

# バージョン 5.5 からの 6.x へのアップグレード VMware ESXi。

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

この資料に Command Line Interface ( CLI ) によってバージョン 5.5 から 6.x に伸縮性がある空 X 統合 ( ESXi ) hypervisor をアップグレードする方法を記述されています。ESXi は仮想化の顧客が好む hypervisor の 1 つで、また仮想化された環境の上を動作するすべての Unified Communication インフラストラクチャ、Sourcefire および他の複数のサーバを含む多重プラットフォームのための Cisco によって優先する hypervisor 行います。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- VMware ESXi hypervisor バージョン 5.5 が付いている Unified Computing System ( UCS )
- ESXi hypervisor へのターミナルアクセス
- Java使用可能なブラウザの Cisco Integrated Management Controller ( CIMC ) Webページへのアクセス

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Unified Computing System C460。
- ESXi hypervisor バージョン 5.5。
- Firefox ブラウザ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 背景説明

VMware は一般のサポートの端および ESXi 5.5 のための技術的な指導の終わりのための死回線を送達しました:

ESXi 5.5	.	2013/09/19	2018/09/19	2020/09/19	EP		A, B
----------	---	------------	------------	------------	----	--	------

それは ESXi 6.0 および 6.5 に仮想化されたインフラストラクチャをアップグレードする好ましい習慣です。

## 設定

CLI によるアップグレード プロセス:

ステップ 1.仮想マシン (VM) をアップグレードされるべき ESXi サーバのその実行シャットダウンして下さい。

ステップ 2.メンテナンス モードに ESXi サーバを置いて下さい。これは hypervisor がサーバが実行し、アップグレードするようにする重要なサービスを消すのを助けます。

vSphere クライアントを使用できます:

The screenshot displays the vSphere Host Configuration Manager interface. The 'General' tab is active, showing host details such as Manufacturer (Cisco Systems Inc), Model (UCSC-C460-M4), CPU Cores (72 CPUs x 2.094 GHz), Processor Type (Intel(R) Xeon(R) CPU E7-8870 v3 @ 2.10GHz), License (VMware vSphere 5 Enterprise Plus - Licensed for 4 physic...), Processor Sockets (4), Cores per Socket (18), Logical Processors (144), Hyperthreading (Active), Number of NICs (6), State (Connected), Virtual Machines and Templates (41), vMotion Enabled (Yes), VMware EVC Mode (Disabled), vSphere HA State (N/A), Host Configured for FT (No), Active Tasks, Host Profile, Image Profile ((Updated) ESXi-5.5.0-1746...), Profile Compliance (N/A), and DirectPath I/O (Supported).

The 'Commands' tab is also visible, listing several actions: New Virtual Machine, New Resource Pool, Enter Maintenance Mode (highlighted with a red box), Reboot, and Shutdown.

または CLI。 そうするために、コマンドを実行して下さい:

```
vim-cmd /hostsvc/maintenance_mode_enter
```

ステップ 3.発信 Hyper Text Transfer Protocol ( HTTP ) 接続を許可する修正する ESXi ファイアウォール。

VMware サーバが実際のアップグレード ファイルのために問い合わせられるので、ESXi サーバからの HTTP 発信接続は許可する必要があります。

vSphere クライアントを使用できます:

The screenshot shows the vSphere Configuration page. The 'Configuration' tab is selected. On the left, the 'Security Profile' is highlighted in the navigation pane. The main area displays the 'Security Profile' and 'Firewall' settings. The 'Firewall' section shows a table of incoming connections with the following data:

Incoming Connections	Port	Protocol	Access
vSphere Client	902,443	(TCP)	All
ovmsds	12345,23451	(UDP)	All
DHCP Client	68	(UDP)	All
DNS Client	53	(UDP)	All
ipfam	6999	(UDP)	All
vmanyp	8080	(TCP)	All
vMotion	8080	(TCP)	All
CEM Secure Server	5989	(TCP)	All
Fault Tolerance	8100,8200,8300	(TCP,UDP)	All

The screenshot shows the 'Firewall Properties' dialog box. The 'Remote Access' tab is selected. The dialog explains that by default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts. It instructs the user to select a check box to provide access to a service or client. The following table shows the services and their access status:

Label	Incoming Ports	Outgoing Ports	Protocols	Daemon	Access
vSphere High Availability Agent	8182	8182	TCP,UDP	Stopped	<input type="checkbox"/>
HBR		31031,44046	TCP	N/A	<input checked="" type="checkbox"/>
rdt	2233	2233	TCP	N/A	<input checked="" type="checkbox"/>
Fault Tolerance	8100,8200,8300	80,8100,8200,8300	TCP,UDP	N/A	<input checked="" type="checkbox"/>
syslog		514,1514	UDP,TCP	N/A	<input type="checkbox"/>
VMware vCenter Agent		902	UDP	Running	<input checked="" type="checkbox"/>
IKED	500	500	UDP	N/A	<input type="checkbox"/>
VM serial port connected over net...	23,1024-65535	0-65535	TCP	N/A	<input type="checkbox"/>
httpClient		80,443	TCP	N/A	<input checked="" type="checkbox"/>
ipfam	6999	6999	UDP	N/A	<input checked="" type="checkbox"/>

Below the table, the 'Service Properties' section is visible, showing 'General' and 'Firewall Settings' tabs. The 'General' tab shows 'Service: SSH Client' and 'Package Information:'. The 'Firewall Settings' tab shows 'Allowed IP Addresses: All'. At the bottom, there are buttons for 'Firewall...', 'Options...', 'OK', 'Cancel', and 'Help'.

または CLI。そうするために、コマンドを実行して下さい:

```
esxcli network firewall ruleset set -e true -r httpClient
```

ステップ 4.利用可能なアップグレードバージョンのクエリ VMware サーバ。

使用されるどれが、これをするを実行しますコマンドをこの場合すべてのアップグレード可能なバージョンは判別するためにリストすることができます:

```
esxcli software sources profile list -d
```

```
https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml |
```

```
grep ESXi-6
```

これはすべてのアップグレード可能なバージョンをリストします。非ツールバージョンはさもないければ、標準アップグレードバージョンが使用することができれば vmware ツールのアップグレードが必要とならなければ選択できます。

ステップ 5.アップグレード プロセスをアップグレードし、開始するためにバージョンを選択して下さい。

アップグレードするべきまさにそのバージョンが決定されれば、アップグレード プロセスはコマンドで開始できます:

```
esxcli software profile update -d
```

```
https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml -p
```

```
ESXi-6.0.0-20170202001-standard
```

ステップ 6.サーバをリブートして下さい。

アップグレード プロセスが完了した後、新しいバージョンが実施されることができるようサーバの再度ブートするが必要となります。コマンドを実行して下さい:

```
reboot
```

ステップ 7.終了メンテナンス モード。

ESXi ホストがオンライン、すべての VM オペレーションを回復するためにメンテナンス モードから終了して下さい。

vSphere クライアントを使用できます:



または CLI。そうするために、コマンドを実行して下さい:

```
vim-cmd /hostsvc/maintenance_mode_exit
```

## 確認

このセクションでは、設定が正常に機能していることを確認します。

アップグレードが正常に完了したことを確認するために、vSphere クライアントを使用できます。ESXi ホストおよび新しいバージョンへのナビゲートは上で見られる場合があります。または使用 CLI。そうするために、コマンドを実行して下さい:

```
vmware -v
```

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。