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 クラスタ設定後の作業で必要となります。
- HX Data Platform で使用される ESXi バージョンには、HyperFlex データ プラットフォーム用に最適化された ESXi の調整と設定が含まれています。ESXi 調整を変更する必要がある場合は、TAC にお問い合わせください。

インストール後のスクリプトの実行

インストール後タスクを完了するには、インストーラ VM 上でインストール後スクリプトを実行できます。この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）を ping して、ファブリックの完全な可用性を確認します。また、このスクリプトは、ノース バウンド スイッチ上のジャンボ フレームの設定と VLAN の正しいタギングも検証します。

重要

- *post_install* スクリプトは、ノースバウンド スイッチ経由の接続を強制します。ネットワークが適切に設定されていない場合は、クラスタ内で 1 つのノードが一時的に接続を失う可能性があります。テストの終了後に、設定が元に戻されます。
- HyperFlex System を展開した後、ただちに *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。
- アップ ストリーム ネットワークをまだ検証していない場合は、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 が読み込まれない場合は、適切なクライアントを使ってインストーラ VM に SSH し、`post_install` スクリプトを実行します。

1. Web ブラウザから、`http://<インストーラ VM IP>/mssh` に移動します。
2. インストーラ VM のルート クレデンシャルを使用してログインします。
3. 「`post_install`」と入力して、`Enter` キーを押します。
4. 次の表に示すように、インストール後スクリプト パラメータを設定します。

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。HyperFlex システムが適切に機能するには、SSH を有効なままにする必要があります。
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。
Enable NTP on ESXi hosts（ESXi ホスト上の NTP を有効にする）	ESXi ホスト上で NTP を設定して有効にします。
Enable Lenient Mode?（寛容モードを有効にするか）	現在は、寛容モードがデフォルトです。続行するには、**Y** キーを押します。

パラメータ	説明
Send test email?（テストメールの送信）	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 リレーが動作す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は、それを修正します。

インストール後スクリプトの例

```
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-l.cpoc-rtp.cisco.com: 192.168.11.151
Adding vmotion to esx-hx-l.cpoc-rtp.cisco.com
Adding vmKernel to esx-hx-l.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-l.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
```

ネットワーク エラーの例

```
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 ホストのルート パスワードの変更

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再設定するには、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） unix パスワード コマンドを使用しないでください。

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 経由の HX Data Platform 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 Data Platform プラグインを介してストレージ クラスタにアクセスします。

ステップ 1 HX Data Platform インストーラから、インストールの完了後に、[概要（Summary）] ページで [vSphere Web Client の起動（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、[vSphere Web Client へのログイン（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 Data Platform プラグインを表示します。

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（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 ナビゲータから、[vCenter インベントリ リスト（vCenter Inventory Lists）] で、**[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > [クラスタ（cluster）] > [管理（Manage）] > [データストア（Datastores）] を選択します。

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、[更新（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 で、**[ホーム（Home）]** > **[vCenter インベントリ リスト（vCenter Inventory Lists）]**[**リソース（Resources）]** > **[クラスタ（Clusters）]**[**ストレージ クラスタ（Storage cluster）]** > **[管理（Manage）]**[**設定（Settings）]** > **[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 [vSphere HA によるクラスタの設定の編集（vSphere HA Edit Cluster Settings）] が表示されます。[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 [vSphere HA をオンにする（Turn on vSphere HA）] が選択されていなければ、これを選択します。

ステップ 5 [アドミッション制御（Admission Control）] を展開し、[ストレージ クラスタ リソースのパーセンテージを予約してフェールオーバー キャパシティを定義する（Define Failover capacity by reserving a percentage of the storage cluster resources）] を選択します。パーセンテージを割り当てます。

ステップ 6 [ハートビート データストア（Heartbeat Datastores）] を展開し、[指定されたリストからのデータストアのみを使用（Use datastore only from the specified list）] を選択します。[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。

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。

構成中に [自動サポートを有効にする（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。

このクラスタ ASUP 構成後の方法の場合	次のトピックを参照してください。
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 （9 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。

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 が有効にされると、それ以降は Call Home メッセージ/アラートが 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、次のものがあります。

- 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 診断およびインベントリ アラームをキャプチャして処理し、指定された連絡先に送信する、プロアクティブ メッセージング。これらのメール メッセージには、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（自動的に作成された場合）。
- 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 チームに転送されます。
- 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。
- Web ベースのアクセス。Call Home のメッセージ、診断、修復の推奨のすべてに 1 か所でアクセスできる他、TAC ケースのステータス、あらゆる Call Home デバイスの最新のインベントリと設定情報に Web でアクセスできます。

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

通常、自動サポート（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。
[Remote Support の有効化（Enable Remote Support）] チェックボックス	サポート担当がHXストレージクラスタにアクセスできるようにします。これにより、クラスタの操作に関する情報を収集し、報告された異常を迅速にトラブルシューティングできます。
[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）]** • **ユーザ名** • **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。

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。

ASUP を有効にした後、クラスタ内のすべてのノードに関するヘルス チェック メールが 1 日 1 回送信されます。

データ収集用の Smart Call Home の設定

データ収集はデフォルトで有効になりますが、インストール時にオプトアウト（無効に）することができます。また、クラスタ作成後にデータ収集を有効にすることもできます。アップグレード中には、従来の設定に基づいて Smart Call Home がセットアップされます。たとえば、`stcli services asup show` が有効であれば、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収集は、`https` を介して Cisco TAC に転送されます。ファイアウォールがインストール済みの場合、クラスタの作成後に Smart Call Home のプロキシ サーバの設定が完了します。

（注） HyperFlex データ プラットフォーム リリース 2.5(1.a) の場合、Smart Call Homeサービス リクエスト（SR）の生成ではプロキシ サーバを使用しません。

Smart Call Home を使用するには、以下が必要です。

- 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 が追加され、Smart Call Homeが自動的に有効にされます。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。

`--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。

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

HX ストレージ クラスタを HyperFlex 1.7.1 から 2.1.1b にアップグレードした場合は、次のコマンドも実行してください。

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

次のエラーを受け取った場合は、サポートに連絡してください。

```
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 （オプション）ポート 443 を介した Smart Call Home アクセスが可能になるようにプロキシ サーバを設定します。

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、クラスタの作成後に Smart Call Home プロキシ サーバを設定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。

Option	必須またはオプション	説明
--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 プロキシ 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 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 ユーザを指定します（該当する場合）。 プロンプトが表示されたら、HTTP プロキシ パスワードを指定します。

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。

   ```
   # 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 の設定が `set` である場合、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、自動サポート（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 または CLI を使用して有効にすることができます。詳細については、HyperFlex の自動サポートと Smart Call Home （7 ページ）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、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 1 とクラスタ 2 をペアリングすると、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 1 上のすべての VM がクラスタ 2 にレプリケートされ、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 がクラスタ 2 にレプリケートされるようになります。

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るたクラスタ 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 （15 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 （16 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 （15 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 （15 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、[仮想マシン ネットワーキングの移行（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 [ハードウェア（Hardware）] で [ネットワーキング（Networking）] をクリックします。
ステップ 6 削除する **vminc** がある **vSwitch** の横の [プロパティ（Properties）] をクリックします。
ステップ 7 [ネットワーク アダプタ（Network Adapters）] タブをクリックします。
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 を右クリックして、[新しい vSphere 分散スイッチ（New vSphere Distributed Switch）] をクリックします。
ステップ 3 [vSphere 分散スイッチの作成（Create vSphere Distributed Switch）] ダイアログボックスで、[vSphere 分散スイッチのバージョン：6.0.0（vSphere Distributed Switch Version: 6.0.0）] を選択します。
ステップ 4 [次へ（Next）] をクリックします。
ステップ 5 [一般プロパティ（General Properties）] タブで、次の項目を指定します。

- **名前**
- **[アップリンク ポートの数（Number of uplink ports）]**

ステップ 6 [次へ（Next）] をクリックします。
ステップ 7 [ホストと物理アダプタの追加（Add Hosts and Physical Adapters）] で、[今すぐ追加（Add Now）] を選択します。
ステップ 8 目的の ESX ホストの下で、[物理アダプタ（Physical Adapters）] を選択します。
ステップ 9 [次へ（Next）] をクリックします。
ステップ 10 [Finish] をクリックします。

デフォルトのポート グループが作成されます。

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 を右クリックして、[設定の編集（Edit Settings）] をクリックします。
ステップ 3 [プライベート VLAN（Private VLAN）] タブを選択します。
ステップ 4 [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 5 [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 6 [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。次のいずれかを指定できます。

- **隔離**
- **コミュニティ**

（注） [無差別（Promiscuous）] 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。

- **混合（プロミスキャス）**
- **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。

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（N1Kv）

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。

さらに支援が必要な場合は、TAC までお問い合わせください。

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 アクセラレータにより、安全性とパフォーマンスに優れた、コスト効率の高い VDI 環境が有効になります。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。	—