HX ストレージ クラスタの管理

クラスタ アクセス ポリシー レベルの変更

ステップ 1 クラスタ アクセス ポリシーを「strict」（厳格）に変更する前に、ストレージ クラスタが正常な状態になっている必要があります。

ステップ 2 ストレージ クラスタ内のストレージ コントローラ VM のコマンド ラインから、次のコマンドを入力します。

```
# stcli cluster get-cluster-access-policy
```

```
# stcli cluster set-cluster-access-policy --name {strict,lenient}
```

クラスタのリバランス

ストレージ クラスタは定期的なスケジュールで再調整されます。これは、使用可能なストレージの変更すべてに対して保存されているデータの分散を再調整し、ストレージ クラスタの健全性を回復するために使用されます。新しいノードが既存のクラスタに追加される場合、追加されたノードは、既存のクラスタに参加するとすぐに新しい書き込みを実行します。必要に応じ

て (通常は 24 時間以内に) クラスタが自動的に再調整され、ストレージ全体の使用率が低い場合、新しいノードは最初に既存のコンバージドノードよりも少ないストレージ使用率を示すことがあります。現在のストレージ使用率が高く、新しいノードがクラスタに追加されると、データは一定期間にわたって新しいノード ドライブに再調整されます。

（注） 手動の再調整を行うことにより、クラスタ上の通常のユーザー IO との干渉が発生し、遅延が増加する可能性があります。したがって、HyperFlex システムは、パフォーマンスのペナルティを最小限に抑えるために必要な場合にのみ、再調整を開始します。

ストレージ コントローラ VM から再調整ステータスを確認します。

a) コマンド ラインで、次のコマンドを入力します。

```
# stcli rebalance status
rebalanceStatus:
rebalanceState:
cluster_rebalance_ongoing
percentComplete: 10
rebalanceEnabled: True
```

b) コマンド ラインを再入力して、プロセスの完了を確認します。

```
# stcli rebalance status
rebalanceStatus:
rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True
```

この例では再調整が有効で、再調整を実行する準備ができていますが、現在ストレージクラスタを再調整していないことを示します。

クラスタの再調整ステータスと自己修復ステータスの確認

ストレージクラスタのリバランスは定期的に行われ、クラスタ内の利用可能なストレージ量が変化したときにも行われます。さらに、利用可能なストレージ量が変化した場合にも、リバランスがトリガーされます。これは自動自己修復機能です。

重要 再調整は、通常、1 つのディスクの使用率が 50 % を超えた場合またはクラスタの集約ディスク使用率が 50 % 以上の場合にのみ発生します。

HX Data Platform プラグインまたはストレージ コントローラ VM コマンドラインから再調整ステータスを確認できます。

ステップ 1 HX Data Platform プラグインからの再調整ステータスの確認

a) vSphere Web クライアント ナビゲータから、**[vCenter Inventory Lists]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***cluster*** > **[サマリ (Summary)]** の順に選択します。

[状態（Status）] ポートレットには**自己修復ステータス**がリストされます。

b) [復元ステータス] を展開して、[自己修復ステータス] セクションを表示します。[Self healing status] フィールドには、再調整アクティビティまたは N/A（再調整が現在アクティブではない場合）が示されます。

ステップ 2 ストレージ コントローラ VM コマンド ラインから再調整ステータスを確認する。

a) `ssh` を使用してコントローラ VM にログインします。

b) コントローラ VM のコマンド ラインから、次のコマンドを実行します。

```
# stcli rebalance status
```

次の出力は、ストレージ クラスタで再調整が現在実行されていないことを示しています。

```
rebalanceStatus:
percentComplete: 0
rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True
```

HX Data Platform プラグインの [最近のタスク（Recent Tasks）] タブに、ステータス メッセージが表示されます。

スペース不足エラーの処理

システムで [スペース不足（Out of Space）] エラーが表示された場合、ノードを追加して空き容量を増やすか、使用されていない既存の VM を削除して領域を解放できます。

[スペース不足（Out of Space）] の状態の場合、VM は応答しません。

（注） ストレージ コントローラ VM は削除しないでください。ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付いています。

ステップ 1 ノードを追加するには、HX Data Platform インストーラのクラスタ拡張機能を使用します。

ステップ 2 未使用の VM を削除するには、次の手順を実行します。

a) どのゲスト VM が削除可能であるかを判断します。VM や命名規則によって使用されるディスク領域などの要因を考慮できます。

b) **[vCenter]** > **[仮想マシン（Virtual Machines）]** に移動して、インベントリ内の仮想マシンを表示します。

c) 削除する VM をダブルクリックします。

d) **[概要（Summary）]** > **[質問に回答（Answer Questions）]** をクリックしてダイアログボックスを表示します。

e) **[キャンセル（Cancel）]** オプション ボタンをクリックして、**[OK]** をクリックします。
f) VM の電源をオフにします。
g) VM を削除します。

ステップ 3 [スペース不足（Out of Space）] の状態がクリアされた後で、次の操作を行います。

a) **[vCenter]** > **[仮想マシン（Virtual Machines）]** に移動して、インベントリ内の VM を表示します。
b) 使用する VM をダブルクリックします。
c) **[概要（Summary）]** > **[質問に回答（Answer Questions）]** をクリックしてダイアログボックスを表示します。
d) **[再試行（Retry）]** オプション ボタンをクリックして、**[OK]** をクリックします。

クリーナ スケジュールの確認

`stcli cleaner` コマンドは、通常、バックグラウンドで継続的に実行されます。`cleaner` は、必要のないときにはスリープモードになっていて、ポリシーによって定義された条件が満たされるとスリープから復帰します。たとえば、ストレージクラスタで ENOSPC 条件が発生すると、クリーナが自動的に高優先度で実行されます。

`cleaner` の実行中は、クラスタを拡張しないでください。cleaner スケジュールを確認するか、必要に応じてスケジュールを調整します。

ステップ 1 ストレージ クラスタ内の任意のコントローラ VM にログインします。コントローラ VM コマンド ラインから、次にリストするコマンドを実行します。

ステップ 2 クリーナ スケジュールを表示します。

```
# stcli cleaner get-schedule --id ID | --ip NAME
```

パラメータ	説明
`--id ID`	ストレージ クラスタ ノードの ID。
`--ip NAME`	ストレージ クラスタ ノードの IP アドレス。

現在の vCenter サーバから新しい VCenter サーバへのストレージ クラスタの移動

始める前に

- このタスクはメンテナンス時間帯に実行します。

- クラスタが正常であることおよびアップグレードの状態が問題なく正常であることを確認します。コントローラ VM コマンドラインから stcli コマンドを使用して、状態を表示できます。

  ```
  # stcli cluster info
  ```

  応答を確認します。

  ```
  upgradeState: ok
  healthState: healthy
  ```

- vCenter が動作している必要があることを確認します。
- vCenter クラスタ間でストレージ クラスタを移動する場合、スナップショット スケジュールはストレージ クラスタと共に移動されません。

ステップ 1 現在の vCenter から、クラスタを削除します。

これは HX ストレージ クラスタの作成時に指定された vCenter クラスタです。

ステップ 2 新しい vCenter では、同じクラスタ名を使用して新しいクラスタを作成します。

ステップ 3 新しく作成されたクラスタで新しい vCenter に ESX ホストを追加します。

次のタスク

vCenter クラスタからのストレージ クラスタの登録解除 （6 ページ） に進みます。

現在の vCenter サーバから新しい VCenter サーバへのストレージ クラスタの移動

始める前に

- このタスクはメンテナンス時間帯に実行します。
- クラスタが正常であることおよびアップグレードの状態が問題なく正常であることを確認します。コントローラ VM コマンドラインから stcli コマンドを使用して、状態を表示できます。

  ```
  # stcli cluster info
  ```

  応答を確認します。

  ```
  upgradeState: ok
  healthState: healthy
  ```

- vCenter が動作している必要があることを確認します。
- vCenter クラスタ間でストレージ クラスタを移動する場合、スナップショット スケジュールはストレージ クラスタと共に移動されません。

ステップ 1 現在の vCenter から、クラスタを削除します。

これは HX ストレージ クラスタの作成時に指定された vCenter クラスタです。

ステップ 2 新しい vCenter では、同じクラスタ名を使用して新しいクラスタを作成します。

ステップ 3 新しく作成されたクラスタで新しい vCenter に ESX ホストを追加します。

次のタスク

vCenter クラスタからのストレージ クラスタの登録解除 （6 ページ） に進みます。

vCenter クラスタからのストレージ クラスタの登録解除

この手順はオプションであり、必須ではありません。HXデータ プラットフォームプラグインの登録は古い vCenter に残しておくことをお勧めします。

始める前に

vCenter サーバから別の vCenter サーバへストレージ クラスタを移動するタスクの一部として、現在の vCenter サーバから新しい VCenter サーバへのストレージ クラスタの移動 （4 ページ）の手順を完了します。

（注）
- 複数の HX クラスタが同じ vCenter に登録されている場合、すべての HX クラスタが別の vCenter に完全に移行されるまで、この手順を試みないでください。この手順を実行すると、vCenterに登録されている既存の HX クラスタが中断します。

ステップ 1 vSphere クライアントからの HX Data Platform ファイルの削除 （8 ページ）の手順を完了します。

ステップ 2 HX クラスタが vCenter から登録解除されていることの確認 （9 ページ）の手順を完了します。

次のタスク

新しい vCenter クラスタによるストレージ クラスタの登録 （10 ページ） に進みます。

EAM 拡張機能の登録解除および削除

HX Data Platform を部分的にインストールしているかアンインストールしている場合、または、当該の vSphere にインストールされている HX クラスタよりも多くのエージェンシーがある HX クラスタを登録解除している場合、HX Data Platform 拡張機能のための古い ESX Agent Manager（EAM）が残っている場合があります。Managed Object Browser（MOB）拡張マネージャを使用して、古い拡張機能を削除します。

始める前に

- まだダウンロードしていない場合は、vSphere ESX Agent Manager SDK をダウンロードします。
- 複数の HX クラスタが同じ vCenter に登録されている場合、すべての HX クラスタが別の vCenter に完全に移行されるまで、この手順を実行しないでください。この手順を実行すると、vCenter に登録されている既存の HX クラスタに問題が生じます。
- vSphere クラスタからデータセンターを削除します。

（注） HyperFlex リリース4.0 以降で新たに導入された HX クラスタは、HyperFlex ストレージ コントローラ VM の vSphere ESX Agent Manager (EAM) を利用できなくなりました。HX 4.0 より前に構築された HX クラスタは引き続き EAM を使用します。そのクラスタが新しい vCenter に移行された場合、EAM 連携は設定されません。

ステップ 1 HX クラスタの UUID を指定します。

各エージェンシーには、基盤となる vSphere 拡張機能を参照するフィールド、`cluster_domain_id` があります。この拡張機能 ID には、Managed Object ID（moid）が使用されています。

HyperFlex クラスタが複数ある場合は、登録を解除する正しいクラスタ ID を選択することを確認します。

ストレージ コントローラ VM コマンド ラインから次のコマンドを実行します。

```
# stcli cluster info | grep vCenterClusterId:
vCenterClusterId: domain-c26
```

ステップ 2 ストレージ クラスタの拡張機能を登録解除する：vCenter サーバ MOB 拡張機能マネージャにログインします。

まず、HyperFlex クラスタを登録解除します。

a) ブラウザで、パスとコマンドを入力します。

`https://vcenter_server/mob/?moid=ExtensionManager`

vcenter_server は、ストレージ クラスタが現在登録されている vCenter の IP アドレスです。

b) 管理者用のログイン クレデンシャルを入力します。

ステップ 3 クラスタ ID を持つ HX ストレージ クラスタ拡張機能を探します。**[プロパティ（Properties）]** > **[extensionList]** をスクロールして、次のストレージ クラスタ拡張機能を探します。

`com.springpath.sysmgmt.cluster_domain_id` および `com.springpath.sysmgmt.uuid.cluster_domain_id`。

クリップボードに、これらの文字列をそれぞれコピーします。文字列の端に二重引用符（”）がある場合、それを除外します。

ステップ 4 各ストレージ クラスタ拡張機能の登録を解除します。

a) [メソッド（Methods）] テーブルから `UnregisterExtension` をクリックします。

b) **[UnregisterExtension]** ポップアップに拡張機能のキー値である `com.springpath.sysgmt.cluster_domain_id` を入力します。

例：`com.springpath.sysgmt.domain-26`

c) **[メソッドの呼び出し（Invoke Method）]** をクリックします。

ステップ 5 古い EAM 拡張機能を削除する：vCenter サーバ MOB ESX エージェンシー拡張機能マネージャにログインします。

次に、HyperFlex クラスタに関連付けられていた古い EAM 拡張機能を削除します。

a) ブラウザで、パスとコマンドを入力します。

`https://vcenter_server/eam/mob/`

vcenter_server は、ストレージ クラスタが現在登録されている vCenter の IP アドレスです。

b) 管理者用のログイン クレデンシャルを入力します。

ステップ 6 当該のクラスタ ID を持つ古い HX ストレージ クラスタの ESX エージェンシー拡張機能を見つけます。

a) **[プロパティ（Properties）]** > **エージェンシー** > **[値（Value）]** までスクロールします。

b) エージェンシーの値をクリックします。

c) **[エージェンシー（Agency）]** ウィンドウで、**[プロパティ（Properties）]** > **[solutionID]** > **[値（Value）]** 拡張機能を確認します。正しい *cluster_domain_id* があることを確認します。

例：`com.springpath.sysgmt.domain-26`

ステップ 7 古い ESX エージェンシー拡張機能を削除します。

a) **[エージェンシー（Agency）]** ウィンドウの **[メソッド（Methods）]** テーブルからメソッドを選択します。

古い ESX エージェンシーは、`destroyAgency` または `uninstall` のいずれかを使用して削除できます。

b) ***[メソッド（method）]*** ポップアップで、**[メソッドの呼び出し（Invoke Method）]** をクリックします。

ステップ 8 **[ExtensionManager]** タブを更新し、**extensionList** エントリに `com.springpath.sysgmt.cluster_domain_id` という拡張機能が含まれていないことを確認します。

ステップ 9 vSphere クライアント サービスを再起動します。

vSphere クライアント サービスが再起動されると、HX Data Platform の拡張機能が削除されます。vSphere クライアント サービスを再起動すると、ブラウザを介した vCenter へのアクセスが一時的に無効になります。

vSphere クライアントからの HX Data Platform ファイルの削除

この作業は HX ストレージ クラスタ を vCenter から登録解除するための手順です。

VSphere クライアントから HX Data Platform ファイルを削除します。方法を選択します。

Linux vCenter

a) Linux vCenter サーバーに ssh を使用して、root ユーザーとしてログインします。
b) HX データ プラットフォーム プラグイン フォルダを含むフォルダに変更します。

vCenter 6.0 の場合

```
# cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

vCenter 5.5 の場合

```
# cd /var/lib/just/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

c) HX データ プラットフォーム プラグイン フォルダとファイルを削除します。

```
# rm -rf com.springpath*
```

d) vSphere クライアントを再起動します。

```
# service vsphere-client restart
```

Windows vCenter

a) Remote Desktop Protocol（RDP）を使用して、Windows vCenter システム コマンド ラインにログインします。
b) HX データ プラットフォーム プラグイン フォルダを含むフォルダに変更します。

```
# cd "%PROGRAMDATA%\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity
```

c) HX データ プラットフォーム プラグイン フォルダとファイルを削除します。

```
# rmdir /com.springpath*
```

d) サービス画面を開きます。

```
# services.msc
```

e) vCenter からログアウトして、vSphere Web クライアントを再起動します。

```
# serviceLogout
```

HX クラスタが vCenter から登録解除されていることの確認

この作業は HX ストレージ クラスタ を vCenter から登録解除するための手順です。

HX クラスタが古い vCenter 上にないことを確認します。

始める前に

次の手順を実行します：vSphere クライアントからの HX Data Platform ファイルの削除 （8 ページ）

ステップ 1 vCenter に再度ログインする前にキャッシュをクリアします。
ステップ 2 古い vCenter からログアウトします。

ステップ 3 古い vCenter に再度ログインし、HX データ プラットフォーム プラグインが削除されていることを確認します。

新しい vCenter クラスタによるストレージ クラスタの登録

始める前に

HyperFlexクラスタをvCenterに登録する前に、すべてのESXiホストでESXiロックダウンモードを無効にし、SSHサービスが有効で実行中であることを確認する必要があります。

vCenter サーバから別の vCenter サーバへストレージ クラスタを移動するタスクの一部として、vCenter クラスタからのストレージ クラスタの登録解除 （6 ページ）の手順を完了します。

ステップ 1 コントローラ VM にログインします。

ステップ 2 `stcli cluster reregister` コマンドを実行します。

stcli cluster reregister [-h] --vcenter-datacenter NEWDATACENTER --vcenter-cluster NEWVCENTERCLUSTER --vcenter-url NEWVCENTERURLIP [--vcenter-sso-url NEWVCENTERSSOURL] --vcenter-user NEWVCENTERUSER

必要に応じて、さらにリストされているオプションを適用します。

構文の説明

Option	必須またはオプション	説明
--vcenter-cluster NEWVCENTERCLUSTER	必須	新しい vCenter クラスタの名前。
--vcenter-datacenter NEWDATACENTER	必須	新しい vCenter データセンター名。
--vcenter-sso-url NEWVCENTERSSOURL	任意	新しい vCenter SSO サーバの URL。指定されない場合、`--vcenter url` から推測されます。
--vcenter-url NEWVCENTERURL	必須	新しい vCenter の URL、*<vcentername>*。ここで、*<vcentername>* には新しい vCenter の FQDN または IP を使用できます。
--vcenter-user NEWVCENTERUSER	必須	新しい vCenter 管理者のユーザー名。 プロンプトが表示されたら vCenter 管理者パスワードを入力します。

レスポンスの例：

```
Reregister StorFS cluster with a new vCenter ...
Enter NEW vCenter Administrator password:
Waiting for Cluster creation to finish ...
```

ストレージクラスタを再登録してから、コンピューティング専用ノードがEAMの登録に失敗したか、EAMクライアント内に存在しないか、vCenter のリソース プール内に存在しない場合は、下のコマンドを実行してコンピューティング専用ノードを再度追加します。

```
# stcli node add --node-ips <computeNodeIP> --controller-root-password <ctlvm-pwd> --esx-username
<esx-user> --esx-password <esx-pwd>
```

サポートが必要な場合は、TAC にお問い合わせください。

ステップ 3 スナップショット スケジュールを再入力します。

vCenter クラスタ間でストレージ クラスタを移動する場合、スナップ ショット スケジュールはストレージ クラスタと共に移動されません。

ステップ 4 （オプション）登録に成功したら、HyperFlexクラスタをvCenterに登録する前にESXiロックダウンモードを無効にします。

HX Connect を使用した vCenter の再登録

次のシナリオで vCenter を再登録する必要がある場合があります。

- コントローラ VM 証明書が変更されます。
- vCenter のアップグレードを実行するたびに、vCenter 拡張機能を再登録することをお勧めします。
- 構成の誤りにより拡張機能を手動で削除する場合は、再登録が必要です。

始める前に

HyperFlexクラスタをvCenterに登録する前に、すべてのESXiホストでESXiロックダウンモードを無効にし、SSHサービスが有効で実行中であることを確認する必要があります。

ステップ 1 HX Connect UI の **[システム情報 (System Information)]** > **[アクション (Actions)]** ドロップダウン メニューに移動します。[アクション(Action)]ドロップダウン メニューは、**[システム概要 (System Overview)]** タブ ウィンドウの右上にあります。

ステップ 2 **[アクション (Action)]** メニューから、**[vCenter 拡張機能の再登録 (Re-register vCenter）]**をオンにします。

ステップ 3 ドロップダウンメニューから **[vCenter の再登録（Re-register vCenter）]** を選択します。

ステップ 4 CVM証明書が変更され、拡張機能が正しく設定されていない場合は、**[vCenterExtensionsの再作成（Re-create vCenterExtensions）]** オプションを選択します。

（注） **[vCenterExtensionsの再作成（Re-create vCenterExtensions）]** オプションは、vCenterのメジャーアップグレード後に拡張機能を再登録する場合にのみ推奨されます。選択した場合、既存のvCenter のユーザー名とパスワードを入力します。

ステップ 5 新しい vCenter 登録の場合は、新しい vCenter のユーザ名、パスワード、および **vCenter を再登録**するための vCenter URL を入力します。

（注） **[vCenter の再登録（Re-register vCenter）]** を選択した場合は、古い vCenter からクラスタを削除し、新しいクラスタを再作成して新しい vCenter にホストを追加する必要があります。

ステップ 6 vCenter データセンター名を入力します。

ステップ 7 関連付けられているクラスタ名を入力します。

vCenter SSO URL を入力するオプションがあります。

ステップ 8 （オプション）再登録が成功したら、vCenter に HyperFlex クラスタを登録する前に ESXi ロックダウンモードを無効にします。

クラスタの名前変更

HX Data Platform ストレージ クラスタを作成した後、プロセスを中断することがなく名前を変更できます。

（注） 次の手順は vCenter クラスタではなく、HX クラスタの名前変更に適用されます。

ステップ 1 vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** の順に選択して名前変更します。

ステップ 2 **[クラスタの名前変更（Rename Cluster）]** ダイアログボックスを開きます。ストレージクラスタを右クリックするか、タブの上部にある **[アクション（Actions）]** ドロップダウンリストをクリックします。

ステップ 3 **[クラスタの名前変更（Rename Cluster）]** を選択します。

ステップ 4 テキスト フィールドにストレージ クラスタの新しい名前を入力します。

HX クラスタ名の最大文字数は 50 文字です。

ステップ 5 **[OK]** をクリックして、新しい名前を適用します。

自己署名証明書の置き換え

VCenter サーバで自己署名証明書を外部証明書へ置換

vCenter の certMgmt モードを **[カスタム (Custom)]** に設定し、サードパーティ証明書を持つ ESXi ホストを vCenter に追加します。

（注） デフォルトでは、certMgmt モードは **vmsa** です。デフォルトの **[vmsa]** モードでは、自己署名証明書を持つ ESX ホストのみ追加できます。CA 証明書を持つ ESX を vCenter に追加する場合、CA 証明書が自己署名証明書に置換されない限り ESX ホストを追加できません。

certMgmt モードを更新するには :

a) ホストを管理する vCenter サーバを選択し、**[設定 (Settings)]** をクリックします。
b) **[詳細設定 (Advanced Settings)]** をクリックしてから、**[編集 (Edit)]** をクリックします。
c) **[フィルタ (Filter)]** ボックスに、**certmgmt** と入力し、証明書管理キーのみを表示します。
d) **vpxd.certmgmt.mode** の値を **custom** に変更して**[OK]** をクリックします。
e) vCenter サーバ サービスを再起動します。

サービスを再起動するには、ブラウザに次のリンクを入力して、**[Enter]** をクリックします。

```
https://<VC URL>:5480/ui/services
```

（注） vCenter のホスト追加動作は、証明書および certMgmt モードによって異なります。

- ホストに certMgmt モードの自己署名証明書がある場合、vCenter の **vmsa**デフォルト値に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - サードパーティ CA 証明書を持つ ESX の追加は許可されていません。
  - 自己署名証明書をサードパーティ CA 証明書に置換した後 ESX を vCenter に追加する場合、システムではサードパーティ CA 証明書を自己署名証明書に置換するように促します。CA 証明書を自己署名証明書に置換した後、ESX ホストを追加できます。
- ホストに certMgmt モードの自己署名証明書がある場合、vCenter の **custom** に設定します。
  - 自己署名証明書をサードパーティ CA 証明書に置換した後 ESX を vCenter に追加する場合、システムは次のエラーをスローします。`ssl thumbprint mismatch and add host fails.` この場合、次のことを実行して、サードパーティ CA s 証明書を自己署名証明書に置換します。
    1. ホストをメンテナンス モード (MM モード) に配置します。
    2. certified rui.crt and rui.key ファイルをバックアップしている以前のキーと証明書に置換します。
    3. hostd および vpxa service を再起動します。CA 証明書が新しいノードに表示されます。
    4. 右クリックして vCenter に接続します。ホストは CA 証明書を削除し、VMware の自己署名証明書に置換します。
- ホストに certMgmt モードのサードパーティ CA 証明書がある場合、vCenter の **vmsa**デフォルト値に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - サードパーティ CA 証明書を持つ ESX の追加は許可されていません。
- ホストに certMgmt モードのサードパーティ CA 証明書がある場合、vCenter の **custom** に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - ESX ホストの自己署名証明書を vCenter の CA 証明書に置換する必要があります。

ESXi ホスト サーバで自己署名証明書を外部証明書へ置換

ステップ 1 ホスト証明書 (rui.crt) およびキー (rui.key) ファイルを生成し、ファイルを証明書機関に送信します。

（注） rui.key および rui.crt ファイルを生成している間に、ESX の適切なホスト名または FQDN が提供されていることを確認します。

ステップ 2 元のホスト証明書(rui)およびキー(rui)ファイルのバックアップを取得した後、各ESXiホストの/etc/vmware/sslディレクトリ内の認定ホスト証明書 (rui) およびキー (rui) ファイルを置き換えます。

（注） メンテナンス モードで 1 個のホストのみ配置してローリング傾向でホスト証明書 (rui.crt) およびキー(rui.key)ファイルを置き換えて、クラスタが正常になるまで待機して、それから別のノードの証明書を置き換えます。

a) 管理者権限を持つ SSH クライアントから ESXi ホストにログインします。
b) ホストをメンテナンス モード (MM モード) に配置します。
c) /etc/vmware/ssl/ ディレクトリの rui.bak ファイルに以前のキーおよび証明書のバックアップを作成します。
d) /etc/vmware/ssl/ ディレクトリに新しい認定 rui.crt および rui.key ファイルをアップロードします。
e) 次のコマンドを使用して、hostd および vpxa サービスを再起動して実行中のステータスを確認します。

```
/etc/init.d/hostd restart
/etc/init.d/vpxa restart
/etc/init.d/hostd status
/etc/init.d/vpxa status
```

f) ホストを vCenter に再接続し、メンテナンス モードを終了します。

（注） すべてのノードで同じ手順を繰り返します。Web でアクセスして各ノードの証明書を確認できます。

HyperFlex クラスタの再登録

認定ファイルを交換した後に vCenter にすべてのホストを追加した後、次のコマンドを使用して、HX クラスタを vCenter に再登録します。

```
stcli cluster reregister
```

（注） HyperFlexクラスタをvCenterに登録する前に、すべてのESXiホストでESXiロックダウンモードを無効にし、SSHサービスが有効で実行中であることを確認する必要があります。登録が成功したら、ロックダウンモードを再度有効にすることができます。

自己署名証明書の再作成

外部 CA 証明書を交換した後にホスト証明書に問題が発生した場合は、次の手順を実行して自己署名証明書を再作成できます。

1. SSH クライアントから ESXi ホストにログインします。
2. /Etc/vmware/ssl/ ディレクトリから、rui.key および rui.crt ファイルを削除します。
3. 次のコマンドを使用して、ホストの自己署名証明書を再作成します。

   ```
   /sbin/generate-certificates
   ```

4. 次のコマンドを使用して、IPICS サービスを再起動します。

   ```
   /etc/init.d/hostd restart
   /etc/init.d/vpxa restart
   ```

ブースト モード

ブースト モードを使用すると、Cisco HyperFlex クラスタでは、ストレージ コントローラ VM の CPU リソースを 4 vCPU で増やしより高い IOP を実現できます。ブースト モードを有効にすると、HX データ プラットフォームのユーザ VM から追加の CPU リソースを取得します。追加の CPU の利点が、展開のサイジングによる影響を上回ると判断された場合にのみ有効にするべきです。ブースト モードでサポートされる CPU の詳細については、Cisco HyperFlex HX220c M6すべてのNVMe、All Flash および Hybrid Server Nodes、および Cisco HyperFlex HX240C M6 All NVMe、All Flash および Hybrid Server Nodes のスペックシートを参照してください。

ブースト モードの設定

ブースト モードを有効にする各クラスタに次の手順を実行します。

始める前に

ブースト モードのサポートは次の設定に制限されています。

- サポート対象ハードウェア：
  - すべての NVMe
  - すべての Flash C240
  - すべての Flash C220
- ハイパーバイザ：ESX のみ
- コントローラ VM vCPU のブースト モード番号：
  - すべての NVMe：16
  - すべての Flash C240：12

- すべての Flash C220：12

- クラスタ拡張では、新しいノードに対してブースト モードを適用する必要があります。
- ブースト モードは Cisco HX リリース 4.0(2a) 以降でサポートされています。
- ブースト モードは、お客様の展開で追加の CPU からメリットが得られるとサポートが判断した場合にのみ、有効にしてください。

（注） CPU：多くの物理コアは、少なくともコントローラ vCPU の新しい数と等しくなければなりません。vSphere クライアントの物理コアの数を確認するには、**[ホスト (host)]** > **[設定 (Configure)]** > **[ハードウェア (Hardware)]** > **[プロセッサ (Processors)]** > **[ソケットあたりのプロセッサ コア (Processor cores per socket)]** をクリックします。

ステップ 1 vCenter から、コントローラ VM と **[ゲスト OS をシャットダウンする (Shut Down Guest OS)]** を右クリックします。

ステップ 2 すべての NVMeに対してコントローラ VM vCPU の数を 16 に増やし、all flash C220 および all flash C240 に対しては 12 に増やします。vSphere クライアントで VM の **[設定の編集 (Edit Settings)]** をクリックし、最初の行にある CPU フィールドの値を変更します。

（注） コントローラ VM vCPU のブースト モード番号：

- すべての NVMe：16
- すべての Flash C240：12
- すべての Flash C220：12

ステップ 3 設定変更を適用するには、**[OK]** をクリックします。

ステップ 4 コントローラ VM の電源をオフにします。

ステップ 5 HX Connect にログインし、クラスタが正常になるまで待機します。

ステップ 6 クラスタ内の各ホストにプロセスを繰り返します。

ブースト モードの無効

ブースト モードを無効にするには、次の手順を実行します。

ステップ 1 From the vCenter, right-click one controller VM and **Shut Down Guest OS**.

ステップ 2 すべての NVMeに対してコントローラ VM vCPU の数を 12 に減らし、all flash C220 および all flash C240 に対しては8 に減らします。vSphere クライアントで VM の **[設定の編集 (Edit Settings)]** をクリックし、最初の行にある CPU フィールドの値を変更します。

ステップ 3 設定変更を適用するには、**[OK]** をクリックします。
ステップ 4 コントローラ VM の電源をオフにします。
ステップ 5 HX Connect にログインし、クラスタが正常になるまで待機します。
ステップ 6 クラスタ内の各ホストにプロセスを繰り返します。

UEFI セキュア ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェースを定義する仕様です。HX Data Platform は、UEFI を使用して BIOS ファームウェア インターフェイスを置換します。これにより、BIOS はレガシー サポートを提供する一方で UEFI で動作できるようになります。

HX Data Platform リリース 4.5（1a）以降、クラスタ内のコンバージド ノードとコンピューティング ノードのブート モードを Unified Extensible Firmware Interface（UEFI）セキュア ブートに無停止で変更する自動ワークフローを提供することで、ハイパーバイザ（ESXi）ブートセキュリティの強化が簡素化されています。信頼チェーンは、UCS ラックおよびブレード サーバに組み込まれたハードウェア トラストアンカー（つまり、Cisco Trust Anchor モジュール）によって固定されます。各ノードのセキュア ブート ステータスの UI および API ベースのクエリも許可するため、オンデマンドでクラスタのセキュリティポスチャを監査できます。

次の制限は、UEFI ブート モードに適用されます。

- UEFI セキュア ブートは、Cisco IMC バージョン 4.1(2a) 以降を実行している HX Edge クラスタでのみ有効にする必要があります。以前のバージョンの Cisco IMC でセキュア ブートが有効になっている場合は、ファームウェアの更新中にセキュア ブートを一時的に無効にする必要があります。
- セキュア ブートのサポートは、HyperFlex ESXi M4/M5/M6 サーバでのみ使用できます。
- クラスタ拡張は M2R1 ノードでサポートされています。
- VMware ESXi でサポートされているバージョンは 6.5、6.7、および 7.0 に対して HX 4.5（1a） です。
- vCenter による ESXi ホストのセキュア ブートのアテステーションはサポートされています。この機能を使用するには、コンバージド ノードまたはコンピューティング ノードに ESXi リリース 6.7 以降と TPM 2.0 モジュールが必要です。TPM および TXT パラメータは、TPM モジュールの使用を有効にするために必要であり、セキュア ブートを有効にする際に自動的に設定されます。アテステーションを使用するための手順は必要ありません。
- 工場で準備されたすべての M.2 RAID エッジ ノードは、HXDP サーバ ファームウェア バージョン 4.1（2a）以降を実行します。顧客が現場でダウングレードするか、既存のセットアップを改良し、HXDP サーバ ファームウェア バージョンが 4.1（2a）より前の M.2RAID ノードを含むクラスタを起動しようとすると、インストールが失敗し、UEFI ブート パラメー

タをレガシー ブート モード用に設定できません。HXDP サーバ ファームウェアをバージョン 4.1（2a）以降にアップグレードしてから、インストールを再試行する必要があります。

セキュア ブート モードの有効化

- セキュア ブートモードを有効にすると、ESXi ホストのブート モードをレガシー BIOS または UEFI (非セキュア) から UEFI セキュア ブートに変更できます。
- HyperFlex クラスタの一部である UCS サーバの UCS Manager または Cisco IMC のブート パラメータを手動で変更しないでください。HyperFlex はこのような変更を認識せず、自動的に修復しません。
- [セキュア ブート ステータスの確認]アクション（ステップ 4 を参照）を使用して、クラスタのセキュア ブート ステータスを監査します。ノードがコンプライアンス違反であることが判明した場合、セキュアブートモードのアップグレードタイプオプションが[アップグレード（Upgrade）]タブで使用可能になり、ユーザはセキュアブートを再度有効にできます。コンプライアンス違反のノードのみがリブートされ、ブートモードが変更されます。

始める前に

- **[セキュア ブート ステータスの確認（Check Secure Boot Status）]**を実行して、セキュア ブートがすでに有効になっているかどうかを確認し、それに応じて続行します。ステップ 4 を参照してください。
- HX リリース 4.5（1a）以降では、HX リリース 4.5（1a） インストールの更新後、または既存のクラスタを HX 4.5（1a） にアップグレードした後、UEFI セキュアブートを別の 2 日目の操作として有効にする必要があります。
- プリフライト検証を実行して、セキュアブートを有効にするクラスタが準備完了状態であることを確認します。
- クラスタにレガシー、UEFI、および UEFI セキュア ブート ノードが存在する場合、セキュア ブート操作はクラスタのすべてのノードで有効になり、それ以降の拡張はセキュア ブートに対応します。
- セキュア ブートを有効にするオプションは、ESXi クラスタでのみ使用できます。
- セキュア ブートを有効にするために ESXi ホストがローリング リブートするため、アクティビティはメンテナンス ウィンドウで計画します。
- セキュア ブートの有効化は、他のアップグレード アクティビティと組み合わせることができません。
- セキュア ブートがすでに有効になっている場合、**[セキュア ブートの有効化（Enable Secure Boot）]** オプションはグレー表示され、それ以上のアクションは必要ありません。

- **[セキュア ブートの有効化（Enable Secure Boot）]** ワークフローが失敗した場合は、vCenter から、ホストがまだ**メンテナンス モード**であるかどうかを確認します。その場合は、**セキュア ブートの有効化**を再試行する前に、**メンテナンス モード** を終了します。

ステップ 1 HX Connect UI から、**[アップグレード (Upgrade)]** > **[アップグレード タイプの選択 (Select Upgrade Type)]** に移動します。

ステップ 2 **[アップグレード タイプの選択 (Select Upgrade Type)]** タブで、**[セキュア ブート モード (Secure Boot mode)]** チェックボックスをオンにします。

（注） セキュア ブートを有効にした後で、無効にすることはできません。

ステップ 3 vCenter と UCSM のクレデンシャル（**ユーザー名**と**管理者パスワード**）を入力し、**[アップグレード (Upgrade)]** をクリックします。

クラスタでセキュアブートを有効にすると、その後に追加された新しいコンバージドノードまたはコンピューティングノードでは、自動的にセキュアブートが有効になります。手動による作業は必要ありません。

ステップ 4 セキュア ブートのステータスを確認するには、**[システム情報]** > **[アクション]** ドロップダウン メニューに移動し、**[セキュア ブートのステータスの確認（Check Secure Boot Status）]** を選択します。

（注） すべてのノードが有効になっている場合は、**すべてのノードでセキュア ブートが有効になっている**というメッセージが表示されます。

ESXi 6.0 から ESXi 7.0U1 にアップグレードされた ESXi でセキュア ブートを有効にできない

説明

（注） VMware では、ESXi 6.0 から ESXi 7.0 への 2 段階のアップグレードが必要です。このシナリオの例は、この 2 段階のアップグレードが完了した後に発生します。

ESXi 6.0 から ESXi 7.0U1 へのアップグレード後にセキュア ブート モードを有効にすると、次のようなエラーが表示されます。

```
Secure Boot cannot be enabled on the following nodes due to signature failures with
multiple VIB(s) nenic
Please check the list of VIBs and remove/upgrade any VIB(s) that are CommunitySupported
 and retry the Enable Secure Boot workflow
```

アクション

このエラーは、元々ESXi 6.0 に導入され、その後アップグレードされたホストで発生します。通常、ESXi 7.0 にアップグレードすると、すべての VIB はシグニチャが埋め込まれた新しい VIB に置き換えられます。まれに、インストール済みの一部の VIB を手動で再インストールして、新しい組み込みシグニチャを強制的にハイパーバイザに保存する必要があります。

この特定の例では、ドライバを適切に確認するためにセキュアブートのために VIB シグニチャが保持されるように、nenic（VIC用の Cisco enic ドライバ）をアンインストールしてすぐに再インストールする必要があります。次の手順では、このドライバの再インストール中に ESXi ネットワーキングが中断されないようにします。

1. ノードにログインし、`esxcli software vib remove -n nenic` コマンドを使用して NENIC をアンインストールします。詳細については、「ホストからの VIB の削除」を参照してください。

（注） nenic ドライバがインストールされていないとネットワーク接続が失われるため、ノードを再起動しないでください。

2. `esxcli software vib install -v /<full path to nenic VIB file>/vibname` コマンドを使用して VIB を再インストールします。
3. 最初の 2 つの手順をすべてのノードで繰り返し、ローリング方式で各ノードを再起動します。
4. セキュア ブート モードの有効化を再試行します。

カタログの更新

互換性カタログ更新機能は、ESXiのCisco HyperFlexリリース4.5（1a）で導入されました。

カタログ更新では、クラスタで実行中のHXDPバージョンをアップグレードすることなく、新しいモデルのドライブのクラスタ作成、拡張、またはホットアド時にクラスタ全体でカタログバージョンを更新できます。

- 現在のカタログでサポートされていないドライブを明確に識別します。
- HXDPをアップグレードする必要がないため、クラスタノードに新しいドライブモデルを追加する際のオーバーヘッドが削減されます。
- HXインストーラ、HX Connect、およびIntersightでサポートされます。
- カタログはオンラインで更新され、実行中のクラスタには影響しません。

ガイドラインと制約事項

- 新しいドライブを追加する前に、HyperFlex リリース ノートを参照して、現在のHXDPバージョンが新しいドライブモデルをサポートしていることを確認します。
- カタログ更新では、ドライブがサポートされていることは保証されません。ハードウェアの問題とHXDPのバージョンによって、ドライブがHXDPで認識されないことがあります。
- より高いドライブ容量ポイントなど、カスタム設定にHXDPの調整が必要なドライブには、カタログアップグレードを使用しないでください。これには、完全なHXDPアップグレードが必要です。
- カタログバンドルを以前のバージョンにダウングレードすることはサポートされていません。

カタログの更新：HX インストーラ

カタログの更新：HX インストーラを使用したクラスタの作成

HX VMベースのインストーラ（OVA）を使用してクラスタの作成中にカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCOからカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

ステップ 1 HX Data Platform インストーラにログインします。

ステップ 2 標準クラスタの **[クラスタの作成]** ワークフローに従います。

ステップ 3 [サーバの選択（Server Selection）]ページで、インストーラはドライブのサポート可能性を検証し、サポートされていないドライブが見つかった場合は、サポートされていないドライブが特定され、**[カタログのアップグレード（Upgrade Catalog）]** ボタンが表示されます。

ステップ 4 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 5 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 6 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして[カタログのアップグレード] ウィンドウを終了します。

カタログのアップグレード後に、ドライブのサポート可能性チェックが再度実行されます。すべてのドライブに互換性のあるカタログがある場合、緑色の成功バナーが表示されます。

カタログの更新：HX インストーラを使用したクラスタ拡張

クラスタを拡張する場合、互換性カタログ機能は、インストーラのカタログがクラスタのカタログよりも低いかどうかを識別し、ドライブのサポート可能性の検証を実行します。HX VM ベースのインストーラ（OVA）を使用してクラスタ拡張中にカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCO からカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

ステップ 1 HX Data Platform インストーラにログインします。

ステップ 2 標準クラスタの **Expand Cluster**） ワークフローに従います。

ステップ 3 [サーバの選択（Server Selection）]ページで、インストーラはドライブのサポート可能性を検証し、サポートされていないドライブが見つかった場合は、サポートされていないドライブが特定され、**[カタログのアップグレード（Upgrade Catalog）]** ボタンが表示されます。

ステップ 4 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 5 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 6 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして [カタログのアップグレード] ウィンドウを終了します。

カタログのアップグレード後に、ドライブのサポート可能性チェックが再度実行されます。すべてのドライブに互換性のあるカタログがある場合、緑色の成功バナーが表示されます。

カタログアップグレードの完了後に現在のカタログバージョンを表示するには、実行中のクラスタの HX Connect のアップグレードページに移動します。

HX インストーラ設定からのカタログの更新

HX VM インストーラ（OVA）のアウトオブバンド カタログアップグレードを実行するには、次の手順を実行します。

ステップ 1 HX Data Platform インストーラにログインします。

ステップ 2 任意のページの **[設定（Settings）]** 歯車アイコンをクリックします。

ステップ 3 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 4 ローカルに保存されたカタログ ファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 5 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして [カタログのアップグレード] ウィンドウを終了します。

カタログ アップグレードの完了後に現在のカタログバージョンを表示するには、**[設定（Settings）]**>**[アップグレード カタログ（Upgrade Catalog）]** をクリックして、アップグレード カタログ ウィンドウに戻ります。

カタログの更新：HX Connect

HX Connect を使用したクラスタ カタログのアップグレード

新しいディスクが HX Connect で認識されない場合は、カタログの更新が必要である可能性があります。HX Connect を使用してカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCO からカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

（注） HXDP バージョンをアップグレードすると、クラスタ カタログが自動的にアップグレードされます。すでに更新されたカタログが含まれているバージョンに HXDP をアップグレードする場合は、カタログを手動で更新する必要はありません。

ステップ 1 HX Connect の **[アップグレード（Upgrade）]** タブをクリックします。

ステップ 2 [アップグレードの選択（Select Upgrade）] タブの **[HX データ プラットフォーム（HX Data Platform）]** ボックスをオンにしてください。

（注） カタログアップグレードと他のタイプのアップグレードの組み合わせはサポートされていません。

ステップ 3 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
カタログファイルのアップロード操作が完了しました。

ステップ 4 アップグレードを完了するには、**[アップグレード（Upgrade）]** をクリックします。

a) HX ストレージクラスタのアップグレードタスクの進行状況をモニタするには、HX Connect の **[アクティビティ（Activity）]** ページをクリックします。

ステップ 5 **[システム情報（System Information）]** ページをクリックし、すべてのディスクが HXDP によって要求され、使用中であることを確認します。

カタログの更新：Intersight

Intersight を使用したカタログのアップグレード

HX インストーラ VM とは異なり、Intersight HX インストーラは最新の互換性カタログで自動的に最新の状態に維持されます。シスコは、Intersight HX インストーラのアップデートを定期的にリリースし、その標準プロセスの一部としてカタログのアップデートを含めています。

同様に、Intersight に接続されたクラスタは、HX Connect を介して手動でダウンロードおよびアップロードする必要なく、自動的に最新のカタログバージョンに更新されます。これらの自動更新を受信するには、HyperFlex クラスタが Intersight に接続されていることを確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。