ステージ 6 ：アップグレードを完了します

Upgrade controllers

NetApp
February 22, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-systems-upgrade/upgrade-arl-manual-app/stage_6_index.html on February 22, 2024. Always check docs.netapp.com for the latest.

目次

ステージ 6 ：アップグレードを完了します 1
概要 1
KMIP サーバを使用して認証を管理します 1
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 1
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Aggregte 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 7

ステージ 6 ：アップグレードを完了します

概要

ステージ6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。

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 9.5 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 setup -node *new_controller_name*`

2. キー管理ツールを追加します。

   「security key-manager -add_key_manager_server_ip_address_`」

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。

   「 securitykey-manager 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 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ペアを有効にします。また、ノード3とノード4が相互に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、ノード3がノード1の

アグリゲートを所有し、ノード4がノード2のアグリゲートを所有していること、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。

手順

1. いずれかのノードで次のコマンドを入力して、ストレージフェイルオーバーを有効にします。

   storage failover modify -enabled true -node *node3*`

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
   -------------- -------------- -------- -------------------
   node3          node4          true     Connected to node4
   node4          node3          true     Connected to node3
   ```

3. 次のいずれかを実行します。

クラスタの種類	説明
2 ノードクラスタ	どちらかのノードで cluster ha modify -configured true コマンドを入力して ' クラスタの高可用性を有効にします
3 ノード以上のクラスタ	に進みます 手順 4。

4. 次のコマンドを入力して、 node3 と node4 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

5. 次のコマンドを入力し、出力を調べて、 node3 と node4 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

6. 次のコマンドを入力し、出力を調べて、 node3 と node4 がクラスタ内の他のノードによってホーム所有されているデータ 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

   node3 または node4 に、クラスタ内の他のノードがホーム所有するデータ LIF がある場合は、「 network interface revert 」コマンドを使用して、データ LIF をホーム所有者にリバートします。

7. ノード 3 がノード 1 のアグリゲートを所有していること、およびノード 4 がノード 2 のアグリゲートを所有していることを確認します。

storage aggregate show-owner-name_node3_`storage aggregate show-owner-name_node4 _`

8. 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 _node3 --state offline `volume show -node _node4 --state off`

9. オフラインのボリュームがある場合は、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 "手順 19（ｄ）" で、各ボリュームに対して次のコマンドを 1 回入力して、アップグレードの準備をし、必要に応じてオフラインのボリュームをオンラインにします。

   'volume online -vserver_name_-volume_name_`

10. ノードごとに次のコマンドを入力して、新しいノード用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、ライセンスキーごとにカンマで区切って複数ずつ追加することもできます。

11. 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：で） "手順 16" of _ Install and boot node3 _）では、変数の設定を解除する必要があります。

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

12. 元のノードから古いライセンスをすべて削除するには、次のいずれかのコマンドを入力します。

    system license clean-up-unused -expired `system license delete -serial-number_node_name --package_license_package_package_`

    - 期限切れのライセンスをすべて削除するには、次のように入力します

      「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するには、次のように入力し

      '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入力します。

      '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

13. 次のコマンドを入力し、出力を調べて、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 "手順 30" で、ノードをアップグレードする準備をしています。

14. 両方のノードで次のコマンドを実行して、 SP を設定します。

    system service-processor network modify -node _node_name _`

    に進みます "参考資料" SP の詳細については ' システム管理リファレンスにリンクし '_System ONTAP 9 コマンド：マニュアルページリファレンスにリンクし 'system 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

15. 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、に進みます "参考資料" ネットワークサポートサイトへのリンクをクリックし、 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 3 とノード 4 でストレージ暗号化が有効になっている場合は、の手順を実行します "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、の手順を実行します "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。

    「 securitykey-manager show -status 」

    「セキュリティキーマネージャクエリー」

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 -add_key_manager_server_ip_address_`」

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。

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

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 setup -node *new_controller_name*`

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 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**Aggregte 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）を使用する場合は、NVEまたはNAE用に新しいコントローラモジュールを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。

「 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. 次のコマンドを使用して、キー管理サーバを追加します。

「security key-manager -add_key_manager_server_ip_address_`」

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. 次のコマンドを使用して、キー管理サーバが正常に追加されたことを確認します。

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

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. 次のコマンドを使用して、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 setup -node *new_controller_name*`

   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。

用途	使用するコマンド
外部キー管理ツール	「 securitykey-manager external restore 」このコマンドには、OKM のパスフレーズが必要です
オンボードキーマネージャ（ OKM ）	「セキュリティキーマネージャオンボード同期」

   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、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。を使用して、それらのボリュームをオンラインに戻します `volume online` コマンドを実行します

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 _`

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。