# 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**

- SSH をすべての ESXi ホストで有効なままにします。これは、次の Cisco HyperFlex クラスタ設定後操作に必要です。
- 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。

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** [Configure] タブをクリックして、[Settings] をクリックします。

**ステップ 3** [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 4** デバイス（NVIDIA GPU など）を選択して、[Toggle passthrough] をクリックします。

**ステップ 5** 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 6** vSphere Web Client を使用して vCenter にログインします。

**ステップ 7** VM を特定して [Manage] タブをクリックします。**[Settings]** > **[VM Hardware]** を選択します。[Edit] をクリックします。

**ステップ 8** [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 9** 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 10** 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 11** 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 VM でインストール後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。スクリプトは、すべてのネットワーク インターフェイス（管理、vMotion、およびストレージ ネットワーク）に ping を実行して、ファブリックが完全に利用できることを確認します。また、ノースバウンド スイッチで VLAN のタギングが正しいことと、ジャンボ フレーム設定を検証します。

重要

- *post_install* スクリプトは、ノースバウンド スイッチ経由で強制的に接続を確立します。ネットワークが正しく設定されていない場合は、1 つのノードがクラスタ内で接続を一時的に失う可能性があります。テストが完了すると、設定が元に戻ります。
- HyperFlex システムを導入したら、すぐに *post_install* を実行し、ネットワークが動作することを確認します。
- アップストリーム ネットワークを以前に検証したことがある場合を除き、実稼働システムでこのスクリプトを実行しないでください。
- Web ベースの SSH がロードされていない場合、優先クライアントを使用してインストーラ VM に SSH で接続し、`post_install` スクリプトを実行します。

1. Web ブラウザから、`http://<installer VM IP>/mssh` にアクセスします。
2. インストーラ VM のルート クレデンシャルでログインします。
3. `post_install` と入力し、[Enter] を押します。
4. 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 |
|---|---|
| クラスタでHA/DRSを有効にするか（Enable HA/DRS on cluster?） | 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。 |
| SSH 警告を無効にするか（Disable SSH warning?） | vCenter で SSH とシェルの警告を抑制します。HyperFlex システムを適切に機能させるには、SSH を有効のままにしておく必要があります。 |
| vMotion インターフェイスを追加する（Add vMotion interfaces） | 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 の入力は必須です。 |
| VM ネットワーク VLAN を追加する（Add VM network VLANs） | Cisco UCS Manager およびすべてのクラスタ ホスト上の ESXi 内にゲスト VLAN を追加します。 |
| ESXi ホストで NTP を有効にする（Enable NTP on ESXi hosts） | ESXi ホストで NTP を設定し、有効にします。 |

| パラメータ | 説明 |
|---|---|
| 寛容モードを有効にする（Enable Lenient Mode?） | 寛容モードはデフォルトになりました。[Y]を押して処理を続行します。 |
| テスト メールを送信する（Send test email?） | SMTP メール サーバと 自動サポート パラメータが設定されている場合は、SMTP リレーが動作していることを確認するためにテスト メールが送信されます。 |

**5.** 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

```
root@Cisco-HX-Data-Platform-Installer:~# post_install
Setting ESX hosts from HX cluster...
vCenter URL: 172.26.17.177
Enter vCenter username (user@domain): administrator@vsphere local
vCenter password:
Found datacenter RTP-DC
Found cluster HX-Cluster

Enable HA/DRS on cluster? (y/n) y

Disable SSH warning? (y/n) y

configure ESXi logging onto HX datastore? (y/n) y
No datastores found
Creating datastore...
Name of datastore: HX-Logs
size (6B): 50
Storing logs on datastore HX-Logs
Creating folder [HX-Logs]/esxi_logs

Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.255.0
VLAN ID: (0-4096) 3093
vMotion IP for esx-hx-6.cpoc-rtp.cisco.com: 192.168.11.154
Adding vmKernel to esx-hx-6.cpoc-rtp.cisco.com
vMotion IP for esx-hx-1.cpoc-rtp.cisco.com: 192.168.11.151
Adding vmotion to esx-hx-1.cpoc-rtp.cisco.com
Adding vmKernel to esx-hx-1.cpoc-rtp.cisco.com
vMotion IP for esx-hx-5 .cpoc- rtp.cisco.com: 192.168.11.153
Adding vmKernel to esx-hx-5.cpoc-rtp.cisco.com
vMotion IP for esx-hx-2.cpoc- rtp.cisco.com: 192.168.11.152
Adding vmKernel to esx-hx-2.cpoc-rtp.cisco.com

Add VM network VLANs? (y/n) n

Enable NTP on ESX hosts? (y/n) y
Starting ntpd service on esx-hx-6.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-1.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-5.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-2.cpoc-rtp.cisco.com

Enable Lenient Mode? (y/n) y
Lenient mode is already set

Send test email? (y/n) n
```

```
Validating cluster health and configuration...
Found UCSM hyper-ucs.cpoc-rtp.cisco.com, logging with username admin. Org is hx-cluster

UCSM Password:

Checking MTU settings
pinging 192.168.16.164 from vmk1
pinging 192.168.10.161 from vmk1
pinging 192.168.16.163 from vmk1
pinging 192.168.1(3.162 from vmk1
Setting vnic2 to active and vmic3 to standby
Pinging 192.168.10.164 from vmk1
pinging 192.168.16.164 with mtu 8972 from vmkl
Pinging 192.168.10.161 from vmk1
pinging 192.168.10.161 with mtu 8972 from vmkl
pinging 192.168.16.163 from vmk1
pinging 192.168.10.163 with mtu 8972 from vmkl
pinging 192.168.10.162 from vmk1
pinging 192. 168.16. 162 with mtu 8972 from vmkl
Setting vmnic3 to active and vnic2 to standby
pinging 172.26.17.154 from vmk0
pinging 172.26.17 .151 from vmk0
pinging 172.26.17.153 from vmk0
Pinging 172.26.17.152 from vmk0
Setting vnicl to active and vmnic0 to standby
pinging 172.26.17.154 from vmk0
Pinging 172.26.17.151 from vmk0
pinging 172.26.17.153 from vmk0
pinging 172.26.17.152 from vmk0
Setting vmnic0 to active and vnicl to standby
pinging 192.168.11.154 from vmk2
pinging 192.168.11.151 from vmk2
pinging 192.168.11.153 from vmk2
pinging 192.168.11.152 from vmk2
Setting vnic7 to active and vmnic6 to standby
pinging 192.168.11.154 from vmk2
pinging 192.168.11.154 with mtu 8972 from vmk2
pinging 192.168.11.151 from vmk2
pinging 192.168.11.151 with mtu 8972 from vmk2
Pinging 192.168.11.153 from vmk2
pinging 192.168.11.153 with mtu 8972 from vmk2
pinging 192.168.11.152 from vmk2
pinging 192.168.11.152 with mtu 8972 from vmk2
Setting vmnic6 to active and vnic7 to standby
```

## サンプルのネットワーク エラー

```
Host: esx-hx-5.cpoc-rtp.cisco.com
Np 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 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 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** HyperFlex ストレージ コントローラの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、変更がストレージ クラスタ内のすべてのコントローラ VM に適用されます。

（注） 新しいコンピューティング ノードを追加し、**scli security password set** コマンドを使用してクラスタ パスワードを再設定しようとすると、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。

コンピューティング ノードでパスワードを変更するには：

1. ESXi ホストからすべてのユーザー VM を vMmotion します。
2. VCenter からストレージ コントローラ VM コンソールを起動し、root ユーザーとしてログインします。
3. **passwd** コマンドを実行して、パスワードを変更します。
4. ログアウトして再度ログインし、パスワードが正常に変更されたことを確認します。
5. **stcli node add -f** コマンドを実行し、ノードをクラスタに再び追加します。

**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。

# vSphere を介した HX データ プラットフォーム プラグインへのアクセス

GUI を介してストレージ クラスタを管理するには、vSphere Web クライアントを起動します。vSphere Web クライアントおよび HX データ プラットフォーム プラグインを使用してストレージ クラスタにアクセスします。

**ステップ 1** HX データ プラットフォーム インストーラから、インストールの完了後に、[Summary] ページで [Launch vSphere Web Client] をクリックします。

**ステップ 2** ログイン ページが表示され、[Login to vSphere Web Client] をクリックして、vSphere クレデンシャルを入力します。

**ステップ 3** HX データ プラットフォーム プラグインが表示されます。

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] を選択します。

# 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** vSphere 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** [Create Datastore] アイコンをクリックします。

**ステップ 3** [Name] にデータストアの名前を入力します。vSphere Web クライアントでは、データストア名に 42 文字の制限が適用されます。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 [Size] 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** [Hosts] タブをクリックして、新しいデータストアの [Mount Status] を確認します。

# 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、[Datastore for Heartbeating] オプションを設定します。

**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**[Home]** > **[Hosts and Clusters]** 、**[cluster]** > **[Configure]**、[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。[Edit] をクリックします。

**ステップ 4** 選択されていなければ、[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 [Admission Control] > **[Define Fallover capacity by]** > **[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 Auto Support 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。

### 自動サポート (ASUP)

自動サポート 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。自動サポートを有効にすると、HX Data Platform から、通知の受信先として指定された電子メール アドレスまたは電子メール エイリアスに通知が送信されます。自動サポートは通常、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] 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 自動サポート 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構成 （10 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 （11 ページ） |
| REST API | Cisco HyperFlex は Cisco DevNet での REST API をサポートします。 |

自動サポート を使用して、HX ストレージ クラスタをモニタリング ツールに接続することもできます。

### 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 システムに組み込まれている製品機能です。 Smart Call Home は Call Home の基本機能を高めるために自動化機能と利便性向上機能を追加します。Smart Call Home を有効にすると、Smart Call Home に Call Home メッセージ/アラートが送信されます。

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。
- カスタマイズされたステータス 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、あなた、そしてサポートの間で自動通信を確保するには、データ コレクションの Smart Call Home の構成 （12 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構成

通常は、HX ストレージ クラスタの作成中に 自動サポート （ASUP）が設定されます。設定されなかった場合、HX Connect ユーザ インターフェイス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。

**ステップ 1** HX Connect にログインします。

**ステップ 2** バナーで、**[Edit settings]**（**歯車アイコン**）> **[Auto Support Settings]** の順にクリックして次のフィールドに記入します。

| UI 要素 | 基本情報 |
|---|---|
| [Enable Auto Support (Recommended)] チェック ボックス | 次を有効にすることで、このHXストレージクラスタの自宅に発信を構成します。<br>• 分析のための Cisco TAC へのデータ配信。<br>• プロアクティブ サポートの一環としてサポートからの通知。 |
| [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。 |
| [Enable Remote Support] チェック ボックス | クラスタ操作に関する情報を収集して報告された異常のトラブルシューティングを高速化するために、サポートのHX ストレージクラスタへのアクセスを有効にします。 |
| [Use Proxy Server] チェックボックス | • **Web プロキシ サーバ** url<br>• **Port**<br>• **Username**<br>• **Password** |

**ステップ 3** [OK] をクリックします。

**ステップ 4** バナーで、**[Edit settings]**（**歯車アイコン**）> **[Notifications Settings]** の順にクリックして次のフィールドに記入します。

| UI 要素 | 基本情報 |
|---|---|
| [Send email notifications for alarms] チェック ボックス | オンにした場合は、次のフィールドを入力します。<br>• **[Mail Server Address]**<br>• [From Address]：サポート サービス チケットの HX ストレージ クラスタを識別するために使用し、また自動サポート通知の送信者として使用するメールアドレスを入力します。現在、サポート情報はこのメール アドレスには送信されません。<br>• **[Recipient list]**（**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確認するには、次の手順に従ってください。

（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。

シンタックス：`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、設定を確認します。

電子メール通知を受信する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。電子メールが複数ある場合はスペースで区切ります。

シンタックス：`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 の IP アドレスを所有しているコントローラ VM から、電子メールにテスト ASUP 通知を送信します。

```
# sendasup -t
```

eth1:0 の IP アドレスを所有しているノードを確認するには、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 コレクションの Smart Call Home の構成

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。アップグレード中に、Smart Call Home がレガシー構成に基づいて設定されます。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） 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** サポート付きの HX ストレージ クラスタを登録します。

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、このメール アドレスは、問題があり TAC のサービス要求が生成されるたびにサポート通知を受け取ります。

（注） Hyperflex で Smart Call Home を設定するときに、登録を完了するためのリンクを含む電子メールが設定済みのアドレスに送信されます。この手順を完了していない場合、デバイスは非アクティブ状態のままになり、自動サービス リクエストはオープンになりません。

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 フローが稼働していることを確認します。

稼働しているデータ フローにより、生じる可能性のある問題のトラブルシューティングをサポートできる関連情報をすぐに利用できます。

-すべて オプションの HX クラスタ内のすべてのノードのコマンドを実行します。

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

HX ストレージ クラスタを HyperFlex 1.7.1 から 2.1.1b にアップグレードする場合は、次のコマンドも実行します。

```
# asupcli [--all] post --type alert
```

次のエラーが表示される場合はサポートに問い合わせてください。

```
root@ucs-stctlvm-554-1:/tmp# asupcli post --type alert
/bin/sh: 1: ansible: not found
Failed to post - not enough arguments for format string
root@ucs-stctlvm-554-1:/tmp#
```

**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**

| オプション | 必須またはオプション | 説明 |
|---|---|---|
| **--email EMAILADDRESS** | 必須です。 | Cisco サポートからのメールを受信する人の電子メールアドレスを追加します。配布リストまたはエイリアスを使用することを推奨します。 |
| **--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 ポータルの URL を指定します（該当する場合）。 |
| **--proxy-url PROXYURL** | オプション。 | HTTP 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 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 プロキシのユーザを指定します（該当する場合）。<br>HTTP 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 サーバが動作しており、データが HX ストレージ クラスタからサポート ロケーションに流れることを確認するために Ping を送信します。

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

   -すべて オプションが HX クラスタ内のすべてのノードで、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 の設定が `set` の場合、自動的に有効になります。

```
# stcli services sch show
```

Smart Call Home が無効の場合は手動で有効にします。

```
# stcli services sch enable
```

**ステップ 6** 自動サポート（ASUP）通知を有効にします。

通常は、HX ストレージ クラスタの作成中に 自動サポート （ASUP）が設定されます。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。詳細については、「HyperFlex の Auto Support と Smart Call Home」を参照してください。

# 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、レプリケーション用 VM の設定の前提条件です。レプリケーション ネットワークと少なくとも 1 つのデータストアは、レプリケーション ペアを作成する前に構成しなければなりません。

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。1 つのクラスタを 2 つ以上の他のクラスタとペアリングすることはできません。ペアになっているクラスタ上の 1 つのデータストアは、他のクラスタ上の 1 つのデータストアとしかペアリングできません。

レプリケーション ペアの作成、編集、および削除の詳細手順については、「Cisco HyperFlex Systems アドミニストレーション ガイド」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 の概要

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 のメンバーであり、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 に属します。無差別ポートに関連付けられ、プライマリ VLAN に関連付けられているセカンダリ VLAN に属するすべてのインターフェイスと通信できます。これらのインターフェイスには、コミュニティ ポートと隔離されたホスト ポートが含まれます。セカンダリ VLAN からのすべてのパケットがこの VLAN を通過します。 |
| 隔離されたセカンダリ VLAN | 隔離されたセカンダリ VLAN に属するホスト ポート。このポートは、アソシエートされている無差別ポートと通信できることを除き、同じプライベート VLAN ドメイン内の他のポートから、完全に隔離されています。 |
| 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。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 配備後、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 を使用するには、次のセクションを参照してください。

- 既存の VM がない状態で VM ネットワークのプライベート VLAN を設定する （17 ページ）。
- 既存の VM で VM ネットワークのプライベート VLAN を設定する （17 ページ）。

# 既存の VM がない状態で VM ネットワークのプライベート VLAN を設定する

**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 ネットワーク管理ガイド』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 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』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 ホストでのプライベート VLAN の設定 （17 ページ） を参照してください。

## ESX ホストでのプライベート 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 分散スイッチを作成します。

**ステップ 3** 無差別、独立、およびコミュニティ VLAN を作成します。

# 既存の VM で VM ネットワークのプライベート VLAN を設定する

**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 ネットワーク管理ガイド』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 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』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、以下を参照してください。ESX ホストでのプライベート VLAN の設定 （17 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、[source network] および [destination network] を選択します。
c) [Next] をクリックします。
d) 移行する**仮想マシン**を選択します。
e) [Finish] をクリックします。

**ステップ 5** VM 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、[Edit Settings] をクリックします。
b) [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) [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を選択します。
d) [OK] をクリックします。

## vSphere 標準スイッチでの VMNIC の削除

**ステップ 1** VMware vSphere クライアントにログインします。
**ステップ 2** [Home] > [Hosts and Clusters] を選択します。
**ステップ 3** VMNIC を削除する ESX ホストを選択します。
**ステップ 4** [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、[Remove] をクリックします。
**ステップ 9** [Yes] をクリックして、選択内容を確認します。
**ステップ 10** [Close] をクリックします。

## vSphere 分散スイッチの作成

**ステップ 1** VMware vSphere クライアントにログインします。
**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** [Finish] をクリックします。

## vSphere 分散スイッチでのプライベート VLAN の作成

**ステップ 1** VMware vSphere クライアントから、[Inventory] > [Networking] を選択します。
**ステップ 2** dvSwitch を右クリックして、[Edit Settings] をクリックします。
**ステップ 3** [Private VLAN] タブを選択します。
**ステップ 4** [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 5** [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 6** [Type] ドロップダウン リストから、VLAN のタイプを選択します。次のいずれかを設定できます。

- **[Isolated]**
- **[Community]**

（注） **無差別**プライベート VLAN が自動的に作成されます。

**ステップ 7** [OK] をクリックします。

## 分散ポート グループでのプライベート 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、[Edit Settings] をクリックします。
**ステップ 2** [Policies] > [VLAN] をクリックします。
**ステップ 3** [VLAN type] ドロップダウン リストから [Private VLAN] を選択します。
**ステップ 4** [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。次のいずれかを設定できます。

- **[Isolated]**
- **[Community]**

（注） コミュニティ プライベート VLAN が推奨されます。

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 ネットワーク用の DVS は、ご使用の環境に vSphere 用の Enterprise Plus ライセンスがある場合にのみ使用できます。
- 同時に使用できるスイッチは、常にこの 2 つのうちのいずれか 1 つだけです。
- HyperFlex と Nexus 1000v の間では、Quality of Service（QoS）ポリシーが競合する可能性があります。N1Kv の QoS クラスが HyperFlex ポリシーに従って設定されるようにしてください。『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、説明のとおりに設定を適用し、HyperFlex ホスト間のトラフィックが FI 上を定常状態でローカルに流れるようにします。正しく設定されていないと、トラフィックの大半がアップストリーム スイッチを経由することになる可能性があります。その場合には遅延が発生します。このような事態を避けるには、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 グループをアクティブ/スタンバイ構成で設定し、フェールオーバーを有効にしてください。

1. UCS Manager を使用して、[Network Control Policy] に**リンク ステータス**を設定します。詳細については、『Cisco UCS Manager GUI Configuration Guide』の「Configuring Network Control Policy」を参照してください。
2. vCenter で vSwitch のプロパティを設定します。

   a. [Network Failure Detection] を [Link Status only] に設定します。

   b. [Failback] を [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」を参照してください。

---

分散スイッチにより、各ノードが同じ構成を使用することになります。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）データ プラットフォームは、HyperFlex 非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。

これらの HX 非依存ネットワークには次のものがあります。

- VMware vMotion ネットワーク

- VMware アプリケーション ネットワーク

HX データ プラットフォームには依存関係があり、次のネットワークが標準の vSwitch を使用します。

- 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-mgmt：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データ プラットフォームのインストール時に、すべてのネットワークが標準のvSwitchネットワークで設定されます。ストレージ クラスタが設定された後、HX 非依存ネットワークを DVS ネットワークに移行できます。次に例を示します。

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

分散仮想スイッチに vMotion ネットワークを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 での vCenter のホスト

HyperFlex クラスタへの vCenter の導入をサポートするには、いくつかの制約事項が伴います。詳細については、 HX データ プラットフォームで vCenter を展開する方法 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 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 の 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 | 手順の指示 |
|---|---|---|
| 1 | サーバに接続されているサービスプロファイルに関して BIOS ポリシーを変更します。 | サポートされるすべての GPU の要件：4 GB を超えるメモリマップド I/O |
| 2 | サーバでに GPU カードをインストールします。 | GPU カードの取り付け |

| ステップ | アクション | 手順の指示 |
|---|---|---|
| 3 | サーバの電源を入れて、GPUがサーバのCisco UCS Managerインベントリで表示されていることを確認します。 | — |
| 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。 | VMware ESXi で AMD 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 Cisco ソフトウェア ダウンロードから、インベントリ リストをダウンロードします。 |
| 5 | VM 設定済みのクラスタで Win10 VM を作成します。 | 対象の仮想マシンを指定する |
| 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 スクリプトを使用する |
| 7 | Win10 Vm に対して前のステップで作成された仮想機能 (VFs) を割り当てます。 | — |