第 6 阶段。完成升级

Upgrade controllers

NetApp
July 05, 2024

目录

第 6 阶段。完成升级

第6阶段概述

在第6阶段、您需要确认新节点设置正确、如果新节点启用了加密、则需要配置和设置存储加密或NetApp卷加密。您还应停用旧节点并恢复SnapMirror操作。

步骤

1. "使用 KMIP 服务器管理身份验证"
2. "确认新控制器设置正确"
3. "在新控制器模块上设置存储加密"
4. "在新控制器模块上设置NetApp卷或聚合加密"
5. "停用旧系统"
6. "恢复 SnapMirror 操作"

使用 KMIP 服务器管理身份验证

您可以使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）服务器管理身份验证密钥。

步骤

1. 添加新控制器：

   s安全密钥管理器外部启用

2. 添加密钥管理器：

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

3. 验证密钥管理服务器是否已配置且可供集群中的所有节点使用：

   s安全密钥管理器外部 `show-status`

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

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

确认新控制器设置正确

要确认设置正确，必须启用 HA 对。此外，还必须验证 node3 和 node4 是否可以访问彼此的存储，并且它们都不拥有属于集群上其他节点的数据 LIF 。此外，您还必须确认 node3 拥有 node1 的聚合， node4 拥有 node2 的聚合，并且两个节点的卷均联机。

步骤

1. 在对 node2 执行后检之后，将为 node2 集群启用存储故障转移和集群 HA 对。操作完成后，两个节点均显示为已完成，系统将执行一些清理操作。
2. 验证是否已启用存储故障转移：

   s存储故障转移显示

   以下示例显示了启用存储故障转移时命令的输出：

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

3. 使用以下命令并检查输出，验证 node3 和 node4 是否属于同一集群：

   ```
   cluster show
   ```

4. 使用以下命令并检查输出，验证 node3 和 node4 是否可以访问彼此的存储：

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

5. 使用以下命令并检查输出，验证 node3 和 node4 均不拥有集群中其他节点拥有的主数据 LIF ：

   ```
   network interface show
   ```

   如果 node3 或 node4 都不拥有集群中其他节点拥有的主数据 LIF ，请将数据 LIF 还原到其主所有者：

   网络接口还原

6. 确认 node3 拥有 node1 中的聚合，而 node4 拥有 node2 中的聚合：

   ```
   storage aggregate show -owner-name <node3>
   ```

   ```
   storage aggregate show -owner-name <node4>
   ```

7. 确定是否有任何卷脱机：

   ```
   volume show -node <node3> -state offline
   ```

   ```
   volume show -node <node4> -state offline
   ```

8. 如果任何卷处于脱机状态，请将其与您在部分中捕获的脱机卷列表进行比较 "准备要升级的节点"，并根据需要使用以下命令使每个卷的任何脱机卷联机一次：

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. 对每个节点使用以下命令，为新节点安装新许可证：

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

   license-code 参数接受一个包含 28 个大写字母字符密钥的列表。您可以一次添加一个许可证，也可以一次添加多个许可证，并以逗号分隔每个许可证密钥。

10. 使用以下命令之一从原始节点中删除所有旧许可证：

    ```
    ssystem license clean-up -unused -expired

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

    - 删除所有已过期的许可证：

      ```
      ssystem license clean-up -expired
      ```

    - 删除所有未使用的许可证：

      ```
      ssystem license clean-up -unused
      ```

    - 在节点上使用以下命令从集群中删除特定许可证：

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

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

    此时将显示以下输出：

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

    输入 `y` 删除所有软件包。

11. 使用以下命令并检查输出，以验证是否已正确安装许可证：

    `s`系统许可证显示

    您可以将输出与在部分中捕获的输出进行比较 "准备要升级的节点"。

12. 如果在配置中使用自加密驱动器，并且您已将变量设置 `kmip.init.maxwait` 为 `off` (例如中的 "安装并启动 node4 步骤 24")，则必须取消设置变量：

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

13. 在两个节点上使用以下命令配置 SP：

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

请参见 "参考资料" 链接到 ONTAP s管理参考 _ 以了解 SP 的相关信息，以及 _SP 9.8 命令：手册页参考 _ 以了解有关 system service-processor network modify 命令的详细信息。

14. 如果要在新节点上设置无交换机集群，请参见 "参考资料" 要链接到 *NetApp* 支持站点 _ 并按照 _*switchover to a two-node switchless cluster* 中的说明进行操作。

完成后

如果在 node3 和 node4 上启用了存储加密，请完成此部分 "在新控制器模块上设置存储加密"。否则，请完成部分 "停用旧系统"。

在新控制器模块上设置存储加密

如果更换的控制器或新控制器的 HA 配对项使用存储加密，则必须为新控制器模块配置存储加密，包括安装 SSL 证书和设置密钥管理服务器。

关于此任务

此操作步骤包含对新控制器模块执行的步骤。您必须在正确的节点上输入命令。

步骤

1. 验证密钥管理服务器是否仍可用，其状态及其身份验证密钥信息：

   s安全密钥管理器外部 show-status

   s安全密钥管理器板载 show-backup

2. 将上一步中列出的密钥管理服务器添加到新控制器的密钥管理服务器列表中。

   a. 添加密钥管理服务器：

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

   b. 对列出的每个密钥管理服务器重复上述步骤。您最多可以链接四个密钥管理服务器。

   c. 验证是否已成功添加密钥管理服务器：

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

3. 在新控制器模块上，运行密钥管理设置向导以设置和安装密钥管理服务器。

   您必须安装与现有控制器模块上安装的密钥管理服务器相同的密钥管理服务器。

   a. 在新节点上启动密钥管理服务器设置向导：

      s安全密钥管理器外部启用

   b. 完成向导中的步骤以配置密钥管理服务器。

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

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

在新控制器模块上设置NetApp卷或聚合加密

如果新控制器的已更换控制器或高可用性(HA)配对系统使用NetApp卷加密(NVE)或NetApp聚合加密(NAE)、则必须为NVE或NAE配置新控制器模块。

关于此任务

此操作步骤包含对新控制器模块执行的步骤。您必须在正确的节点上输入命令。

板载密钥管理器

使用板载密钥管理器配置NVE或NAE。

步骤

1. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

   ```
   sSecurity key-manager 板载同步
   ```

外部密钥管理

使用外部密钥管理配置NVE或NAE。

步骤

1. 验证密钥管理服务器是否仍可用，其状态及其身份验证密钥信息：

   ```
   sSecurity key-manager key query -node node
   ```

2. 将上一步中列出的密钥管理服务器添加到新控制器的密钥管理服务器列表中：

   a. 添加密钥管理服务器：

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

   b. 对列出的每个密钥管理服务器重复上述步骤。您最多可以链接四个密钥管理服务器。

   c. 验证是否已成功添加密钥管理服务器：

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

3. 在新控制器模块上，运行密钥管理设置向导以设置和安装密钥管理服务器。

   您必须安装与现有控制器模块上安装的密钥管理服务器相同的密钥管理服务器。

   a. 在新节点上启动密钥管理服务器设置向导：

      s安全密钥管理器外部启用

   b. 完成向导中的步骤以配置密钥管理服务器。

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

   s安全密钥管理器外部还原

   此命令需要OKM密码短语

   有关详细信息、请参见知识库文章 "如何从ONTAP 启动菜单还原外部密钥管理器服务器配置"。

完成后

检查是否有任何卷因身份验证密钥不可用或无法访问 EKM 服务器而脱机。使用 `volume online` 命令将这些卷

恢复联机。

停用旧系统

升级后，您可以通过 NetApp 支持站点停用旧系统。停用系统会告知 NetApp 系统不再运行，并将其从支持数据库中删除。

步骤

1. 请参见 "参考资料" 链接到 _NetApp 支持站点 _ 并登录。
2. 从菜单中选择 * 产品 > 我的产品 * 。
3. 在 * 查看已安装系统 * 页面上，选择要用于显示系统信息的 * 选择条件 * 。

   您可以选择以下选项之一来查找您的系统：

   - 序列号（位于设备背面）
   - " 我的位置 " 的序列号
4. 选择 * 执行！ *

   下表显示了集群信息，包括序列号。
5. 在表中找到集群，然后从产品工具集下拉菜单中选择 * 停用此系统 * 。

恢复 SnapMirror 操作

您可以恢复升级前暂停的 SnapMirror 传输，并恢复 SnapMirror 关系。升级完成后，更新将按计划进行。

步骤

1. 验证目标上的 SnapMirror 状态：

   ```
   snapmirror show
   ```
2. 恢复 SnapMirror 关系：

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