Phase 6: Schließen Sie das Upgrade ab

Upgrade controllers

NetApp
July 05, 2024

Inhalt

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

MetroCluster FC-Konfiguration

In einer MetroCluster FC-Konfiguration müssen die Knoten für Disaster Recovery/Failover-Standort so schnell wie möglich ersetzt werden. Nicht übereinstimmende Controller-Modelle in einem MetroCluster wird nicht unterstützt, weil eine falsche Übereinstimmung des Controller-Modells dazu führen kann, dass Disaster Recovery-Spiegelung offline geht. Umgehen Sie MetroCluster-Überprüfungen mit dem `-skip -metrocluster-check true` Befehl, wenn Sie Nodes am zweiten Standort ersetzen.

Authentifizierungsmanagement mit KMIP-Servern

Mit ONTAP 9.8 oder höher können KMIP-Server (Key Management Interoperability Protocol) Authentifizierungsschlüssel managen.

Schritte

1. Hinzufügen eines neuen Controllers:

   ```
   security key-manager external enable
   ```

2. Fügen Sie den Schlüsselmanager hinzu:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

   ```
   security key-manager external show-status
   ```

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um das korrekte Setup zu bestätigen, müssen Sie das HA-Paar aktivieren. Sie müssen außerdem überprüfen, dass Node3 und node4 auf den Storage der jeweils anderen Person zugreifen können und dass keine der logischen Datenschnittstellen zu anderen Nodes im Cluster vorhanden sind. Darüber hinaus müssen Sie bestätigen, dass Node3 zu Aggregaten node1 gehört und dass node4 die Aggregate von node2 besitzt und dass die Volumes für beide Nodes online sind.

Schritte

1. Nach den Tests nach der Prüfung von „node2“ werden das Storage Failover und das Cluster HA-Paar für den node2 Cluster aktiviert. Nach Abschluss des Vorgangs werden beide Nodes als abgeschlossen angezeigt, und das System führt einige Bereinigungsvorgänge aus.
2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   ```
   storage failover show
   ```

   Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

   ```
   cluster::> storage failover show
                      Takeover
   Node     Partner  Possible   State Description
   -------- -----    -------    ------------------
   node3    node4    true       Connected to node4
   node4    node3    true       Connected to node3
   ```

3. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

   ```
   cluster show
   ```

4. Stellen Sie sicher, dass node3 und node4 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

   ```
   storage failover show -fields local-missing-disks, partner-missing-disks
   ```

5. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn keine der Knoten „Node3“ oder „node4“ Daten-LIFs besitzt, die sich im Besitz anderer Nodes im Cluster befinden, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

   ```
   network interface revert
   ```

6. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

```
storage aggregate show -owner-name node3

storage aggregate show -owner-name node4
```

7. Legen Sie fest, ob Volumes offline sind:

```
volume show -node node3 -state offline

volume show -node node4 -state offline
```

8. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie im Abschnitt erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor", Und Online-Laufwerk eines der Offline-Volumes, nach Bedarf, durch Verwendung des folgenden Befehls, einmal für jedes Volume:

```
volume online -vserver vserver_name -volume volume_name
```

9. Installieren Sie neue Lizenzen für die neuen Nodes mithilfe des folgenden Befehls für jeden Node:

```
system license add -license-code license_code,license_code,license_code…
```

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

10. Entfernen Sie alle alten Lizenzen mithilfe eines der folgenden Befehle von den ursprünglichen Nodes:

```
system license clean-up -unused -expired

system license delete -serial-number node_serial_number -package
licensable_package
```

   - Alle abgelaufenen Lizenzen löschen:

     ```
     system license clean-up -expired
     ```

   - Alle nicht verwendeten Lizenzen löschen:

     ```
     system license clean-up -unused
     ```

   - Löschen Sie eine bestimmte Lizenz von einem Cluster mit den folgenden Befehlen auf den Nodes:

     ```
     system license delete -serial-number node1_serial_number -package *

     system license delete -serial-number node2_serial_number -package *
     ```

   Die folgende Ausgabe wird angezeigt:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

Eingabe `y` Um alle Pakete zu entfernen.

11. Überprüfen Sie, ob die Lizenzen korrekt installiert sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

    ```
    system license show
    ```

    Sie können die Ausgabe mit der im Abschnitt erfassten Ausgabe vergleichen "Bereiten Sie die Knoten für ein Upgrade vor".

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie die eingestellt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel in "installieren und booten sie node4, Schritt 27"), Sie müssen die Einstellung der Variable aufheben:

    ```
    set diag; systemshell -node node_name -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. Konfigurieren Sie die SPs mit dem folgenden Befehl auf beiden Knoten:

    ```
    system service-processor network modify -node node_name
    ```

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen *ONTAP 9.8: Manual Page Reference* für detaillierte Informationen zum System `service-processor network modify` Befehl.

14. Informationen zum Einrichten eines Clusters ohne Switches auf den neuen Nodes finden Sie unter "Quellen" Um eine Verbindung zur NetApp Support Site_ zu erhalten, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node3 und node4 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

    ```
    security key-manager external show-status
    ```

```
security key-manager onboard show-backup
```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.
   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.
   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager external show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.
4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Onboard Key Manager

Konfigurieren Sie NVE oder NAE mit dem Onboard Key Manager.

Schritte

1. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager onboard sync
   ```

Externes Verschlüsselungsmanagement

Konfigurieren Sie NVE oder NAE mit externem Verschlüsselungsmanagement.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager key query -node node
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      security key-manager external add-servers -key-servers *key_management_server_ip_address*

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager external show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore
   ```

   Für diesen Befehl ist die OKM-Passphrase erforderlich

Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder EKM-Server nicht erreicht werden konnten. Stellen Sie diese Volumes mithilfe der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.

5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```

2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```