



ストレッチ クラスタ アップグレード

- [概要 \(1 ページ\)](#)
- [ストレッチ クラスタのアップグレードのガイドライン \(2 ページ\)](#)
- [HX Connect を使用した HyperFlex ストレッチ クラスタのアップグレード \(2 ページ\)](#)
- [HXDP リリース 5.0\(x\) 以前の監視 VM のアップグレード \(4 ページ\)](#)
- [Cisco HyperFlex ストレッチ クラスタの ESXi の手動アップグレード \(7 ページ\)](#)
- [UCS FW アップグレード用のストレッチ クラスタの設定 \(8 ページ\)](#)

概要

このセクションでは、Cisco HyperFlex ストレッチ クラスタのアップグレードに関連する情報を示します。ストレッチ クラスタのアップグレードを実行する手順は、通常の HyperFlex クラスタのアップグレード手順と似ています。

Cisco HyperFlex ストレッチ クラスタのアップグレードプロセスでは、次の3つのコンポーネントがアップグレードされます。

- Cisco HyperFlex データ プラットフォーム
- VMware vSphere ESXi
- Cisco UCS サーバ ファームウェア

HyperFlex データプラットフォームと VMware ESXi のアップグレードを組み合わせると、HyperFlex ストレッチ クラスタの単一のアップグレードにすることができます。シスコでは、HyperFlex Connect からのこれら2つのコンポーネントを組み合わせることを推奨しています。一度に1つまたは2つのコンポーネントをアップグレードすることを選択できます。

個々のコンポーネントを1つずつアップグレードする場合は、[UCS ファームウェア](#)、[HX Data Platform](#) および [VMware vSphere のアップグレード：個別コンポーネントのアップグレード](#) を参照してください。標準クラスタと HyperFlex ストレッチ クラスタのコンポーネントアップグレードプロセスは同じです。

このセクションでは、HyperFlex データプラットフォームと VMware vSphere ESXi の複合アップグレードを実行する手順について説明します。このプロセスでは、HyperFlex ノードは、

VMware vMotion を使用してワークロードを中断することなく、最適化されたローリングリブートを実行します。

ストレッチ クラスタのアップグレードのガイドライン



重要 HyperFlex ストレッチ クラスタを HXDP 5.0(2b) にアップグレードしないでください。ソフトウェア アドバイザリを参照してください。 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/sw-advisory-hyperflex-release-5-0-2b.html

- UCS サーバーファームウェアのアップグレードは、HX コネクトを通じてサポートされていません。UCS ファームウェアのアップグレードは、Cisco UCS Manager を使用して手動で行う必要があります。 [Cisco UCS Manager によるファームウェアの管理](#) を参照してください。
- HyperFlex Witness ノードのアップグレードは、ストレッチ クラスタをアップグレードするときには必要ありませんが、強く推奨されます。使用可能な最新の監視バージョンについては、 [\[Cisco HyperFlex ソフトウェアの要件と推奨事項 \(Cisco HyperFlex Software Requirements and Recommendations\)\]](#) を参照してください。
- 正常性チェック：アップグレードする前に、Hypercheck クラスタでこのプロアクティブな正常性チェックを実行することを推奨します。詳細については、 [アップグレード前の Intersight 正常性チェック](#) を参照してください。

HX Connect を使用した HyperFlex ストレッチ クラスタのアップグレード

始める前に

- アップグレード前の検証チェックを完了します。
- 既存のクラスタを以前のリリースからアップグレードするための最新の *Cisco HX Data Platform Upgrade Bundle* を [\[Software Download\]](#) から、ダウンロードします。
- [Cisco UCS インフラストラクチャ](#) をアップグレードします。
- UCS サーバーファームウェアのアップグレード詳細については、 [Cisco UCS Manager によるファームウェアの管理](#) を参照してください。
- ストレージコントローラ VM でスナップショットスケジュールを無効にします。HyperFlex クラスタ IP に SSH 接続し、 `stcli snapshot-schedule --disable snapshot schedule` コマンドを実行します。
- DRS が有効な場合、VM は自動的に vMotion を持つ他のホストに移行されます。



(注) DRSが無効に設定されている場合は、VMに対して手動でvMotionを実行して、アップグレードプロセスを続行します。詳細については、VMwareのマニュアルで、vMotionを使用した移行の説明を参照してください。

ステップ 1 HX Connect にログインします。

- a) 管理者ユーザのユーザ名とパスワードを入力します。
- b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[アップグレード タイプの選択 (Select Upgrade Type)]** ページで **[HX Data Platform]** および **[ESXi]** を選択し、次のフィールドの値を入力します。

ステップ 4 **[Select Upgrade Type]** ページで **[HX Data Platform]** を選択し、次のフィールドの値を入力します。

UI 要素	[基本情報 (Essential Information)]
HX ファイルをここにドラッグするか、または [参照] をクリックします	「 Download Software : HyperFlex HX Data Platform 」から、前の release.tgz パッケージを使用した既存のクラスタをアップグレードするための Cisco HyperFlex Data Platform アップグレードバンドルをアップロードします。 サンプルファイル名の形式: storfs-packages-4.5.1a-31601.tgz
現在のバージョン	現在の HyperFlex Data Platform バージョンが表示されます。
現在のクラスタの詳細	HyperFlex バージョン および クラスタ アップグレード状態 のような HyperFlex クラスタの詳細がリストされます。
Bundle version	アップロードされたバンドルの HyperFlex Data Platform バージョンが表示されます。
(任意) [チェックサム (Checksum)] フィールド	MD5 チェックサム番号は、Cisco.com のソフトウェア ダウンロードセクションのファイル名にカーソルを合わせてホバーさせると表示されます。 このオプションステップは、アップロードされたアップグレードパッケージバンドルの整合性を検証するのに役立ちます。

ステップ 5 VMware ESXi カスタム イメージのオフライン アップグレードバンドルをアップロードします。

ステップ 6 vCenter ログイン情報を指定します。

基本情報 (Essential Information)	基本的な情報
[ユーザ名 (User Name)] フィールド	vCenter <admin> ユーザ名を入力します。
[Admin Password] フィールド	vCenter <admin> パスワードを入力します。

ステップ 7 [アップグレード (Upgrade)] をクリックして、複合アップグレードプロセスを開始します。

ステップ 8 [アップグレードの進行状況 (Upgrade Progress)] ページの [Validation Screen] に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。

(注) この時点で、すべてのアップグレード前のチェックと検証が、最初のアップグレード段階とともに実行されます。数分以内に HX Connect が返され、アップグレードの確認と開始を求めるプロンプトが表示されます。両方の手順が UI で実行されるまで、アップグレードは完了しません。システムは、アップグレードの最初のステップのみが完了した状態のままにしないでください。

ステップ 9 HyperFlex Connect の UI は、アップグレードの最初のステップの後に更新され、UCS および vCenter のクレデンシャルを入力してアップグレードプロセスの第 2 段階を開始するように求めるバナーがポップアップ表示されます。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、「**Websocket の接続が失敗しました**」というメッセージが表示される場合があります。自動更新が無効になりました。エラーメッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラーメッセージは問題なく無視することができます。

(注) アップグレードが完了したら、アップグレード後のタスクを実行します。アップグレードが失敗した場合は、アップグレードを再試行するか、Cisco TAC に連絡してサポートを受けてください。

HXDP リリース 5.0(x) 以前の監視 VM のアップグレード

始める前に



注目 このワークフローは、既存のストレッチクラスタインストール (HXDP リリース 5.0(x) 以前) で使用します。HXDP 5.5(1a) 以降を使用した新しいストレッチ クラスタは、サイト アービトレーション用に非表示のクラウド監視を自動構成します。非表示クラウドウィットネスは、最新のバージョンを自動的に実行します。このコンポーネントのユーザメンテナンスは必要ありません。

- アップグレードする HXDP バージョンをサポートする Witness VM バージョンを選択します。

サポートされているバージョンについては、それぞれのアップグレードのために「[\[Cisco HyperFlex ソフトウェア要件と推奨事項\]](#)」の「ストレッチ クラスタ セクションの *HX* データプラットフォーム ソフトウェア バージョンの *HyperFlex* 監視ノード」

を参照してください。

- **HyperFlex ストレッチ クラスタのアップグレード**
- アップグレードされた **HyperFlex** ストレッチ クラスタは正常な状態である必要があります。アップグレード後にストレッチ クラスタのヘルス状態を確認するには、次のコマンドを実行します。

```
root@StCtlVM:~# hxcli cluster info | grep healthy
```

ステップ 1 SSH を使用して監視 VM にログインし、次のコマンドを実行してサービス **exhibitor** を停止します。

```
root@WitnessVM:~# service exhibitor stop
```

ステップ 2 /usr/share/exhibitor/ パスで使用可能な **exhibitor** ファイルを、**exhibitor.properties** ファイルを取得できるリモートマシンにコピーします。

```
scp root@<Witness-VM-IP>:  
/usr/share/exhibitor/exhibitor.properties user@<Remote-Machine>:  
/directory/exhibitor.properties
```

ステップ 3 監視 VM からログアウトします。電源をオフにして、監視 VM の名前を **WitnessVM** に変更します。

(注) Ping を使用して、古い監視 VM の IP アドレスが到達不能であることを確認します。

ステップ 4 新しい監視 VM を展開し、古い監視 VM と同じ IP アドレスを設定します。

(注) IP アドレスに到達できない場合、監視 OVA の導入には /var/run/network ディレクトリ内の古いエントリが含まれている可能性があります。これらのエントリを手動で削除し、VM を再起動して、割り当てられた IP アドレスがネットワーク上で到達可能になるようにする必要があります。

VM をリブートするには、vCenter/vSphere で VM コンソールを開き、次のコマンドを実行します。

```
rm -rf /var/run/network/*  
reboot
```

ステップ 5 SSH を使用して新しい監視 VM にログインし、次のコマンドを実行してサービス **exhibitor** を停止します。

```
root@WitnessVM:~# service exhibitor stop
```

ステップ 6 **Exhibitor** ファイルをリモートマシン (**ステップ 2** でコピー) から新しい監視 VM の /usr/share/exhibitor/ パスにコピーします。

```
scp /directory/exhibitor.properties root@<Witness-VM-IP>:  
/usr/share/exhibitor/exhibitor.properties
```

ステップ 7 次のシンボリック リンクが新しい監視 VM に保持されているかどうかを確認します。

```

root@Cisco-HX-Witness-Appliance:~# cd /etc/exhibitor/
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al
total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties

```

シンボリック リンクが使用できない場合は、次のコマンドを実行します。

```

root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln
-s /usr/share/exhibitor/exhibitor.properties exhibitor.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln -s /usr/share/
exhibitor/log4j.properties log4j.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties
-> /usr/share/exhibitor/exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties
-> /usr/share/exhibitor/log4j.pr

```

ステップ 8 重要 バージョン 4.5(2a) より前の HX リリースにアップグレードする場合は、この手順をスキップします。

コントローラー VM の /etc/springpath/clusteruuid ファイルからクラスタ UUID 値を取得し、/usr/share/zookeeper/conf/server.jaas.conf を編集して、HX_PLACEHOLDER をクラスタ UUID に置き換えます。

例：

```

On any Storage Controller VM, get the contents of clusteruuid
file -cat /etc/springpath/clusteruuid 5b4f718033594dad:663273adab09777a
On the Witness VM, replace the HX_PLACEHOLDER value with the cluster
UUID -Before -QuorumServer {
  org.apache.zookeeper.server.auth.DigestLoginModule required
user_hyperflex="HX_PLACEHOLDER";};QuorumLearner {
  org.apache.zookeeper.server.auth.DigestLoginModule required
  username="hyperflex"
  password="HX_PLACEHOLDER";};
After -QuorumServer {org.apache.zookeeper.server.auth.DigestLoginModule
required user_hyperflex="5b4f718033594dad:663273adab09777a";};
QuorumLearner { org.apache.zookeeper.server.auth.DigestLoginModule
required
  username="hyperflex"
  password="5b4f718033594dad:663273adab09777a";};

```

ステップ 9 (注) この手順は、アップグレードされるウィットネス VM が 1.1.1 バージョンよりも前のバージョンの場合、Witness VM Node バージョン 1.1.1 以降に移行するユーザーに必要です。

/usr/share/exhibitor/setexhibitorconfig.sh コマンドを実行して、Witness 出展構成にアップグレードします。

(注) setexhibitorconfig.sh は、showor.properties ファイルの編集プロセスを自動化し、対応するコントローラ VM ごとに、すべてのデータ IP アドレスを管理 IP アドレスに置き換えます。

(注) 1.1.1 より古い Witness VM からアップグレードする場合、このコマンドが出力を表示しないのは正常です。

ステップ 10 次のコマンドを実行して、service exhibitor を起動します。

```
root@Cisco-HX-Witness-Appliance:~# service exhibitor start
exhibitor start/running, process <ID>
```

Cisco HyperFlex ストレッチ クラスタの ESXi の手動アップグレード

ステップ 1 いずれかのホストを選択し、vSphere Web クライアントを使用して HX メンテナンス モードにします。ホストがメンテナンス モードになったら、次の手順を実行します。

ステップ 2 SCP を使用してファイルをコピーするには、同様に、接続先 ESXi ホストの SSH サービスを開始します。

- (注)
- HX240 では、ローカルの SpringpathDS データストアまたはマウントされた HX データストアを使用できます。
 - HX220 では、マウントされた HX データストアを使用するか、一時的な RAM ディスクを作成することができます。

```
scp local_filename user@server:/path/where/file/should/go
```

ステップ 3 ESXi にログインし、次のコマンドを実行して使用可能なイメージプロファイルの一覧を照会し、プロファイル名を確認します。

```
esxcli software sources profile list -d <データストア上の ESXi zip バンドルの場所>
```

注目 esxcli ソフトウェア コマンドを使用する際はフルパスを指定する必要があります。

例 :

```
[root@localhost:~] esxcli software sources profile list -d /vmfs/volumes/5d3a21da-7f370812-ca58-0025
b5a5a102/HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10-upgrade-bundle.zip
Name                               Vendor  Acceptance Level  Creation Time
Modification Time
-----
HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10  Cisco  PartnerSupported  2019-04-02T00:14:56
2019-04-02T13:38:34
```

ステップ 4 次のコマンドを実行して、アップグレードを実行します。

```
esxcli software profile update -d <path_to_profile_ZIP_file> -p <profile name>
```

例 :

```
[root@HX-ESXi-01:/vmfs/volumes/1a234567-89bc1234] esxcli software profile update -d
/vmfs/volumes/1a234567-89bc1234/HX-Vmware-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10.zip
-p HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10
```

ステップ 5 ESXi ホストが起動したら、ホストが適切なバージョンで起動済みであることを確認します。

```
vmware -v1
```

ステップ 6 vSphere Web クライアントを使用して、メンテナンス モードを終了します。

ステップ 7 次の ESXi のアップグレードに進む前に、クラスタが正常な状態になっていることを確認します。

```
hxccli cluster info [flags]
```

ステップ 8 クラスタ内のすべてのホストに対して順番にこのプロセスを繰り返します。

(注) ESXi をアップグレードするごとに、クラスタが正常な状態であることを確認してから、次の ESXi のアップグレードに進んでください。

UCS FW アップグレード用のストレッチ クラスタの設定

アップグレード時に、次に示すカスタマイズされた UCS ポリシーが検証され、HyperFlex 用に調整されます。

- **HFP (ホストファームウェアパッケージ)** : ホストファームウェアパッケージは、HyperFlex ノードの複数のコンポーネントに一貫したファームウェア ファイルを提供します。これには、CIMC、BIOS、HBA および SAS エクスパンダファームウェア、VIC およびその他のコンポーネントが含まれます。通常の UCS ホストファームウェアパッケージとは異なり、これらのファームウェアファイルは、ディスクファームウェアも制御します。HyperFlex データプラットフォームにおいては、このことが特に重要だからです。自己暗号化ドライブ (SED) ファームウェアは、UCS マネージャポリシーではなく、HyperFlex データプラットフォームによって直接制御されることに注意してください。
- **VNIC テンプレート** : 仮想 NIC (VNIC) テンプレートは、UCS ファブリック間の VNIC の一貫した設定を提供します。HyperFlex VNIC テンプレートは、1 つの UCS ファブリック上の HyperFlex VNIC への変更がもう一方に適用されるように、冗長ペアとして設定されます。
- **イーサネットアダプタポリシー** : イーサネットアダプタポリシーは、HyperFlex VNIC のパフォーマンス関連のプロパティを提供します。
- **BIOS ポリシー** : BIOS ポリシーは、HyperFlex ノード上の主要なハードウェアリソース (CPU やメモリなど) の設定とパフォーマンスを制御します。HyperFlex は、一貫して高いパフォーマンスを提供するため、特定の設定を使用します。
- **VNIC/VHBA 配置ポリシー** : VNIC/VHBA 配置ポリシーは、特定の VNIC/VHBA の HyperFlex ノードに提供される PCI アドレスを決定します。HyperFlex はこれを一貫した方法で設定するので、さらに詳細な構成も適切に行えます。

ステップ 1 サイト上の任意の CVM に SSH で接続し、ディレクトリを /tmp に変更します。

ステップ 2 /usr/local/bin/hx.py --upgrade-cluster-config コマンドを実行します。これにより、customer_site_config.json というファイルが生成され、/tmp ディレクトリに保存されます。

ステップ3 customer_site_config.json ファイルを編集して、ファームウェアのバージョンと組織名を適切に変更します。次に例を示します。

例：

```
{
  "id": "Advanced",
  "collapse": true,
  "label": "Advanced",
  "groups": [
    {
      "id": "firmware",
      "label": "UCS Firmware",
      "items": [
        {
          "id": "version",
          "label": "UCS Firmware Version",
          "type": "text",
          "description": "UCS Firmware Version to be used on the HX servers",
          "placeholder": "ex: 3.2(2d)",
          "defaultValue": "3.2(2d)",
          "value": "4.1(1d)" #<<<<<----- Change this
        },
        {
          "id": "version-m5",
          "label": "UCS Firmware Version",
          "type": "text",
          "description": "UCS Firmware Version to be used on the M5 HX servers",
          "placeholder": "ex: 3.2(2d)",
          "defaultValue": "3.2(2d)",
          "value": "4.1(1i)" #<<<<<----- Change this
        }
      ]
    },
    {
      "id": "org",
      "items": [
        {
          "id": "name",
          "label": "Hyperflex Org name",
          "type": "text",
          "value": "Faridabad", #<<<<<----- Change this
          "description": "The name of the org in ucsd which is to be used for creation
of all the policies and profiles for this Hyperflex cluster"
        }
      ]
    }
  ]
}
```

ステップ4 コマンドを再度実行し、UCSM IP とクレデンシャルを入力します。

次に例を示します。

```
/usr/local/bin/hx.py --upgrade-cluster-config
```

例：

```
[root@SpringpathControllerVP0RX5DWTC:/# /usr/local/bin/hx.py --upgrade-cluster-config
[UCS Manager] [in_progress][ 0.00%][ETA: 0:18:00] Login to UCS API
UCS host name or virtual IP address: 10.42.17.11
Connecting to admin@10.42.17.11...
Password:
```

ステップ 5 コマンドがエラーを出さずに実行されることを確認します。エラーがあれば、Cisco TAC に連絡してください。

(注) このコマンド (`hx.py`) は、第1のサイト FI ドメインに対して実行されます。後で第2のサイト FI ドメインに対して同じ手順を実行する必要があります。

ステップ 6 vCenter および UCSM で次の手順を実行します。

- a) UCSM の保留中のアクティビティに [Pending reboot] が表示されていることを確認します。
- b) ホストをメンテナンス モードにします。
- c) サーバを再起動し、サーバがオンラインになり、クラスタがオンライン/正常になるまで待ちます。
- d) 残りのノードで同じ手順を実行します。

ステップ 7 他のサイトに対してステップ 4、5、および 6 を繰り返します。

翻訳について

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