クラスタ設定後のタスク

クラスタ設定後のガイドライン

重要

- すべての ESXi ホストで SSH を有効なままにしてください。これは、これ以降の Cisco HyperFlex post クラスタ設定後の作業で必要となります。
- これらの事前設定された値は、シスコの承認を得ずに変更しないでください。

ホスト上のネットワーク デバイスの PCI パススルー有効化

パススルーデバイスは、より効率的にリソースを使用して環境内のパフォーマンスを向上させるための手段を提供します。PCI パススルーを有効化することで、VM はホスト デバイスを、VM に直接接続されているように使用できます。

⚠

注意 HXDP クラスタの重要なデバイスを PCI パススルー用にセットアップしないでください。

次の手順では、ESXi ホスト上の PCI パススルー用にネットワーク デバイス（NVIDIA GPU など）を設定する方法を説明します。

ステップ 1 vSphere Client のナビゲーション パネルで ESXi ホストを参照します。

ステップ 2 GPU がインストールされているノードで、HX メンテナンス モードを開始します。メンテナンス モードを開始するには、ノードを右クリックし、**[Cisco HX Maintenance Mode (Cisco HX メンテナンス モード)>]** > **[Enter HX Maintenance Mode (HX メンテナンス モードの開始)]** の順に選択します。

ステップ 3 新しいブラウザ ウィンドウで、ESXi ノードに直接ログインします。

ステップ 4 [Manage] をクリックします。

ステップ 5 [Hardware] タブで、 [PCI Devices] をクリックします。利用可能なパススルー デバイスのリストが表示されます。

ステップ 6 パススルーに対して有効にする PCI デバイスを選択します。**[Toggle passthrough (パススルーのトグル)]** をクリックします。

ステップ 7 ホストを再起動して、PCI デバイスを利用可能にします。

ステップ 8 リブートが完了したら、ノードがメンテナンス モードになっていないことを確認します。

ステップ 9 vCenter Server にログインします。

ステップ 10 VM を検索して右クリックし、**[Edit Settings (設定の編集)]** を選択します。

ステップ 11 [New device] ドロップダウン メニューで [PCI Device] を選択して、[Add] をクリックします。

ステップ 12 使用するパススルー デバイス（例：NVIDIA GPU）をクリックして、[OK] をクリックします。

ステップ 13 ESXi ホストにログインし、仮想マシンの設定ファイル（.vmx）をテキスト エディタで開きます。

```
cd /vmfs/volumes/[datastore_name]/[vm_name]
vi [vmname].vmx
```

ステップ 14 次の行を追加して保存し、テキスト エディタを終了します。

```
# pciPassthru.64bitMMIOSizeGB = "64"
# Firmware = "efi"
# pciPassthru.use64bitMMIO = "TRUE"
```

インストール後のスクリプトの実行

インストーラ後のスクリプトを実行することで、インストール後のタスクを完了できます。

重要

- HyperFlex System を展開した後、ただちに *hx_post_install* を実行して、ネットワークの動作を確認してください。

1. SSH クライアントを使用して、admin ログインを使用してクラスタ仮想 IP に接続します。
2. 「`hx_post_install`」と入力して、`Enter` キーを押します。
3. 次の表に指定しているように、インストール後スクリプト パラメータを設定します。

（注） インストール後スクリプトに問題が発生した場合は、インストール後スクリプトのパラメータを手動で設定します。

パラメータ	説明
Enable HA/DRS on cluster?（クラスタで HA/DRS を有効にするか）	ベスト プラクティスに従って vSphere 高可用性（HA）機能を有効にします。
Disable SSH warning?（SSH 警告を無効にするか）	vCenter 内での SSH 警告とシェル警告を抑制します。
Add vMotion interfaces（vMotion インターフェイスの追加）	ベスト プラクティスに従って vMotion インターフェイスを設定します。*IP* アドレスと *VLAN ID* の入力が必要です。
Add VM network VLANs（VM ネットワーク VLAN の追加 ）	すべてのクラスタ ホスト上の ESXi 内、および Cisco UCS Manager にゲスト VLAN を追加します。

4. ネットワーク エラーが報告された場合には修正します。

サンプルのインストール後のスクリプト: オプション 1 新規/既存のクラスタ

サンプルのインストール後のスクリプト: オプション 3 Generate Certificate

ネットワーク エラーの例

```
Host: esx-hx-5.cpoc-rtp.cisco.com
No errors found
```

```
Host: esx-hx-6.cpoc-rtp.clsco.com
No errors found

Host: esx-hx-l.cpoc-rtp.cisco.com
No errors found

Host: esx-hx-2.cpoc-rtp.cisco.com
No errors found

controller VM clocks:
stctlVM-FCH1946V34Y - 2016-09-16 22:34:04
stCtlVM-FCH1946V23M - 2016-09-16 22:34:04
stctIVM-FCH1951V2TT - 2016-09-16 22:34:04
stctlVM-FCH2004VINS - 2016-09-16 22:34:04

Cluster:
Version - 1.8.1a-19499
Model - HX220C-M4S
Health - HEALTHY
Access policy - LENIENT
ASUP enabled - False
SMTP server - smtp.cisco.com
```

ESXi ホストのルート パスワードの変更

次のシナリオで、デフォルトの ESXi パスワードを変更できます。

- 標準およびストレッチ クラスタの作成時（コンバージド ノードのみをサポート）
- 標準クラスタの拡張時 （コンバージド ノードまたはコンピューティング ノードの両方の拡張をサポート）
- エッジ クラスタの作成時

（注） 上記の場合、インストールが完了するとすぐに ESXi のルート パスワードが保護されます。後続のパスワード変更が必要である場合、下に概要を示している手順をインストール後に使用して、ルート パスワードを手動で変更することができます。

ESXi は工場出荷時のデフォルト パスワードで提供されているため、セキュリティ上の理由からパスワードを変更する必要があります。インストール後のデフォルトの ESXi ルート パスワードを変更するには、次の手順を実行します。

（注） ESXi ルート パスワードを忘れた場合は、パスワードの復旧について Cisco TAC にお問い合わせください。

ステップ 1 SSH を使用して ESXi ホスト サービス制御にログインします。

ステップ 2 ルート権限を取得します。

```
su -
```

ステップ 3 現在のルート パスワードを入力します。

ステップ 4 ルート パスワードを変更します。

```
passwd root
```

ステップ 5 新しいパスワードを入力し、**Enter** キーを押します。確認のためにパスワードを再入力します。

（注） 2 回目に入力したパスワードが一致しない場合は、最初からやり直す必要があります。

ストレージ コントローラのパスワードの変更

インストール後に HyperFlex ストレージ コントローラのパスワードをリセットするには、次の手順を実行します。

ステップ 1 ストレージ コントローラ VM にログインします。

ステップ 2 Cisco HyperFlex ストレージ コントローラ パスワードを変更します。

```
# stcli security password set
```

このコマンドによって、ストレージ クラスタ内のすべてのコントローラ VM に変更が適用されます。

（注） 新しいコンピューティング ノードを追加し、**stcli security password set** コマンドを使用してクラスタ パスワードをリセットしようとすると、コンバージド ノードは更新されますが、コンピューティング ノードはデフォルト パスワードのままになることがあります。コンピューティング ノードのパスワードを変更するには、次の手順を使用します。

ステップ 3 新しいパスワードを入力します。

ステップ 4 **Enter** を押します。

VMware vCenter の Cisco HyperFlex HTML プラグイン

Cisco HyperFlex vCenter プラグインは、vSphere Web クライアントと統合され、HX Data Platform のインストール後の管理およびモニタリング機能をすべてサポートします。インストールと使用法に関する完全な情報については、『Cisco HyperFlex Data Platform Administration Guide』の「Cisco HyperFlex HTML Plugin for VMware vCenter」の章を参照してください。

ストレージ クラスタでのデータストアの追加

新しい HyperFlex クラスタでは、仮想マシン ストレージ用のデフォルト データストアが設定されていないため、VMware vSphere Web クライアントを使用してデータストアを作成する必要があります。

（注） 高可用性を実現するために、最低 2 つのデータストアを作成することを推奨します。

ステップ 1 Web クライアント ナビゲータの **[Global Inventory Lists]** で、**[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **[cluster]** > **[Manage]** > **[Datastores]** の順に展開します。

ステップ 2 [データストアの作成（Create Datastore）] アイコンをクリックします。

ステップ 3 データストアの**名前**を入力します。vSphere Web クライアントはデータストア名に 42 文字の制限を適用します。各データストアに固有の名前を割り当てます。

ステップ 4 データストアの**サイズ**を指定します。ドロップダウンリストから、[GB] または [TB] を選択します。[OK] をクリックします。

ステップ 5 新しいデータストアを表示するには、[Refresh] ボタンをクリックします。

ステップ 6 新しいデータストアの [マウント ステータス（Mount Status）] を表示するには、[ホスト（Hosts）] タブをクリックします。

HA ハートビートの設定

vSphere HA の設定では、使用可能なデータストアのリストから任意のデータストアを選択できるように、[ハートビーティングのデータストア（Datastore for Heartbeating）] オプションを必ず設定してください。

ステップ 1 vSphere にログインします。

ステップ 2 DRS が有効になっていることを確認します。

vSphere の**[ホーム (Home)]** > **[ホストとクラスタ (Hosts and Clusters)]** > 、**[クラスタ (cluster)]** > **[設定 (Configure)]**、**[サービス (Services)]**を選択します。[vSphere DRS] をクリックします。

ステップ 3 [Edit] ボタンをクリックします。[vSphere HA] をクリックします。[編集（Edit）] をクリックします。

ステップ 4 選択されていなければ、**[vSphere HA をオンにする (Turn on vSphere HA)]** を選択します。

ステップ 5 ドロップダウン メニューから **[アドミッション コントロール (Admission Contro)l]** > **[フェールオーバ容量の定義 (Define Fallover capacity by)]** > **[クラスタ リソース割合 (Cluster resource percentage)]** を展開します。デフォルト値を使用することも、[Override calculated failover capacity] を有効にしてパーセンテージを入力することもできます。

ステップ 6 [Heartbeat Datastores] を展開し、[Use datastore only from the specified list] を選択します。含めるデータストアを選択します。

ステップ 7 [OK] をクリックします。

HyperFlex の自動サポートと Smart Call Home

HX ストレージ クラスタを構成して、文書化されたイベントに関する自動化された電子メール通知を送信することができます。通知内の収集されたデータを使用して、HX ストレージ クラスタの問題のトラブルシューティングに役立てることができます。

（注） Auto Support (ASUP) および Smart Call Home (SCH) は、プロキシ サーバの使用をサポートしています。プロキシ サーバの使用を有効にし、HX Connect を使用して、両方のプロキシ設定を構成できます。

Auto Support（ASUP）

Auto Support は、HX Data Platform を通じて提供されるアラート通知サービスです。Auto Support を有効にすると、HX Data Platform から、指定されたメール アドレスまたは通知を受信したい電子メール エイリアスに通知が送信されます。通常、Auto Support は、HX ストレージ クラスタの作成時に、SMTP メール サーバを設定し、電子メールの受信者を追加して設定します。

（注） 未認証の SMTP のみが ASUP のサポート対象となります。

構成中に **[Enable Auto Support (Auto Support を有効にする)]** チェック ボックスが選択されていない場合、次の方法を使用して Auto Support をクラスタの作成後に有効にすることができます。

クラスタ作成後の ASUP 構成方法	関連トピック
HX Connect ユーザ インターフェイス	HX Connect を使用した自動サポートの設定 （8 ページ）
コマンドライン インターフェイス（CLI）	CLI を使用した通知設定の構成 （10 ページ）
REST API	Cisco HyperFlex は Cisco DevNet での REST API をサポートします。

Auto Support は、監視ツールに HX ストレージ クラスタを接続するためにも使用できます。

Smart Call Home（SCH）

Smart Call Home は、HX ストレージ クラスタを監視し、ビジネスの運営に影響をおよぼす前に問題にフラグ付けして解決を開始する、自動化されたサポート機能です。これにより高いネットワーク可用性と運用効率の向上をもたらします。

Call Home は、さまざまな障害や重要なシステム イベントを検出してユーザに通知する、Cisco デバイスのオペレーティング システムに埋め込まれている製品機能です。Smart Call Home は、基本的な Call Home 機能を強化するための自動化と便利な機能を追加します。Smart Call Home を有効にすると、Call Home のメッセージとアラートは Smart Call Home に送信されます。

Smart Call Home は Cisco の多くのサービス契約に含まれており、次が含まれます。

- 自動化された、24 時間の機器監視、プロアクティブな診断、リアルタイムの電子メール アラート、サービス チケットの通知、および修復の推奨。
- Call Home 診断とインベントリ アラームをキャプチャおよび処理することにより指定された連絡先に送信される、プロアクティブなメッセージング。これらの電子メール メッセージには、自動的に作成された場合に Smart Call Home ポータルと TAC ケースへのリンクが含まれています。
- Cisco Technical Assistance Center（TAC）による優先サポート。Smart Call Home では、アラートが十分に重大な場合、TAC ケースが自動的に生成され、デバッグおよび他の CLI 出力が添付されて、`https` 経由で適切なサポート チームにルーティングされます。
- カスタマイズ可能なステータス レポートおよびパフォーマンス分析。
- 次に対する Web ベースのアクセス 1 箇所における修復のためのすべての Call Home メッセージ、診断、および推奨、TAC ケースのステータス、すべての Call Home デバイスの最新のインベントリおよび構成情報。

HX ストレージ クラスタ、ユーザ、サポートの間で自動的に通信が行われるように設定する方法については、データ収集用の Smart Call Home の設定 （11 ページ）を参照してください。

HX Connect を使用した自動サポートの設定

一般に、Auto Support（ASUP）は HX ストレージ クラスタの作成中に設定されます。設定されなかった場合は、クラスタ作成後に HX Connect ユーザ インターフェイスを使用して有効にすることができます。

ステップ 1 HX Connect にログインします。

ステップ 2 バナーで、**[設定の編集（Edit settings）]**（歯車アイコン）>**[自動サポートの設定（Auto Support Settings）]** をクリックして、次のフィールドに値を入力します。

UI 要素	基本的な情報
[自動サポートの有効化（推奨）（Enable Auto Support (Recommended)）] チェックボックス	以下を有効にすることにより、この HX ストレージ クラスタの Call Home を設定します。 • Cisco TAC への分析用データの配信。 • プロアクティブ サポートの一環としてのサポートからの通知。
[サービス チケット通知の送信先（Send service ticket Notifications to）] フィールド	通知を受信する電子メール アドレスを入力します。
[Terms and Conditions (使用条件)] チェック ボックス	エンドユーザー使用契約。自動サポート機能を使用するには、このチェック ボックスをオンにする必要があります。
[プロキシ サーバを使用（Use Proxy Server）] チェックボックス	• **Web プロキシ サーバ** URL • **[ポート（Port）]** • **ユーザー名（Username）** • **パスワード**

ステップ 3 [OK] をクリックします。

ステップ 4 バナーで、**[設定の編集（Edit settings）]**（**歯車アイコン**）>**[通知の設定（Notifications Settings）]** をクリックして、次のフィールドに値を入力します。

UI 要素	基本的な情報
[電子メール通知によるアラームの送信（Send email notifications for alarms）] チェックボックス	オンにした場合は、次のフィールドに値を入力します。 • **メールサーバアドレス** • **送信元アドレス（From Address）**：サポート サービス チケットでHXストレージクラスタを特定するために使われる電子メールアドレスを、自動サポート通知の送信者として入力します。現在、この電子メールアドレスにはサポート情報が送信されません。 • **受信者リスト(カンマ区切り)**

ステップ 5 [OK] をクリックします。

CLI を使用した通知設定の構成

HX ストレージ クラスタからアラーム通知を受信する設定を構成および検証するには、次の手順に従います。

（注） 未認証の SMTP のみが ASUP のサポート対象となります。

ステップ 1 ssh を使用して HX ストレージ クラスタ内のストレージ コントローラ VM にログインします。

ステップ 2 SMTP メール サーバを設定し、設定を確認します。

指定された受信者に電子メール通知を送信するために SMTP メール サーバで使用される電子メール アドレスです。

構文：`stcli services smtp set [-h] --smtp SMTPSERVER --fromaddress FROMADDRESS`

例：

```
# stcli services smtp set --smtp mailhost.eng.mycompany.com --fromaddress smtpnotice@mycompany.com
# stcli services smtp show
```

ステップ 3 ASUP 通知を有効にします。

```
# stcli services asup enable
```

ステップ 4 受信者の電子メール アドレスを追加して、設定を確認します。

電子メール通知を受信する一連の電子メール アドレスまたは電子メール エイリアスのリストです。複数の電子メールはスペースで区切ります。

構文：`stcli services asup recipients add --recipients RECIPIENTS`

例：

```
# stcli services asup recipients add --recipients user1@mycompany.com user2@mycompany.com
# stcli services asup show
```

ステップ 5 HX ストレージ クラスタの eth1:0 IP アドレスを所有しているコントローラ VM から、電子メールでテスト ASUP 通知を送信します。

```
# sendasup -t
```

eth1:0 IP アドレスを所有しているノードを判別するには、ssh を使用して HX ストレージ クラスタの各ストレージ コントローラ VM にログインし、ifconfig コマンドを実行します。他のノードから sendasup コマンドを実行しても、出力は何も返されず、受信者はテストを受信しません。

ステップ 6 すべてのストレージ コントローラ VM の IP アドレスから電子メールを送信できるように電子メール サーバを設定します。

データ収集用の Smart Call Home の設定

データ コレクションはデフォルトで有効にされますが、インストール時にオプトアウト（無効化）することができます。クラスタ作成後のデータ コレクションを有効にすることもできます。アップグレード中、Smart Call Home の有効化はレガシー構成によって決まります。たとえば、`stcli services asup show` を有効にすると、アップグレード時に Smart Call Home が有効になります。

HX ストレージ クラスタに関するデータ コレクションは、`https` を介して Cisco TAC に転送されます。インストールされているファイアウォールがある場合、Smart Call Home のプロキシ サーバの構成は、クラスタ作成の後に完了します。

（注） HX クラスタからの発信接続がプロキシ サーバを通過する必要がある展開では、Smart Call Home はプロキシ サーバの使用をサポートしていません。

（注） HyperFlex Data Platform リリース 2.5(1.a) では、Smart Call Home Service Request（SR）の生成でプロキシ サーバは使用されません。

Smart Call Home を使用するには、次のものが必要です。

- 対応する Cisco Unified Computing Support Service 契約または Cisco Unified Computing Mission Critical Support Service 契約と関連付けられた Cisco.com ID。
- 登録されるデバイス用の Cisco Unified Computing Support Service または Cisco Unified Computing Mission Critical Support Service

ステップ 1 HX ストレージ クラスタ内のストレージ コントローラ VM にログインします。

ステップ 2 HX ストレージ クラスタをサポートに登録します。

HX ストレージ クラスタを登録すると、収集されたデータに ID を追加し、Smart Call Home を自動的に有効にします。HX ストレージ クラスタを登録するには、電子メール アドレスを指定する必要があります。登録後、問題が発生して TAC サービス要求が生成されるたびに、このメール アドレスはサポート通知を受け取ります。

構文：

```
stcli services sch set [-h] --email EMAILADDRESS
```

例：

```
# stcli services sch set --email name@company.com
```

ステップ 3 HX ストレージ クラスタからサポートへのデータ フローが機能していることを確認します。

データ フローが機能していれば、問題が発生した場合にサポートがそれをトラブルシューティングするうえで役立つ関連情報が確実に得られます。

（注） TAC に連絡して接続を確認してください。

```
# asupcli [--all] ping
```

`--all` オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

ステップ 4 （省略可能）ポート 443 を介した Smart Call Home のアクセスを有効にするためにプロキシ サーバを設定します。

クラスタの作成後、HX ストレージ クラスタがファイアウォールの背後にある場合は、Smart Call Home プロキシ サーバを構成する必要があります。サポートは、`url: https://diag.hyperflex.io:443` エンドポイントでデータを収集します。

1. 既存の登録メールとプロキシ設定をすべてクリアします。

   ```
   # stcli services sch clear
   ```

2. プロキシと登録メールを設定します。

   構文：

   stcli services sch set [-h] --email EMAILADDRESS [--proxy-url PROXYURL] [--proxy-port PROXYPORT] [--proxy-user PROXYUSER] [--portal-url PORTALURL] [--enable-proxy ENABLEPROXY]

構文の説明

Option	必須またはオプション	説明
--email EMAILADDRESS	必須。	シスコ サポートから電子メールを受信するユーザのために、電子メールアドレスを追加します。配信リストまたはエイリアスを使用することをお勧めします。
--enable-proxy ENABLEPROXY	オプション。	プロキシの使用を明示的に有効または無効にします。
--portal-url PORTALURL	オプション。	代替の Smart Call Home ポータル URL を指定します（該当する場合）。
--proxy-url PROXYURL	オプション。	HTTP または HTTPS プロキシの URL を指定します（該当する場合）。
--proxy-port PROXYPORT	オプション。	HTTP または HTTPS プロキシの ポート を指定します（該当する場合）。
--proxy-user PROXYUSER	オプション。	HTTP または HTTPSプロキシの URL を指定します（該当する場合）。 HTTP または HTTPS プロキシのパスワードを指定します（メッセージが表示される場合）。

例：

```
# stcli services sch set
  --email name@company.com
  --proxy-url www.company.com
  --proxy-port 443
  --proxy-user admin
  --proxy-password adminpassword
```

3. プロキシ サーバが動作していること、および HX ストレージ クラスタからサポート ロケーションにデータが流れることを確認するために ping を送信します。

   （注） TAC に連絡して接続を確認してください。

   ```
   # asupcli [--all] ping
   ```

   `--all` オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

ステップ 5 Smart Call Home が有効になっていることを確認します。

Smart Call Home 構成が設定されると、自動的に有効になります。

```
# stcli services sch show
```

ステップ 6 自動サポート（ASUP）通知を有効にします。

一般に、Auto Support（ASUP）は HX ストレージ クラスタの作成中に設定されます。設定されなかった場合、HX Connect または CLI を使用してクラスタ作成後の設定を有効にすることができます。

Smart Call Home が無効になっている場合は、手動で有効にします。

```
# stcli services sch enable
```

自己署名の証明書を CA 署名の証明書で置き換える

（注） リリース 5.0(1x) 以前の場合、次の証明書置換スクリプトを実行するには、コントローラ VM へのルート レベルのアクセスが必要です。TAC に連絡して、証明書置換プロセスを完了してください。リリース 5.0(2a) 以降では、**diag** ユーザー シェルにアクセスして CAPTCHA テストを完了する必要があります。プロセスの説明については、『Cisco HyperFlex Data Platform 管理ガイド、リリース 5.0』の 「Diag ユーザーの概要」 を参照してください。

CA 証明書のインポートは、シェルスクリプトによって自動化されています。任意の CVM、できれば CIP ノードから CSR（証明書署名要求）を生成します。各 CVM は同じ証明書でインストールする必要があるため、クラスタに必要な CSR は 1 つだけです。CSR を生成するときに、管理 CIP に割り当てられたホスト名をサブジェクトの識別名の共通名として入力する必要があります。

次に例を示します。

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:HyperFlex
Common Name (e.g. server FQDN or YOUR name) []:<hostname-cluster-management-IP>
Email Address []:support@cisco.com
```

CA 証明書を取得した後で、自動スクリプトを使用して証明書をインポートします。スクリプトは、その CVM の証明書のみを更新します。

（注） クラスタ拡張の場合は、証明書をインポートするために、同じ証明書とキーファイルを使用して、拡張されたノード CVM でスクリプトを再度実行する必要があります。

diag シェルにアクセスしたら、次の手順を実行します。

ステップ 1 CVM でのスクリプトの場所は、/usr/share/springpath/storfs-misc/hx-scripts/ です。

```
diag/usr/share/springpath/storfs-misc/hx-scripts/certificate_import_input.certificate_import_input.sh

    run stcli cluster reregister
```

ステップ 2 コントローラ VM（CIP を指す）で、このコマンドを実行して CSR 要求を生成します。

```
openssl req -nodes -newkey rsa:2048 -keyout /etc/ssl/private/<Host Name of the CVM>.key -out
/etc/ssl/certs/<Host Name of the CVM>.csr
   cat /etc/ssl/certs/<host name mapped to the management CIP>.csr - Copy the request to any notepad.

    Send the request to CA to generate the certificate
```

ステップ 3 CA（.crt ファイル）から証明書を受信したら、証明書とキーを各 CVM にコピーします。

ステップ 4 各CVMで、./certificate_import_input.sh スクリプトを使用して証明書をインポートします。

```
root@SpringpathControllerVUFSTDS58L:/usr/share/springpath/storfs-misc/hx-scripts#
./certificate_import_input.sh
```

ステップ 5 キーのパスとして、/etc/ssl/private/<CVM のホスト名>.key を入力します。

ステップ 6 <CA へのパス.crt ファイル> という証明書形式で証明書のパスを入力します。

（注） すべての入力を入力した後、インポートプロセスが完了するまでにいくらか時間がかかります。

ステップ 7 CIP をポイントしている CVM から **stcli reregister** コマンドを実行して、クラスタを vCenter に再登録します。証明書をインポートしたら、クラスタを再登録する必要があります。

レプリケーション ペアリング

レプリケーション クラスタ ペアの作成は、VM をレプリケーション用にセットアップするための前提条件です。レプリケーション ペアを作成する前に、レプリケーション ネットワークと少なくとも 1 つのデータストアを設定する必要があります。

クラスタ 2 とクラスタ 1 をペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ 1 上のすべての VM はクラスタ 2 にレプリケートでき、レプリケーション用に明示的に設定されたクラスタ 2 上のすべての VM はクラスタ 1 にレプリケートできることを指定しています。

クラスタ 1 のデータストア A とクラスタ 2 のデータストア B をペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ 1 上のすべての VM では、データストア A にファイルがある場合、それらのファイルはクラスタ 2 のデータストア B にレプリケートされることを指定しています。同様に、レプリケーション対象として明示的に設定されたクラスタ 2 上のすべての VM では、データストア B にファイルがある場合、それらのファイルがクラスタ 1 のデータストア A にレプリケートされます。

ペアリングは厳密に 1 対 1 で行われます。クラスタは、他のクラスタのうち 1 つとだけペアリング可能です。ペアリングされるクラスタ上のデータストアは、もう一方のクラスタ上の 1 つのデータストアとだけペアリングできます。

レプリケーション ペアの作成、編集、および削除の詳細な手順については、『Cisco HyperFlex Systems Administration Guide』を参照してください。

プライベート VLAN の追加

プライベート VLAN について

プライベート VLAN では VLAN のレイヤ 2 ブロードキャスト ドメインがサブドメインに分割されるので、スイッチで相互にポートを分離できます。サブドメインは、1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN で構成されます。プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバーで、プライマリ VLAN は、プライベート VLAN ドメイン全体です。

プライベート VLAN ポートの概要

表 *1*: プライベート *VLAN* ポートのタイプ

VLAN ポート	説明
Promiscuous Primary VLAN	プライマリ VLAN に属しています。無差別ポートに関連付けられているセカンダリ VLAN に属しているインターフェイス、およびプライマリ VLAN に関連付けられているインターフェイスのすべてと通信できます。それらのインターフェイスには、コミュニティ ポートと独立ホスト ポートも含まれます。セカンダリ VLAN からのすべてのパケットは、この VLAN を経由します。
独立したセカンダリ VLAN	度クリスしたセカンダリ VLAN に属するホスト ポートです。このポートは同じプライベート VLAN ドメイン内のその他のポートから完全に分離されていますが、関連付けられている無差別ポートとは通信できます。
コミュニティ セカンダリ VLAN	コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。

HX の導入に従い、VM ネットワークはデフォルトで通常の VLAN を使用します。VM ネットワークにプライベート VLAN を使用する場合は、次のセクションを参照してください。

- 既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定 （16 ページ）。
- 既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定 （17 ページ）。

既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『 Cisco UCS Manager Network Management Guide』を参照してください。

ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

ステップ 3 ESX ホストでプライベート VLAN を設定するには、ESX ホスト上でのプライベート VLAN の設定 （16 ページ）を参照してください。

ESX ホスト上でのプライベート VLAN の設定

ESX ホストでプライベート VLAN を設定するには、次の手順を実行します。

ステップ 1 VMware vSphere クライアントから vSphere 標準スイッチ上の VMNIC を削除します。
ステップ 2 前の手順で削除した VMNIC を使用して新しい vSphere 分散型スイッチを作成します。
ステップ 3 無差別（プロミスキャス）、独立、およびコミュニティ VLAN を作成します。

既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『 Cisco UCS Manager Network Management Guide』を参照してください。
ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。
ステップ 3 ESX ホストでプライベート VLAN を設定するには、を参照してください。 ESX ホスト上でのプライベート VLAN の設定 （16 ページ）
ステップ 4 vSphere 標準スイッチから、新しく作成された vSphere 分散型スイッチに VM を移行します。
a) vCenter 仮想マシンを右クリックして、[Migrate Virtual Machine Networking] をクリックします。
b) ドロップダウン リストから、[送信元ネットワーク（source network）] および [送信先ネットワーク（destination network）] を選択します。
c) [次へ（Next）] をクリックします。
d) 移行する [仮想マシン（Virtual Machines）] を選択します。
e) [Finish] をクリックします。
ステップ 5 VM 上のネットワーク アダプタのネットワーク接続をプライベート VLAN に変更します。
a) vCenter 仮想マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。
b) [ハードウェア（Hardware）] タブから、変更するネットワーク アダプタを選択します。
c) [ネットワーク ラベル（Network Label）] ドロップダウン リストから、使用する [ネットワーク接続（Network Connection）] を選択します。
d) [OK] をクリックします。

VSphere 標準スイッチ上での VMNIC の削除

ステップ 1 VMware vSphere クライアントにログオンします。
ステップ 2 [ホーム（Home）] > [ホストとクラスタ（Hosts and Clusters）] を選択します。
ステップ 3 削除する VMNIC がある ESX ホストを選択します。
ステップ 4 [設定（Configuration）] タブを開きます。
ステップ 5 [Networking] をクリックします。

ステップ 6 VMNIC を削除する**スイッチ**を選択します。
ステップ 7 [Manage the physical adapters connected to the selected switch] ボタンをクリックします。
ステップ 8 削除する **vminc** を選択し、[削除（Remove）] をクリックします。
ステップ 9 [はい（Yes）] をクリックして、選択内容を確認します。
ステップ 10 [閉じる（Close）] をクリックします。

vSphere 分散型スイッチの作成

ステップ 1 VMware vSphere クライアントにログオンします。
ステップ 2 [Home] > [Networking] を選択します。
ステップ 3 クラスタを右クリックして、[Distributed Switch] > [New Distributed Switch] を選択します。
ステップ 4 [Name and Location] ダイアログボックスに、分散スイッチの名前を入力します。
ステップ 5 [Select Version] ダイアログボックスで、バージョンと構成の要件に対応する分散スイッチ バージョンを選択します。
ステップ 6 [Next] をクリックします。
ステップ 7 [Edit Settings] ダイアログボックスで、次のように指定します。

- [Number of uplink ports]
- [Network I/O Control] を**有効化**します。
- [Create a default port group] をオンにします。
- [Port Group Name] ボックスに、デフォルト ポート グループの**名前**を入力します。

ステップ 8 [Next] をクリックします。
ステップ 9 [Ready to Complete] ダイアログボックスで、設定した内容を確認します。
ステップ 10 **[終了]** をクリックします。

vSphere 分散型スイッチ上でのプライベート VLAN の作成

ステップ 1 VMware vSphere クライアントから、[インベントリ（Inventory）]>[ネットワーキング（Networking）] を選択します。
ステップ 2 dvSwitch を右クリックします。
ステップ 3 [Edit Settings] をクリックします。
ステップ 4 [プライベート VLAN（Private VLAN）] タブを選択します。
ステップ 5 [プライマリ プライベート VLAN ID（Primary private VLAN ID）] タブで、**プライベート VLAN ID** を入力します。

ステップ 6 [セカンダリ プライベート VLAN ID（Secondary private VLAN ID）] タブで、**プライベート VLAN ID** を入力します。

ステップ 7 [タイプ（Type）] ドロップダウン リストから、VLAN のタイプを選択します。有効な値は次のとおりです。

- **隔離**
- **コミュニティ**
- **無差別**(デフォルト)

ステップ 8 [OK] をクリックします。

分散型ポート グループ内のプライベート VLAN の設定

始める前に

vSphere 分散スイッチでプライベート VLAN を作成します。

ステップ 1 [dvSwitch] の下の [dvPortGroup] を右クリックして、[設定の編集（Edit Settings）] をクリックします。

ステップ 2 [ポリシー（Policies）] > [VLAN] をクリックします。

ステップ 3 [VLAN タイプ（VLAN type）] ドロップダウン リストから [プライベート VLAN（Private VLAN）] を選択します。

ステップ 4 [プライベート VLAN エントリ（Private VLAN Entry）] ドロップダウン リストから、プライベート VLAN のタイプを選択します。次のいずれかを指定できます。

- **隔離**
- **コミュニティ**

（注） コミュニティ プライベート VLAN が推奨されています。

混合モード ポートはサポートされていません。

ステップ 5 [OK] をクリックします。

分散型仮想スイッチと Cisco Nexus 1000v

分散型スイッチを導入する際の検討事項

（注）

- 分散型仮想スイッチ（DVS）または Cisco Nexus 1000v（NK1v）の使用はオプションであり、必須の手順ではありません。
- VMotion ネットワークの DVS は、環境に vSphere の Enterprise Plus ライセンスが設定されている場合にのみ使用できます。
- 特定の時点で 2 つのスイッチのどちらかだけを使用できます。
- Hyperflex と Nexus 1000v の間で Quality of Service（QoS）ポリシーが競合する可能性があります。HyperFlex ポリシーに従って N1Kv の QoS クラスが設定されていることを確認する必要があります。『Network and Storage Management Guide』の「*Creating a QoS Policy*」を参照してください。
- N1Kv スイッチを導入する場合は、HyperFlex ホスト間のトラフィックが安定した状態で FI 上をローカルに流れるように、説明に従って設定を適用します。正確に設定しない場合、ほとんどのトラフィックがアップストリーム スイッチを通過して遅延が発生する可能性があります。このシナリオを回避するには、ストレージコントローラ、管理ネットワーク、および vMotion ポート グループがアクティブ/スタンバイで設定され、フェールオーバーが有効になっていることを確認してください。

1. UCS Manager を使用して、[ネットワーク制御ポリシー（Network Control Policies）] の [リンク ステータス（link status）] を設定します。詳細については、『Cisco UCS Manager GUI Configuration Guide』の「Configuring Network Control Policy」のセクションを参照してください。
2. vCenter で vSwitch プロパティを設定します。
   a. [ネットワーク障害検出（Network Failure Detection）] を [リンク ステータスのみ（Link Status only）] に設定します。
   b. [フェールバック（Failback）] を [はい（Yes）] に設定します。詳細については、『Cisco UCS Manager VM-FEX for VMware Configuration guide』の「Configuring the VM-FEX for VMware」のセクションを参照してください。

分散型スイッチにより、各ノードで同じ設定が確実に使用されます。こうしてトラフィックに優先順位を付けることができ、アクティブな vMotion トラフィックがないときに、使用可能な帯域幅を他のネットワーク ストリームで活用できるようになります。

HyperFlex（HX）Data Platform では、非 HyperFlex 依存ネットワークに分散型仮想スイッチ（DVS）ネットワークを使用できます。

このような非 HX 依存ネットワークには以下のものが含まれます。

- VMware vMotion ネットワーク
- VMware アプリケーション ネットワーク

HX Data Platform には、次のネットワークが標準的な vSwitch を使用するという依存関係があります。

- vswitch-hx-inband-mgmt：ストレージ コントローラ管理ネットワーク
- vswitch-hx-inband-mgm：管理ネットワーク
- vswitch-hx-storage-data：ストレージ ハイパーバイザ データ ネットワーク
- vswitch-hx-storage-data：ストレージ コントローラ データ ネットワーク

HX Data Platform のインストール時に、すべてのネットワークで標準 vSwitch ネットワークが設定されます。ストレージクラスタを設定した後、非HX依存ネットワークをDVSネットワークに移行することができます。次に例を示します。

- vswitch-hx-vm-network：VM ネットワーク
- vmotion：vmotion pg

vMotion ネットワークを分散型仮想スイッチに移行する方法の詳細については、『Network and Storage Management Guide』の「*Migrating vMotion Networks to Distributed Virtual Switches (DVS) or Cisco Nexus 1000v (N1Kv)*」を参照してください。

HX Data Platform 上での vCenter のホスト

HyperFlex クラスタ上で vCenter の展開をサポートする場合、いくつかの制約があります。詳細については、『How to Deploy vCenter on the HX Data Platform』テクニカル ノートを参照してください。

AMD GPU の展開

AMD FirePro S7150 シリーズ GPU は HX240c M5/M6 ノードでサポートされます。これらのグラフィック アクセラレータでは、非常に安全な高いパフォーマンス、そしてコスト効率の良い VDI 展開を有効にします。HyperFlex に AMD GPU を展開するには、次の手順に従います。

ステップ	アクション	手順の説明
1	サーバに接続されているサービス プロファイルの BIOS ポリシーを変更します。	サポートされるすべてのGPUに関する要件：メモリマップド I/O 4 GB 以上
2	サーバにGPUカードをインストールします。	GPU カードのインストール
3	サーバの電源をオンにして、GPUがサーバの Cisco UCS Manager インベントリに表示されることを確認します。	—

ステップ	アクション	手順の説明
4	AMD GPU カードの vSphere インストール バンドル（VIB）をインストールして、再起動します。	Cisco ソフトウェア ダウンロードから、VMware ESXi 上の AMD 用の C シリーズ スタンドアロンファームウェア/ソフトウェア バージョンバンドル 3.1(3) の最新ドライバ ISO を含むインベントリ リストをダウンロードします。
5	VM 設定を使用してクラスタ上で Win10 VM を作成します。	対象の仮想マシンの指定
6	各 ESXi ホストで、`MxGPU.sh` スクリプトを実行して GPU を設定し、GPU から仮想機能を作成します。	MxGPU セットアップ スクリプトの使用
7	前のステップで作成した仮想機能（VF）を Win10 Vm に割り当てます。	—

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。