アップグレード後の作業

アップグレードが完了したことの確認

ステップ 1 Cisco UCS Manager にログインして、保留中のサーバ アクティビティが HX ノードに存在しないことを確認します。

[サーバ（Servers）] タブ > 、[サーバ（Servers）] > [保留中のアクティビティ（Pending Activities）] タブで、すべてのサーバ アクティビティを確認してください。

ステップ 2 HX ノードが、期待されるファームウェア バージョンに一致することを確認します。

Cisco UCS Manager で、**[機器（Equipment）] > [ファームウェア管理（Firmware Management）] > [インストールされたファームウェア（Installed Firmware）]** タブを選択し、正しいファームウェア バージョンであることを確認します。

ステップ 3 SSH を介していずれかのコントローラ VM にログインします。

```
# ssh root@controller_vm_ip
```

ステップ 4 HyperFlex Data Platform バージョンを確認します。

```
# stcli cluster version


Cluster version: 2.5(1c)
Node HX02 version: 2.5(1c)
Node HX05 version: 2.5(1c)
Node HX01 version: 2.5(1c)
Node HX03 version: 2.5(1c)
Node HX04 version: 2.5(1c)
```

ステップ 5 HX ストレージ クラスタがオンラインであり、正常な状態であることを確認します。

```
# stcli cluster info|grep -i health

Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

ステップ 6 データストアが稼働中であり、ESXi ホストに適切にマウントされていることを確認します。

HX コントローラ VM から：

```
# stcli datastore list
```

ESXi ホストから：

```
# esxcfg-nas -l
```

ステップ 7 アップグレードが完了し、成功したことを確認します。

```
stcli cluster upgrade-status

Nodes up to date:
[HX-Cluster, HX-Node-1(1.1.1.1), HX-Node-2(1.1.1.2), HX-Node-3(1.1.1.3)]
Cluster upgrade succeeded.
```

クリーナが実行中であるかどうかの確認

アップグレードが失敗した場合

アップグレードが失敗した場合は、クリーナを実行します。たとえアップグレードを続行しない場合でも、この作業は必須です。

クリーナを手動で実行するには、次のコマンドを使用してストレージ クラスタ クリーナを再起動します。

stcli cleaner start [-h] [--id ID | --ip NAME]

構文の説明

Option	必須またはオプション	説明
--id ID	オプション。	ストレージ クラスタ ノードの ID。ID は、`stcli cluster info` コマンドでリストされます。
--ip NAME	オプション。	ストレージクラスタ ノードの IP アドレス。IP は、`stcli cluster info` コマンドでリストされます。

アップグレードが完了した場合

アップグレードが完了した場合は、クリーナが実行中であるかどうかを確認します。指定のノードのストレージ クラスタ クリーナに関する情報を取得するには、次のコマンドを使用します。

stcli cleaner info [-h] [--id ID | --ip NAME]

構文の説明

Option	必須またはオプション	説明
--id ID	オプション。	ストレージ クラスタ ノードの ID。ID は、`stcli cluster info` コマンドでリストされます。
--ip NAME	オプション。	ストレージクラスタ ノードの IP アドレス。IP は、`stcli cluster info` コマンドでリストされます。

スナップショットスケジューラを有効にする（オプション）

アップグレードを開始する前にスナップショットスケジューラを無効にしていた場合は、ここでスケジュールを有効にします。HyperFlex クラスタ IP に SSH で接続し、コマンド *stcli snapshot-schedule –enable* snapshot schedule を実行します。

Enable HyperFlex Software Encryption

HyperFlex ソフトウェア暗号化は、保存データのファイル レベルのエンドツーエンド AES 256 ビット暗号化を提供します。HyperFlex ソフトウェア暗号化の機能を活用して、ドライブ、サーバー、またはクラスタ全体などのデバイスの盗難からデータの機密性を保護できます。暗号化キーは、Intersight SaaS と Intersight 仮想アプライアンスの両方で利用可能な Intersight Key Manager によって安全にリモートに保存されます。

クラスタで HyperFlex ソフトウェア暗号化を有効にするには、HX Data Platform および Intersight のライセンス要件を満たしていることを確認してください。『Cisco HyperFlex Systems Ordering and Licensing Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/b_Cisco_HyperFlex_Systems_Ordering_and_Licensing_Guide.htmlライセンス要件が満たされていることを確認した後、HyperFlex ソフトウェア暗号化を有効にするには、My Cisco Entitlement から暗号化パッケージをダウンロードし、パッケージをインストールしてから、Intersight からの暗号化を有効にする必要があります。詳細については、HyperFlex ソフトウェア暗号化を参照してください。https://intersight.com/help/saas/resources#cisco_intersight_service_mesh_manager