# 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。

### 手順

**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 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。

**重要**

- 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。

1. インストーラ VM でシェルに接続するには、SSH クライアントを使用します。
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。 |
| 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。 |

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
Select post_install workflow-

 1. New/Existing Cluster
 2. Expanded Cluster
 3. Generate Certificate

 Note:  Workflow No.3 is mandatory to have unique SSL certificate in the cluster.
 By Generating this certificate, it will replace your current certificate.
 If you're performing cluster expansion, then this option is not required.

 Selection: 3
 Certificate generation workflow selected

Logging in to controller 10.20.1.64
HX CVM admin password:
Getting ESX hosts from HX cluster...

Select Certificate Generation Workflow-

 1. With vCenter
 2. Without vCenter

 Selection: 1
vCenter URL: 10.33.16.40
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Starting certificate generation and re-registration.
Trying to retrieve vCenterDatacenter information ....
Trying to retrieve vCenterCluster information ....
Certificate generated successfully.
Cluster re-registration in progress ....
Cluster re-registered successfully.
root@HyperFlex-Installer:~#
```

## サンプルのネットワーク エラー

```
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-1.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
```

# Changing ESXi Host Root Password

You can change the default ESXi password for the following scenarios:

- During creation of a standard and stretch cluster (supports only converged nodes)
- During expansion of a standard cluster (supports both converged or compute node expansion)
- During Edge cluster creation

**Note** In the above cases, the ESXi root password is secured as soon as installation is complete. In the event a subsequent password change is required, the procedure outlined below may be used after installation to manually change the root password.

As the ESXi comes up with the factory default password, you should change the password for security reasons. To change the default ESXi root password post-installation, do the following.

**Note** If you have forgotten the ESXi root password, for password recovery please contact Cisco TAC.

**Procedure**

ステップ **1** Log in to the ESXi host service control using SSH.

ステップ **2** Acquire root privileges.

```
su -
```

ステップ **3** Enter the current root password.

ステップ **4** Change the root password.

```
passwd root
```

ステップ **5** Enter the new password, and press **Enter**. Enter the password a second time for confirmation.

**Note** If the password entered the second time does not match, you must start over.

# Changing Storage Controller Password

To reset the HyperFlex storage controller password post-installation, do the following.

### Procedure

ステップ 1 Log in to a storage controller VM.

ステップ 2 Change the Cisco HyperFlex storage controller password.

```
# stcli security password set
```

This command applies the change to all the controller VMs in the storage cluster.

**Note** If you add new compute nodes and try to reset the cluster password using the **`scli security password set`** command, the converged nodes get updated, but the compute nodes may still have the default password. To change the compute node password, use the following procedure.

To change the password on compute nodes:

**a.** Vmotion all the user VMs off the ESXi hosts.

**b.** Launch the storage controller VM console from vCenter and log in as the root user.

**c.** Run the **`passwd`** command to change the password.

**d.** Log out and re-login to confirm that the password changed successfully.

**e.** Run the **`stcli node add -f`** command to add the node back into the cluster.

ステップ 3 Type in the new password.

ステップ 4 Press **Enter**.

# 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。

### 手順

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、**[vSphere Web Client にログイン (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 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。

### 手順

**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。

### 手順

**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。[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。

# Auto Support and Smart Call Home for HyperFlex

You can configure the HX storage cluster to send automated email notifications regarding documented events. You can use the data collected in the notifications to help troubleshoot issues in your HX storage cluster.

**Note** Auto Support (ASUP) and Smart Call Home (SCH) support the use of a proxy server. You can enable the use of a proxy server and configure proxy settings for both using HX Connect.

### Auto Support (ASUP)

Auto Support is the alert notification service provided through HX Data Platform. If you enable Auto Support, notifications are sent from HX Data Platform to designated email addresses or email aliases that you want to receive the notifications. Typically, Auto Support is configured during HX storage cluster creation by configuring the SMTP mail server and adding email recipients.

**Note** Only unauthenticated SMTP is supported for ASUP.

If the **Enable Auto Support** check box was not selected during configuration, Auto Support can be enabled post-cluster creation using the following methods:

| Post-Cluster ASUP Configuration Method | Associated Topic |
|---|---|
| HX Connect user interface | Configuring Auto Support Using HX Connect, on page 9 |
| Command Line Interface (CLI) | Configuring Notification Settings Using CLI, on page 10 |
| REST APIs | Cisco HyperFlex Support REST APIs on Cisco DevNet. |

Auto Support can also be used to connect your HX storage cluster to monitoring tools.

### Smart Call Home (SCH)

Smart Call Home is an automated support capability that monitors your HX storage clusters and then flags issues and initiates resolution before your business operations are affected. This results in higher network availability and increased operational efficiency.

Call Home is a product feature embedded in the operating system of Cisco devices that detects and notifies the user of a variety of fault conditions and critical system events. Smart Call Home adds automation and convenience features to enhance basic Call Home functionality. After Smart Call Home is enabled, Call Home messages/alerts are sent to Smart Call Home.

Smart Call Home is included with many Cisco service contracts and includes:

- Automated, around-the-clock device monitoring, proactive diagnostics, real-time email alerts, service ticket notifications, and remediation recommendations.
- Proactive messaging sent to your designated contacts by capturing and processing Call Home diagnostics and inventory alarms. These email messages contain links to the Smart Call Home portal and the TAC case if one was automatically created.
- Expedited support from the Cisco Technical Assistance Center (TAC). With Smart Call Home, if an alert is critical enough, a TAC case is automatically generated and routed to the appropriate support team through `https`, with debug and other CLI output attached.
- Customized status reports and performance analysis.
- Web-based access to: all Call Home messages, diagnostics, and recommendations for remediation in one place; TAC case status; and up-to-date inventory and configuration information for all Call Home devices.

To ensure automatic communication among your HX storage cluster, you, and Support, see Configuring Smart Call Home for Data Collection, on page 11.

# Configuring Auto Support Using HX Connect

Typically, Auto Support (ASUP) is configured during HX storage cluster creation. If it was not, you can enable it post cluster creation using the HX Connect user interface.

### Procedure

ステップ 1 Log in to HX Connect.

ステップ 2 In the banner, click **Edit settings (gear icon)** > **Auto Support Settings** and fill in the following fields.

| UI Element | Essential Information |
|---|---|
| **Enable Auto Support (Recommended)** check box | Configures Call home for this HX storage cluster by enabling:<br>• Data delivery to Cisco TAC for analysis.<br>• Notifications from Support as part of proactive support. |
| **Send service ticket notifications to** field | Enter the email address that you want to receive the notifications. |

| UI Element | Essential Information |
|---|---|
| **Terms and Conditions** check box | End user usage agreement. The check box must be checked to use the Auto-Support feature. |
| **Use Proxy Server** check box | • **Web Proxy Server** url<br>• **Port**<br>• **Username**<br>• **Password** |

ステップ 3 Click **OK**.

ステップ 4 In the banner, click **Edit settings (gear icon)** > **Notifications Settings** and fill in the following fields.

| UI Element | Essential Information |
|---|---|
| **Send email notifications for alarms** check box | If checked, fill in the following fields:<br>• **Mail Server Address**<br>• **From Address**—Enter the email address used to identify your HX storage cluster in Support service tickets, and as the sender for Auto Support notifications. Support information is currently not sent to this email address.<br>• **Recipient List (Comma separated)** |

ステップ 5 Click **OK**.

# Configuring Notification Settings Using CLI

Use the following procedure to configure and verify that you are set up to receive alarm notifications from your HX storage cluster.

**Note** Only unauthenticated SMTP is supported for ASUP.

### Procedure

ステップ 1 Log in to a storage controller VM in your HX storage cluster using `ssh`.

ステップ 2 Configure the SMTP mail server, then verify the configuration.

Email address used by the SMTP mail server to send email notifications to designated recipients.

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

Example:

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

**ステップ 3** Enable ASUP notifications.

```
# stcli services asup enable
```

**ステップ 4** Add recipient email addresses, then verify the configuration.

List of email addresses or email aliases to receive email notifications. Separate multiple emails with a space.

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

Example:

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

**ステップ 5** From the controller VM that owns the eth1:0 IP address for the HX storage cluster, send a test ASUP notification to your email.

```
# sendasup -t
```

To determine the node that owns the eth1:0 IP address, log in to each storage controller VM in your HX storage cluster using `ssh` and run the `ifconfig` command. Running the `sendasup` command from any other node does not return any output and tests are not received by recipients.

**ステップ 6** Configure your email server to allow email to be sent from the IP address of all the storage controller VMs.

# Configuring Smart Call Home for Data Collection

Data collection is enabled by default but, during installation, you can opt-out (disable). You can also enable data collection post cluster creation. During an upgrade, Smart Call Home is set up based on your legacy configuration. For example, if `stcli services asup show` is enabled, Smart Call Home is enabled on upgrade.

Data collection about your HX storage cluster is forwarded to Cisco TAC through `https`. If you have a firewall installed, configuring a proxy server for Smart Call Home is completed post cluster creation.

**Note** In HyperFlex Data Platform release 2.5(1.a), Smart Call Home Service Request (SR) generation does not use a proxy server.

Using Smart Call Home requires the following:

- A Cisco.com ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.
- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

### Procedure

ステップ 1 Log in to a storage controller VM in your HX storage cluster.

ステップ 2 Register your HX storage cluster with Support.

Registering your HX storage cluster adds identification to the collected data and automatically enables Smart Call Home. To register your HX storage cluster, you need to specify an email address. After registration, this email address receives support notifications whenever there is an issue and a TAC service request is generated.

**Note** Upon configuring Smart Call Home in Hyperflex, an email will be sent to the configured address containing a link to complete registration. If this step is not completed, the device will remain in an inactive state and an automatic Service Request will not be opened.

Syntax:

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

Example:

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

ステップ 3 Verify data flow from your HX storage cluster to Support is operational.

Operational data flow ensures that pertinent information is readily available to help Support troubleshoot any issues that might arise.

`--all` option runs the commands on all the nodes in the HX cluster.

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

If you upgraded your HX storage cluster from HyperFlex 1.7.1 to 2.1.1b, also run the following command:

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

Contact Support if you receive the following error:

```
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 (Optional) Configure a proxy server to enable Smart Call Home access through port 443.

If your HX storage cluster is behind a firewall, after cluster creation, you must configure the Smart Call Home proxy server. Support collects data at the `url: https://diag.hyperflex.io:443` endpoint.

**a.** Clear any existing registration email and proxy settings.

```
# stcli services sch clear
```

**b.** Set the proxy and registration email.

Syntax:

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

**Syntax Description**

| Option | Required or Optional | Description |
|---|---|---|
| **--email EMAILADDRESS** | Required. | Add an email address for someone to receive email from Cisco support. Recommendation is to use a distribution list or alias. |
| **--enable-proxy ENABLEPROXY** | Optional. | Explicitly enable or disable use of proxy. |
| **--portal-url PORTALURL** | Optional. | Specify an alternative Smart Call Home portal URL, if applicable. |
| **--proxy-url PROXYURL** | Optional. | Specify the HTTP proxy URL, if applicable. |
| **--proxy-port PROXYPORT** | Optional. | Specify the HTTP proxy port, if applicable. |
| **--proxy-user PROXYUSER** | Optional. | Specify the HTTP proxy user, if applicable.<br>Specify the HTTP proxy password, when prompted. |

Example:

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

**c.** Ping to verify the proxy server is working and data can flow from your HX storage cluster to the Support location.

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

`--all` option runs the command on all the nodes in the HX cluster.

**ステップ 5** Verify Smart Call Home is enabled.

When Smart Call Home configuration is `set`, it is automatically enabled.

```
# stcli services sch show
```

If Smart Call Home is disabled, enable it manually.

```
# stcli services sch enable
```

**ステップ 6** Enable Auto Support (ASUP) notifications.

Typically, Auto Support (ASUP) is configured during HX storage cluster creation. If it was not, you can enable it post cluster creation using HX Connect or CLI.

# 自己署名の証明書を CA 署名の証明書で置き換える

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、可能であればCIP ノードからのものから、CSR (証明書署名のリクエスト) を生成します。必要となるのは 1 つの CSR だけです。各 CVM には同じ証明書をインストールする必要があるからです。CSR を生成するときには、管理CIP に割り当てられたホスト名を、対象の識別名の共通名として入力します。

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 証明書を取得したら、自動化スクリプトを使用して証明書をインポートします。このスクリプトは、その CVM の証明書のみをアップデートします。

（注） クラスタ展開では、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。

### 手順

**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。

```
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、CSR リクエストを生成するためのコマンドを実行します。

```
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 から証明書 (.crt ファイル) を受け取ったら、各 CVM に証明書とキーをコピーします。

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

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

**ステップ 5** キーへのパスを入力します: /etc/ssl/private/<CVM のホスト名>.key

**ステップ 6** 証明書のパスを証明書形式で入力します: <CA .crt ファイルへのパス>

（注） すべての入力を終えた後、インポートプロセスを完了するにはしばらくかかります。

**ステップ 7** CIP を指している CVM から、**stcli reregister** コマンドを実行して vCenter にクラスタを再登録します。証明書がインポートされたら、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、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 （16 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

### 手順

**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。

### 手順

**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

### 手順

**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

**手順**

**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** [閉じる（Close）] をクリックします。

# vSphere 分散スイッチの作成

**手順**

**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** [完了（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

### 手順

**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 を右クリックします。

**ステップ 3** [Edit Settings] をクリックします。

**ステップ 4** [Private VLAN] タブを選択します。

**ステップ 5** [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** [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** [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。

- **[Isolated]**
- **[Community]**
- **無差別**(デフォルト)

**ステップ 8** [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。

### 手順

**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。

| 手順 | 操作 | 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 |
| 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。 | — |