      Idle           -         true    -
4 entries were displayed.
```

   Überprüfen Sie für jede SnapMirror-Beziehung, ob der Beziehungsstatus **frei** ist. Wenn der Status **Transfer** lautet, warten Sie, bis die SnapMirror-Übertragung abgeschlossen ist, und geben Sie dann den Befehl erneut ein, um zu überprüfen, ob sich der Status in **Idle** geändert hat.

Für jede SnapMirror Beziehung, die für die Ausführung nach einem Zeitplan konfiguriert ist, sollten Sie überprüfen, ob der erste geplante SnapMirror Transfer erfolgreich abgeschlossen wurde.

Festlegen der Anzeigeebene für die gewünschten NT-ACL-Berechtigungen für NFS-Clients

Nach dem Upgrade von ONTAP 8.3 hat sich die standardmäßige Verarbeitung für die Anzeige von NT ACL-Berechtigungen für NFS-Clients geändert. Sie sollten die

Einstellung überprüfen und bei Bedarf auf die gewünschte Einstellung für Ihre Umgebung ändern. Diese Aufgabe gilt nicht, wenn Sie ein Upgrade von ONTAP 8.3.1 oder höher durchführen.

In Multi-Protokoll-Umgebungen zeigt ONTAP den NFS-Clients die Berechtigungen von NTFS-Dateien und -Verzeichnissen basierend auf dem Zugriff an, den jeder Benutzer durch die NT ACL gewährt hat. In ONTAP 8.3 wird ONTAP standardmäßig für NFS-Clients die Berechtigung basierend auf dem maximalen Zugriff angezeigt, der von der NT-ACL gewährt wurde. Nach der Aktualisierung ändert sich die Standardeinstellung, um Berechtigungen basierend auf dem von der NT-ACL gewährten Mindestzugriff anzuzeigen. Diese Änderung bezieht sich auf neue und vorhandene Storage Virtual Machines (SVMs).

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Überprüfen Sie die Einstellung für die Anzeige von NT ACL-Berechtigungen für NFS-Clients: `vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms`

   Nach dem Upgrade von 8.3 ist der Wert für diesen neuen Parameter deaktiviert, was bedeutet, dass ONTAP die Mindestberechtigungen anzeigt.
3. Wenn Sie die maximalen Berechtigungen anzeigen möchten, ändern Sie die Einstellung nach Bedarf individuell für jede SVM: `vserver nfs modify -vserver vserver_name -ntacl-display -permissive-perms enabled`
4. Vergewissern Sie sich, dass die Änderung wirksam wurde: `vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms`
5. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Durchsetzung von SHA-2 bei Passwörtern des Administratorkontos

Vor ONTAP 9.0 erstellte Administratorkonten verwenden nach dem Upgrade weiterhin MD5-Passwörter, bis die Passwörter manuell geändert werden. MD5 ist weniger sicher als SHA-2. Daher sollten Sie nach dem Upgrade Benutzer von MD5-Konten auffordern, ihre Passwörter zu ändern, um die Standard-SHA-512-Hash-Funktion zu verwenden.

Mit der Passwort-Hash-Funktion können Sie Folgendes tun:

- Zeigt Benutzerkonten an, die mit der angegebenen Hash-Funktion übereinstimmen.
- Verfallen von Konten, die eine angegebene Hash-Funktion verwenden (z. B. MD5), sodass die Benutzer ihre Passwörter bei der nächsten Anmeldung ändern müssen.
- Konten sperren, deren Passwörter die angegebene Hash-Funktion verwenden.
- Wenn Sie auf eine Version vor ONTAP 9 zurücksetzen, setzen Sie das Kennwort des Clusteradministrators zurück, damit es mit der Hash-Funktion (MD5) kompatibel ist, die von der früheren Version unterstützt wird.

ONTAP akzeptiert vorgehackte SHA-2-Passwörter nur mithilfe des NetApp Manageability SDK (Security-Login-create und Security-Login-modify-password).

"Bessere Managebarkeit"

1. Migrieren Sie die MD5-Administratorkonten auf die SHA-512-Passwort-Hash-Funktion:
   a. Alle MD5-Administratorkonten verfallen: `security login expire-password -vserver * -username * -hash-function md5`

Dadurch werden MD5-Kontobenutzer gezwungen, ihre Passwörter bei der nächsten Anmeldung zu ändern.

b. Benutzer von MD5-Konten bitten, sich über eine Konsole oder SSH-Sitzung anzumelden.

Das System erkennt, dass die Konten abgelaufen sind, und fordert Benutzer auf, ihre Passwörter zu ändern. SHA-512 wird standardmäßig für die geänderten Passwörter verwendet.

2. Bei MD5-Konten, deren Benutzer sich nicht anmelden, um ihre Passwörter innerhalb eines bestimmten Zeitraums zu ändern, erzwingen Sie die Kontomigration:

a. Konten sperren, die weiterhin die MD5-Hash-Funktion verwenden (erweiterte Berechtigungsebene): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

Nach der von -Lock-after angegebenen Anzahl von Tagen können Benutzer nicht auf ihre MD5-Konten zugreifen.

b. Entsperren Sie die Konten, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver vserver_name -username user_name`

c. Benutzer müssen sich über eine Konsole oder SSH-Sitzung bei ihren Konten anmelden und ihre Passwörter ändern, wenn das System sie dazu auffordert.

Ändern von Benutzerkonten, die auf den Service Processor zugreifen können

Wenn Sie Benutzerkonten in ONTAP 9.8 und älteren Versionen erstellt haben, die ohne Administratorrolle auf den Service-Prozessor (SP) zugreifen und auf ONTAP 9.9.1 oder höher aktualisieren, erhalten Sie im keinen Administratorwert `-role` Parameter wurde in geändert `admin`.

Weitere Informationen finden Sie unter "Konten, die auf den SP zugreifen können".

Entfernen Sie den LIF-Dienst aus den Netzwerkdienstrichtlinien

Wenn Sie EMS-Nachrichten (Event Management System) eingerichtet haben, bevor Sie ein Upgrade von ONTAP 9.7 oder früher auf ONTAP 9.8 oder höher nach dem Upgrade durchführen, werden Ihre EMS-Nachrichten möglicherweise nicht zugestellt.

Während des Upgrades wird Management-ems, der der EMS-LIF-Dienst, zu allen bestehenden Service-Richtlinien hinzugefügt. Dadurch können EMS-Nachrichten von einem der LIFs gesendet werden, die mit einer der Service-Richtlinien verknüpft sind. Wenn das ausgewählte LIF nicht auf das Ziel der Ereignisbenachrichtigung zugreifen kann, wird die Meldung nicht ausgegeben.

Um dies zu verhindern, sollten Sie nach dem Upgrade den EMS-LIF-Dienst aus den Netzwerkdienstpolices entfernen, die keine Erreichbarkeit des Ziels bieten.

Schritte

1. Identifizieren Sie die LIFs und zugehörigen Netzwerk-Service-Richtlinien, über die EMS-Meldungen gesendet werden können:

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------ ------------------
cluster-1      cluster_mgmt
                                    default-management
cluster-1      node1-mgmt
                                    default-management
cluster-1      node2-mgmt
                                    default-management
cluster-1      inter_cluster
                                    default-intercluster
4 entries were displayed.
```

2. Überprüfen Sie jede LIF auf Verbindung zum EMS-Ziel:

   `network ping -lif lif_name -vserver svm_name -destination destination_address`

   Führen Sie dies auf jedem Knoten aus.

   Beispiele

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Geben Sie die erweiterte Berechtigungsebene ein:

   `set advanced`

4. Entfernen Sie für die LIFs, die nicht über diese verfügen, den Management-ems LIF-Service aus den entsprechenden Service-Richtlinien:

   `network interface service-policy remove-service -vserver svm_name -policy service_policy_name -service management-ems`

5. Überprüfen Sie, dass die Management-ems LIF jetzt nur mit den LIFs verknüpft ist, die die Erreichbarkeit des EMS-Ziels bieten:

   `network interface show -fields service-policy -services management-ems`

Verwandte Links

"LIFs und Service-Richtlinien in ONTAP 9.6 und höher"

Wenn Sie das Disk Qualification Package aktualisieren müssen

Das Disk Qualification Package (DQP) bietet vollständige Unterstützung für neu qualifizierte Laufwerke.

ONTAP behandelt Festplatten anders als normalerweise erwartet, beispielsweise weist ONTAP unterschiedliche Sektorgrößen zu als die vom Hersteller angegebenen. Das DQP enthält die richtigen Parameter für ONTAP für alle neu qualifizierten Laufwerke. Wenn Sie daher eine ONTAP-Version mit einem DQP verwenden, das keine Informationen für ein neu qualifiziertes Laufwerk enthält, verfügt ONTAP nicht über die Informationen, die für die ordnungsgemäße Konfiguration des Laufwerks erforderlich sind.

Sie müssen das DQP in den folgenden Situationen herunterladen und installieren. Eine Best Practice besteht darin, auch das DQP regelmäßig zu aktualisieren, z. B. jedes Quartal oder halbjährlich.

- Jedes Mal, wenn Sie ein Upgrade auf eine neue Version von ONTAP durchführen.

  Das DQP wird im Rahmen eines ONTAP-Upgrades nicht aktualisiert.

- Immer wenn Sie dem Node einen neuen Laufwerkstyp oder eine neue Größe hinzufügen

  Wenn Sie beispielsweise bereits über 1-TB-Laufwerke verfügen und 2-TB-Laufwerke hinzufügen, müssen Sie nach dem aktuellen DQP-Update suchen.

- Jedes Mal, wenn Sie die Festplatten-Firmware aktualisieren
- Immer wenn neuere Festplatten-Firmware oder DQP-Dateien verfügbar sind

Verwandte Informationen

"NetApp Downloads: Disk Qualification Package"

"NetApp Downloads: Festplatten-Firmware"