ステージ 7 ：アップグレードを完了します

Upgrade controllers

NetApp
February 22, 2024

目次

ステージ 7 ：アップグレードを完了します

概要

ステージ7では、新しいノードが正しくセットアップされていることを確認し、暗号化が有効な新しいノードがある場合は、ストレージ暗号化またはNetApp Volume Encryptionを設定およびセットアップします。また、古いノードの運用を停止し、SnapMirrorの処理を再開する必要があります。

手順

1. "KMIP サーバを使用して認証を管理します"
2. "新しいコントローラが正しくセットアップされていることを確認します"
3. "新しいコントローラモジュールで Storage Encryption をセットアップします"
4. "新しいコントローラモジュールでNetApp VolumeまたはAggregate Encryptionをセットアップします"
5. "古いシステムの運用を停止"
6. "SnapMirror 処理を再開します"

KMIP サーバを使用して認証を管理します

ONTAP 9.10.1 以降では、 Key Management Interoperability Protocol （ KMIP ）サーバを使用して認証キーを管理できます。

手順

1. 新しいコントローラを追加します。

   「 security key-manager external enable 」と入力します

2. キー管理ツールを追加します。

   「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

3. キー管理サーバが設定され、クラスタ内のすべてのノードで使用できることを確認します。

   「 security key-manager external show-status 」

4. リンクされたすべてのキー管理サーバの認証キーを新しいノードにリストアします。

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

新しいコントローラが正しくセットアップされていることを確認します

セットアップが正しいことを確認するには、HAペアが有効になっていることを確認しま

す。また、ノード1とノード2がお互いのストレージにアクセスできること、およびクラスタの他のノードに属するデータLIFをどちらも所有していないことを確認します。さらに、すべてのデータアグリゲートが正しいホームノードにあること、および両方のノードのボリュームがオンラインであることを確認します。新しいノードの 1 つにユニファイドターゲットアダプタがある場合は、ポート設定をすべてリストアする必要があり、場合によってはアダプタの使用方法の変更が必要になることがあります。

手順

1. node2 のチェック後、 node2 クラスタのストレージフェイルオーバーとクラスタ HA ペアが有効になります。処理が完了すると、両方のノードに「 Completed 」と表示され、クリーンアップ処理が実行されます。
2. ストレージフェイルオーバーが有効になっていることを確認します。

   「 storage failover show 」をクリックします

   次の例は、ストレージフェイルオーバーが有効になっている場合のコマンドの出力例を示しています。

   ```
   cluster::> storage failover show
                                Takeover
   Node        Partner        Possible      State Description
   ----------  -----------    ------------  ------------------
   node1       node2          true          Connected to node2
   node2       node1          true          Connected to node1
   ```

3. 次のコマンドを使用して出力を調べ、 node1 と node2 が同じクラスタに属していることを確認します。

   「 cluster show 」を参照してください

4. 次のコマンドを使用して、 node1 と node2 が相互のストレージにアクセスできることを確認します。

   「 storage failover show -fields local-missing-disks 、 partner-missing-disks 」というメッセージが表示されます

5. 次のコマンドを使用して、 node1 と node2 のどちらもクラスタ内の他のノードがホーム所有するデータ LIF を所有していないことを確認します。

   「 network interface show 」を参照してください

   クラスタ内の他のノードがホーム所有するデータ LIF をノード 1 とノード 2 のどちらも所有していない場合は、データ LIF をホーム所有者にリバートします。

   「 network interface revert 」の略

6. アグリゲートがそれぞれのホームノードで所有されていることを確認します。

   storage aggregate show-owner-name_node1_`

   storage aggregate show-owner-name_node2_`

7. オフラインになっているボリュームがないかを確認します。

   volume show -node node1 __-state offline`

   volume show -node-node2 --状態オフライン

8. オフラインになっているボリュームがある場合は、セクションで取得したオフラインボリュームのリストと比較します "ノードをアップグレードする準備をします"必要に応じて、次のコマンドを使用して、ボリュームごとに 1 回、オフラインボリュームをオンラインにします。

   'volume online -vserver_name_-volume_name_`

9. ノードごとに次のコマンドを使用して、新しいノードの新しいライセンスをインストールします。

   'system license add -license-code_license_code'license_code'license_code…_`

   license-code パラメータには、アルファベットの文字キーをアルファベットの大文字 28 個まで入力できます。ライセンスは一度に 1 つずつ追加することも、複数追加することもできます。各ライセンスキーをカンマで区切って指定することもできます。

10. 次のいずれかのコマンドを使用して、元のノードから古いライセンスをすべて削除します。

    「システムライセンスのクリーンアップ - 未使用 - 期限切れ」

    'system license delete -serial-number_node_name --package_license_package_`

    - 期限切れのライセンスをすべて削除します。

      「システムライセンスのクリーンアップ - 期限切れ」

    - 未使用のライセンスをすべて削除します。

      'System license clean-up-unused （システムライセンスのクリーンアップ - 未使用）'

    - クラスタから特定のライセンスを削除するには、ノードで次のコマンドを使用します。

      'system license delete -serial-number_node1_serial_number_-package *`system license delete -serial-number_node2 serial_number-package *`

    次の出力が表示されます。

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

    すべてのパッケージを削除するには 'y' を入力します

11. 次のコマンドを使用して出力を調べ、ライセンスが正しくインストールされていることを確認します。

    「 system license show 」を参照してください

でキャプチャした出力と比較できます "ノードをアップグレードする準備をします" セクション。

12. 構成で自己暗号化ドライブを使用している場合は、を設定します `kmip.init.maxwait` 変数をに設定します `off` （例：In_Boot node2と交換用システムモジュール_、 "手順 1."）を使用している場合は、次のように変数を設定解除

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

13. 両方のノードで次のコマンドを使用して SP を設定します。

    system service-processor network modify -node _node_name _`

    を参照してください "参考資料" SP および _SP ONTAP 9 コマンドの詳細については ' システム管理リファレンスにリンクするには ' マニュアルページリファレンスを参照してください system の service-processor network modify コマンドの詳細については ' を参照してください

14. 新しいノードにスイッチレスクラスタをセットアップする場合は、を参照してください "参考資料" ネットアップサポートサイトへのリンクを設定するには、 _2 ノードスイッチレスクラスタへの移行の手順に従ってください。

完了後

ノード 1 とノード 2 でストレージ暗号化が有効になっている場合は、セクションを完了します "新しいコントローラモジュールで Storage Encryption をセットアップします"。それ以外の場合は、の項を実行します "古いシステムの運用を停止"。

新しいコントローラモジュールで **Storage Encryption** をセットアップします

交換したコントローラまたは新しいコントローラの HA パートナーで Storage Encryption が使用されている場合は、 SSL 証明書のインストールやキー管理サーバのセットアップなど、新しいコントローラモジュールを Storage Encryption 用に設定する必要があります。

このタスクについて

この手順には、新しいコントローラモジュールで実行する手順が含まれています。コマンドは正しいノードで入力する必要があります。

手順

1. キー管理サーバがまだ使用可能であり、ステータスと認証キー情報が正しいことを確認します。

   「 security key-manager external show-status 」

   「 securitykey manager onboard show-backup 」を参照してください

2. 前の手順で確認したキー管理サーバを、新しいコントローラのキー管理サーバのリストに追加します。

   a. キー管理サーバを追加します。

      「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

b. リストされている各キー管理サーバについて、同じ手順を繰り返します。最大 4 台のキー管理サーバをリンクできます。

c. キー管理サーバが正常に追加されたことを確認します。

「 security key-manager external show 」と入力します

3. 新しいコントローラモジュールで、キー管理セットアップウィザードを実行して、キー管理サーバをセットアップしてインストールします。

既存のコントローラモジュールと同じキー管理サーバをインストールする必要があります。

a. 新しいノードでキー管理サーバセットアップウィザードを起動します。

「 security key-manager external enable 」と入力します

b. ウィザードの手順に従って、キー管理サーバを設定します。

4. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

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

新しいコントローラモジュールで**NetApp Volume**または**Aggregate Encryption**をセットアップします

新しいコントローラの交換したコントローラまたはハイアベイラビリティ（HA）パートナーがNetApp Volume Encryption（NVE）またはNetApp Aggregate Encryption（NAE）を使用している場合は、新しいコントローラモジュールをNVEまたはNAE用に設定する必要があります。

このタスクについて

この手順には、新しいコントローラモジュールで実行する手順が含まれています。コマンドは正しいノードで入力する必要があります。

オンボードキーマネージャ

オンボードキーマネージャを使用してNVEまたはNAEを設定します。

手順

1. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

   「セキュリティキーマネージャオンボード同期」

外部キー管理

外部キー管理を使用してNVEまたはNAEを設定します。

手順

1. キー管理サーバがまだ使用可能であり、ステータスと認証キー情報が正しいことを確認します。

   「 securitykey manager key query -node node 」を参照してください

2. 前の手順で確認したキー管理サーバを新しいコントローラのキー管理サーバリストに追加します。
   a. キー管理サーバを追加します。

      「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

   b. リストされている各キー管理サーバについて、同じ手順を繰り返します。最大 4 台のキー管理サーバをリンクできます。
   c. キー管理サーバが正常に追加されたことを確認します。

      「 security key-manager external show 」と入力します

3. 新しいコントローラモジュールで、キー管理セットアップウィザードを実行して、キー管理サーバをセットアップしてインストールします。

   既存のコントローラモジュールと同じキー管理サーバをインストールする必要があります。

   a. 新しいノードでキー管理サーバセットアップウィザードを起動します。

      「 security key-manager external enable 」と入力します

   b. ウィザードの手順に従って、キー管理サーバを設定します。
4. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

   「セキュリティキーマネージャの外部リストア」

   このコマンドには、OKMのパスフレーズが必要です

   詳細については、技術情報アーティクルを参照してください "ONTAP ブートメニューから外部キー管理サーバの設定をリストアする方法"。

完了後

認証キーを使用できなかったか、 EKM サーバに到達できなかったためにボリュームがオフラインになっていないか確認してください。volume online コマンドを使用して ' これらのボリュームをオンラインに戻します

完了後

認証キーを使用できなかったか、外部キー管理サーバにアクセスできなかったためにボリュームがオフラインになっていないかを確認します。volume online コマンドを使用して ' これらのボリュームをオンラインに戻します

古いシステムの運用を停止

アップグレード後は、ネットアップサポートサイトから古いシステムの運用を停止できます。システムの運用を停止すると、そのシステムは動作していないことがネットアップに通知され、サポートデータベースから削除されます。

手順

1. を参照してください "参考資料" からネットアップサポートサイトにリンクしてログインします。
2. メニューから [製品]>[マイ製品] を選択します。
3. [インストール済みシステムの表示 **]** ページで、システムに関する情報の表示に使用する ***Selection Criteria** を選択します。

   次のいずれかを選択してシステムを検索できます。

   - シリアル番号（ユニットの背面に記載）
   - 所在地のシリアル番号
4. 「 * Go ！ * 」を選択します

   シリアル番号を含むクラスタ情報が表に表示されます。

5. テーブルでクラスタを見つけ、 Product Tool Set （製品ツールセット）ドロップダウンメニューから * Decommission this system * （このシステムのデコミッション）を選択します。

SnapMirror 処理を再開します

アップグレード前に休止していた SnapMirror 転送を再開し、 SnapMirror 関係を再開できます。更新はアップグレードの完了後にスケジュールどおりに実行されます。

手順

1. デスティネーションで SnapMirror のステータスを確認します。

   「 Snapmirror show 」のように表示されます

2. SnapMirror 関係を再開します。

   snapmirror resume -destination–vserver_vserver_name _`