



バーチャル ワイヤレス LAN コントローラ 導入ガイド 8.2

[はじめに 4](#)

[8.2 の新機能 4](#)

[バーチャル ワイヤレス LAN コントローラ バージョン 8.2 のハードウェア要件 5](#)

[Cisco バーチャル ワイヤレス LAN コントローラのダウンロード 6](#)

[VMware 仮想マシン 8](#)

[UCS サーバに接続されたスイッチ インターフェイスの設定 10](#)

[vWLC OVA の導入 16](#)

[オプションの仮想コントローラ コンソール ポート 23](#)

[セットアップが簡単な vWLC 30](#)

[Linux のカーネルベース仮想マシン \(KVM\) 38](#)

[ネットワーク設定 41](#)

[Fedora に仮想マシン マネージャ \(VMM\) を使用した vWLC のインストール 43](#)

[vWLC および Ubuntu 搭載の KVM のインストール 50](#)

[VMM を使用した vWLC の起動 53](#)

[vWLC および Suse Linux 搭載のホスト Linux のインストール 54](#)

[ネットワーク設定 55](#)

[VMM を使用した vWLC のインストール 57](#)

RTU ライセンス 57

スマート ライセンス 60

Cisco Prime 3.0 搭載の仮想コントローラ管理 63

はじめに

リリース7.4以前、ワイヤレスLAN（WLAN）コントローラソフトウェアは、購入が予想される専用ハードウェアで実行されました。バーチャルワイヤレスLANコントローラ（vWLC）は、業界標準の仮想化インフラストラクチャの一般的なハードウェアで動作します。vWLCは、仮想インフラストラクチャでの小規模および中規模の導入に最適で、オンプレミスのコントローラが必要です。分散ブランチ環境は、少ないブランチ（最大 200）が必要な集中型仮想コントローラで利用することもできます。

vWLC は配布するハードウェア コントローラの代わりにはなりません。vWLC の機能は、仮想インフラストラクチャを使用したデータセンターが存在するか、または考慮されているコントローラサービスの展開の特長と利点を提供します。

vWLC の特長

- 要件に基づいたハードウェア選択の柔軟性。
- 複数のボックスが仮想アプライアンスの複数のインスタンスを実行する単一のハードウェアに置き換えられることによる、コスト削減、スペース要件などのオーバーヘッド。

8.2 の新機能

8.2 の新機能は次のとおりです。

- 1 運用の簡素化、柔軟な導入と成長に合わせた投資モデルのためにプライベート クラウドで小規模および大規模な vWLC の導入に対して拡張されたスケール サポート
 - 1 小規模 vWLC は 200 のアクセス ポイントをサポート
 - 2 大規模 vWLC は 3000 のアクセス ポイントをサポート
- 2 vWLC 用スマート ライセンスのサポート：カスタマーが所有および使用しているもののクラウド ベース ライセンスを可視化します。これにより可視性、削減された有効化の複雑さ、最適な使用率が向上します。

シスコ バーチャル WLC ではサポートされない機能（8.2.100.0 以前）

- 内部 DHCP サーバ
- TrustSec SXP
- ローカル モードのアクセス ポイント
- モビリティ/ゲスト アンカー
- マルチキャスト
- Cisco WLC と Lync SDN の統合



(注) FlexConnect ローカル スイッチ マルチキャスト トラフィックは、同じ VLAN 上の有線およびワイヤレスの両方で透過的にブリッジングされます。FlexConnect アクセス ポイントは、IGMP または MLD スヌーピングに基づいてトラフィックを制限しません。

サポートされないハイ アベイラビリティ機能

- AP SSO HA
- N+1 HA (CSCuf38985)



(注) AP は、異なる vWLC 間を移動する場合に、2 番目の vWLC への join を拒否することがあります。これは、サーバハードウェアに障害が発生しているか、vWLC の新しいインスタンスが作成される場合に発生します。vMotion などの VMware レベルまたは一部のオーケストレータで、サーバミラーリングスキームを実装することをお勧めします。アクセス ポイントが以前 join していたモビリティドメインからの、VM インスタンスのスナップショットを保持することを強くお勧めします。スナップショットを使用して、vWLC インスタンスを開始します。その後、アクセスポイントは vWLC に join します。この方法は、物理的なコントローラではなくアクセスポイントのプライミングにも使用できます。

- PMIPv6
- ワークグループブリッジ
- 中央スイッチングに対するクライアント ダウンストリーム レート制限
- SHA2 証明書

バーチャルワイヤレス LAN コントローラバージョン 8.2 のハードウェア要件

設定	小	大
vCPU の最小数	1	2
最小メモリ	2 GB	8 GB
ストレージが必要	8 GB	8 GB
VMNIC の最小数	2	2
最大のアクセス ポイント	200	3000

設定	小	大
最大のクライアント サポート	6000	32000
小規模* へのアップグレード	Yes	No
大規模* へのアップグレード	No	Yes

* アップグレードは同じプラットフォームでサポートされます。

Cisco バーチャル ワイヤレス LAN コントローラのダウンロード

最新の 8.x ソフトウェアを次からダウンロードします。 <https://software.cisco.com/download/type.html?mdfid=284464214&i=rm>



Download Software

 [Download Cart \(0 Items\)](#)
[Feedback](#)
[Help](#)

[Downloads Home](#) >
[Products](#) >
[Wireless](#) >
[Wireless LAN Controller](#) >
[Standalone Controllers](#) >
[Virtual Wireless Controller](#) >
[Wireless LAN Controller Software-8.2.100.0\(ED\)](#)

Virtual Wireless Controller

Release 8.2.100.0 ED

[Release Notes for 8.2.100.0](#)

[Add Device](#)
[Add Notification](#)

Expand All | Collapse All

- ▼ Suggested
- 8.0.120.0(ED)
- ▼ Latest
- 8.2.100.0(ED)
- 8.1.131.0(ED)
- 8.0.121.0(ED)
- 7.4.140.0(MD)
- All Releases
- Deferred Releases

File Information	Release Date	Size	
Cisco Wireless LAN Small Scale Virtual Controller upgrade. <small>AIR-CTVM-K9-8-2-100-0.aes</small>	16-DEC-2015	229.40 MB	Download Add to cart
Cisco Wireless LAN Small Scale Virtual Controller Installation with 60 day evaluation license. <small>AIR_CTVM-K9_8_2_100_0.ova</small>	16-DEC-2015	322.39 MB	Download Add to cart
Cisco Wireless LAN Large Scale Virtual Controller. <small>AIR_CTVM_LARGE-K9_8_2_100_0.aes</small>	15-DEC-2015	229.40 MB	Download Add to cart
Cisco Wireless LAN Large Scale Virtual Controller. <small>AIR_CTVM_LARGE-K9_8_2_100_0.ova</small>	15-DEC-2015	322.39 MB	Download Add to cart
Cisco Wireless LAN Small Scale Virtual Controller Installation with 60 day evaluation license (KVM). <small>MFG_CTVM_8_2_100_0.iso</small>	15-DEC-2015	322.30 MB	Download Add to cart
Cisco Wireless LAN Large Scale Virtual Controller Installation with 60 day evaluation license (KVM). <small>MFG_CTVM_LARGE_8_2_100_0.iso</small>	16-DEC-2015	322.30 MB	Download Add to cart

ソフトウェアリリース 8.2 では、バーチャルワイヤレスコントローラは、2種類の展開「小規模」または「大規模」で、*.aes（ソフトウェアアップグレード）または*.ova（VMware）または*.iso（KVM）形式で提供されます。ターゲットの導入をサポートするのに必要なハードウェア要件を参照してください。

ソフトウェアアップグレードは*.aes形式です。

小規模 Cisco ワイヤレス LAN バーチャル コントローラのアップグレード

AIR-CTVM-K9-8-2-100-0.aes

大規模 Cisco ワイヤレス LAN バーチャル コントローラ

AIR_CTVM_LARGE-K9_8_2_100_0.aes

既存の vWLC をアップグレードするには、*.aes ソフトウェアを使用して、WLC の通常のアップグレードプロセスを実行します。



(注) vWLCのアップグレードは、同じタイプ（たとえば、小規模から小規模、大規模から大規模）のみをサポートします。混合はサポートされません（たとえば、小規模から大規模、または大規模から小規模）。

Download file to Controller	
File Type	Code
Transfer Mode	TFTP
Server Details	
IP Address(Ipv4/Ipv6)	10.10.105.99
Maximum retries (1 to 254)	10
Timeout (1 to 254 seconds)	6
File Path	/
File Name	AS_CTVM_SMALL_8_2_1_128.aes

VMware で新しいバーチャル ワイヤレス コントローラをインストールする場合、*.ova を使用します。

60 日間の評価ライセンスを備えた小規模 Cisco ワイヤレス LAN バーチャル コントローラのインストール

AIR_CTVM-K9_8_2_100_0.ova

大規模 Cisco ワイヤレス LAN バーチャル コントローラ

AIR_CTVM_LARGE-K9_8_2_100_0.ova

KVM に新しいバーチャル ワイヤレス コントローラをインストールする場合、*.iso を使用します。

60 日間の評価ライセンスを備えた小規模 Cisco ワイヤレス LAN バーチャル コントローラのインストール (KVM)

MFG_CTVM_8_2_100_0.iso

60 日間の評価ライセンスを備えた大規模 Cisco ワイヤレス LAN バーチャル コントローラのインストール (KVM)

MFG_CTVM_LARGE_8_2_100_0.iso

VMware 仮想マシン

このドキュメントは、CUWN 8.2 ソフトウェア リリースに基づいた vWLC と VMware ESX のサポートについて更新されています。VMware は、シスコ ワイヤレス リリース 7.4 以降のリリースでサポートされます。

ホスティング バーチャル ワイヤレス LAN コントローラ (vWLC) の VMware 前提条件

次は、ホスティング vWLC の VMware 前提条件です。

- 最小で 2 G (小) または 8 G (大) のメモリ

- 最小で1つの vCPU (小) または2つの vCPU (大)
- 最小で2つのネットワーク インターフェイス
- 8 G のストレージが必要

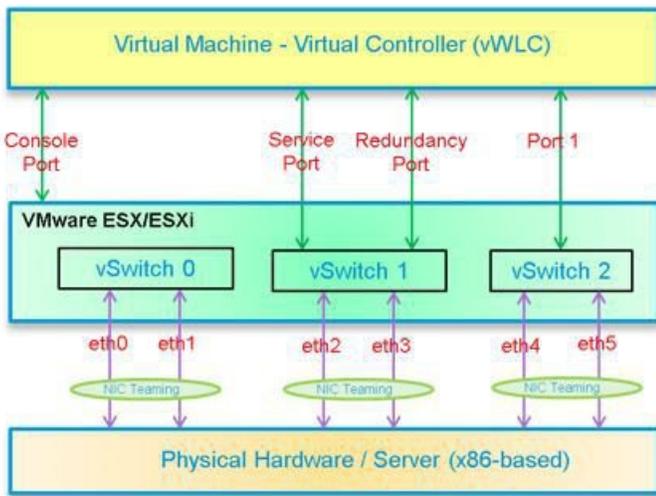
ESXi では、vWLC をサポートするのに必要な適切なネットワーキングを設定します。Dataport のトランク、および次の例のようなサービス ポート* のオプションのアクセス ポートを使用することを推奨します。



(注) * vWLC サービス ポートは、Cisco WLC の初期を簡素化した (または 0 日のコントローラ プロビジョニング設定) 機能を有効化するために使用できます。これは、クライアントブラウザを使用し、手順の最小設定に従って代替設定を提供します。簡素化された設定を使用することによって、RF パラメータ最適化などのベスト プラクティスのデフォルトおよびネットワーク プロファイルを有効にします。

仮想コントローラの仮想インターフェイス

- 管理インターフェイス
- 仮想インターフェイス
- 動的インターフェイス
- AP マネージャ インターフェイス



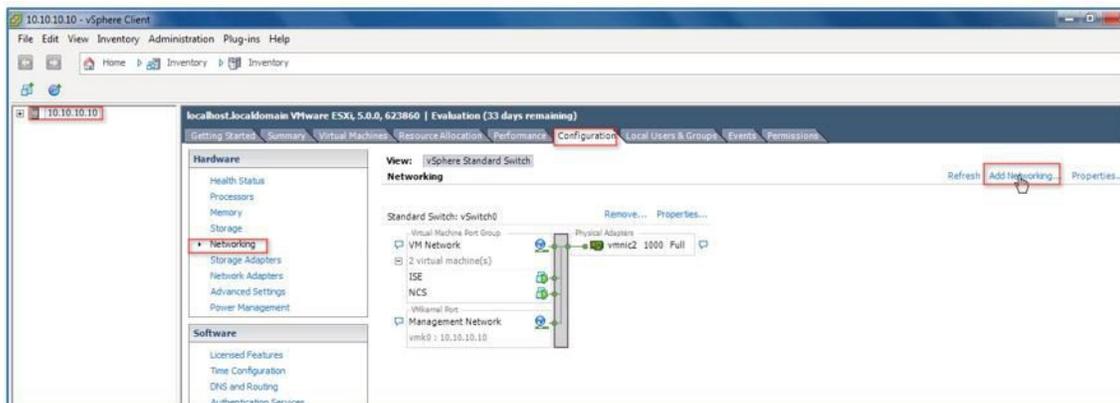
UCS サーバに接続されたスイッチ インターフェイスの設定

トランク インターフェイスとしての仮想スイッチ用 ESXi サーバへの Cisco Catalyst インターフェイス接続の設定例。管理インターフェイスは、スイッチのアクセスポートに接続できます。

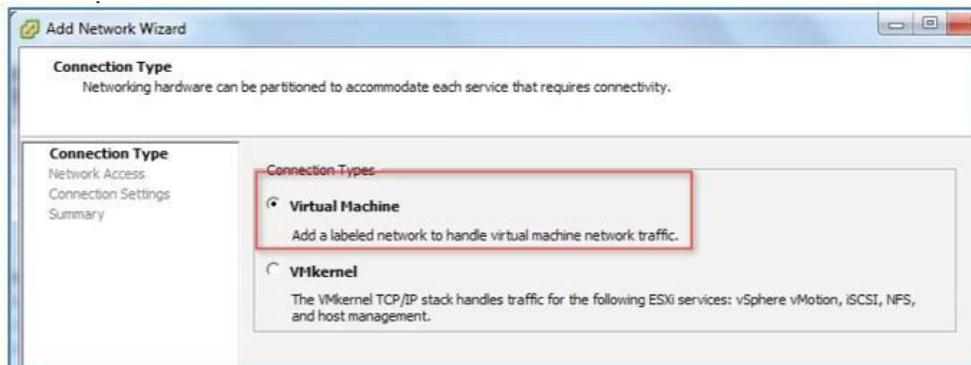
```
interface GigabitEthernet1/1/2
description ESXi Management
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/1/3
description ESXi Trunk
switchport trunk encapsulation dot1q
switchport mode trunk
end
```

手順

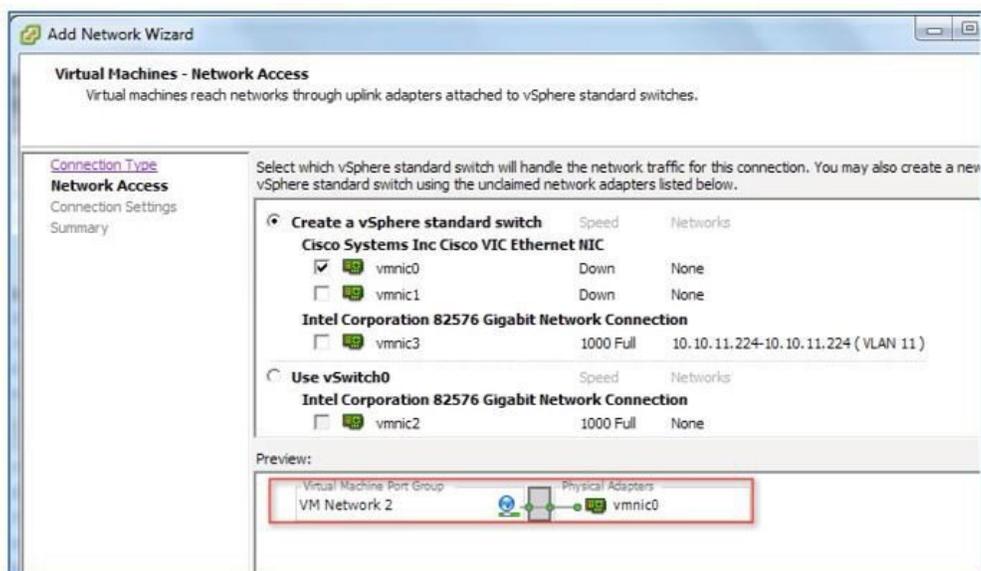
ステップ 1 仮想コントローラ サービスとデータポートにマッピングするために2つの別個の仮想スイッチを作成します。[ESX] > [Configuration] > [Networking] に移動し、[Add Networking] をクリックします。



ステップ2 [Virtual Machine] を選択し、[Next] をクリックします。



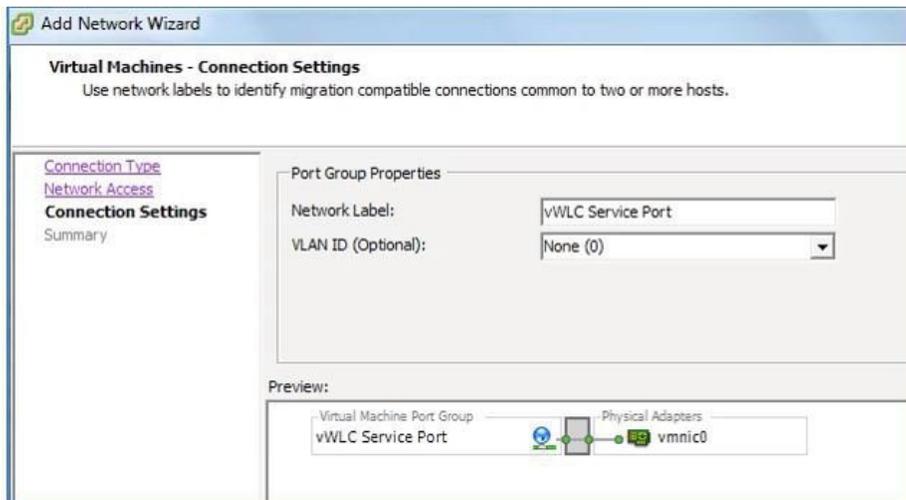
ステップ3 vSwitch を作成し、vWLC サービス ポートに接続するために物理 NIC を割り当てます。サービス ポートは、ネットワークの部分に接続する必要がない（通常、切断されているか使用されていない）ため、どの NIC でも（切断されていても）vSwitch に使用できます。



ステップ4 [Next] をクリックして続行します。

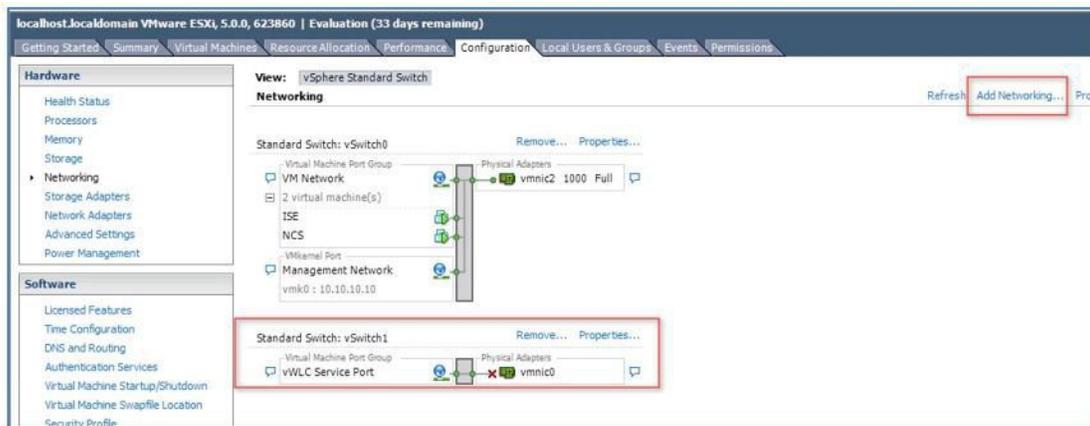
ステップ5 ラベルを、次の例のように指定します。
例「vWLC Service Port」。

ステップ6 通常、サービス ポートはアクセス ポートであるため、VLAN ID に「None (0)」を選択します。



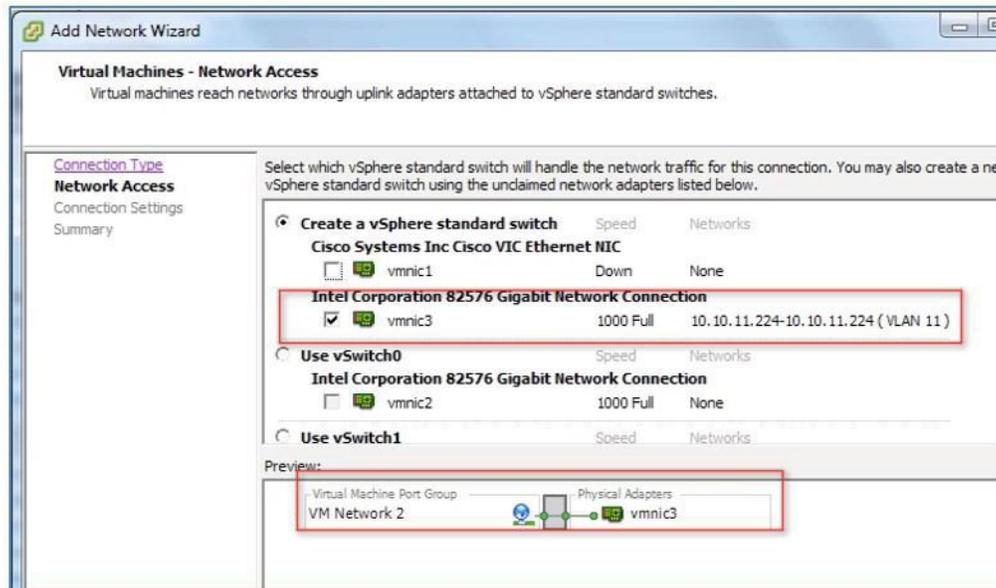
ステップ7 [Next] をクリックして続行します。

ステップ8 下のスクリーンショットでは、「vWLC Service Port」に vSwitch1 が作成されたことがわかります。データポートの繰り返しには、[Add Networking] をクリックします。



新しい vSwitch の場合、スイッチの EtherChannel に複数の NIC またはポート グループが割り当てられている場合は、トランク ポートに接続された物理 NIC を選択します。

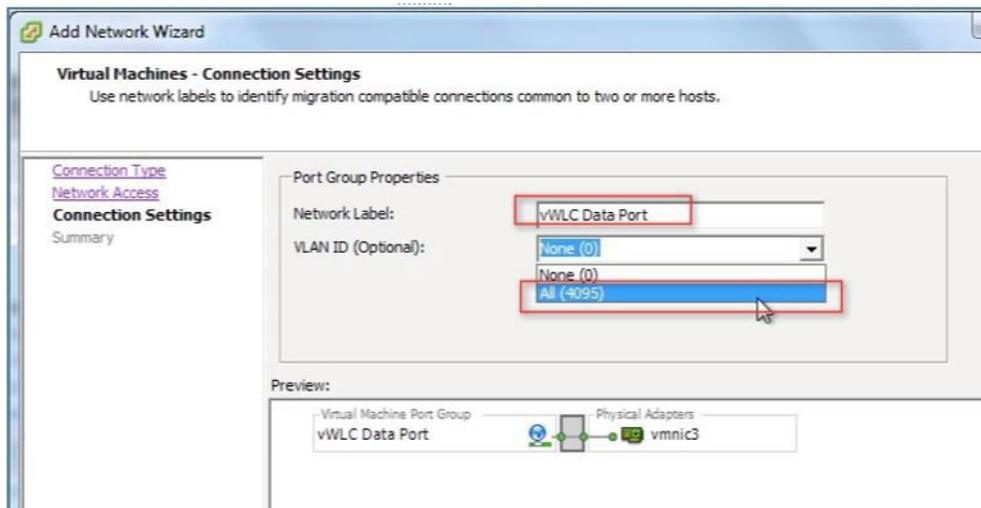
ステップ9 NIC を追加します。



ステップ 10 [Next] をクリックして続行します。

ステップ 11 ラベルを指定します。例「vWLC Data Port」。

ステップ 12 VLAN ID の場合、これがスイッチ トランク ポートに接続されるため、[ALL(4095)] を選択します。



ステップ 13 vSwitch を追加するための手順を完了するまで [Next] をクリックします。

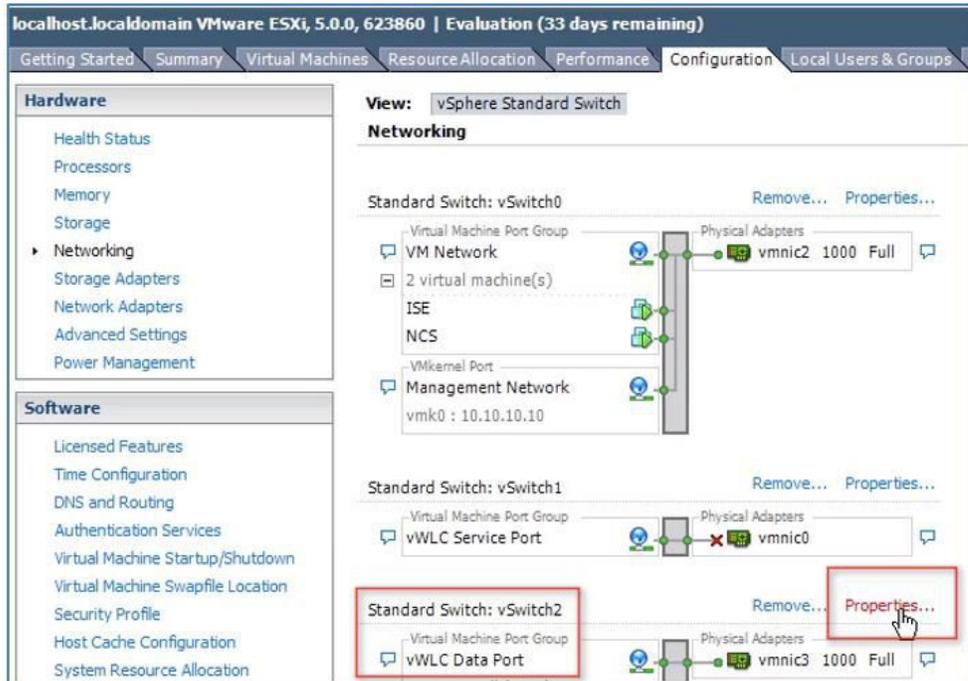
VMware 無差別モード定義：無差別モードは、vSphere ESX/ESXi の仮想スイッチまたはポートグループレベルで定義できるセキュリティポリシーです。無差別モードの使用が可能なポートグループの仮想マシン、サービス コンソールまたは VM カーネル ネットワーク インターフェイスは、仮想スイッチを通過するすべてのネットワーク トラフィックを表示できます。

デフォルトでは、ゲストオペレーティングシステムの仮想ネットワークアダプタは、用意されたフレームのみを受信します。無差別モードでゲストネットワークアダプタを配置すると、関連のポートグループの VLAN ポリシーで割り当てられた仮想スイッチで渡されるすべてのフレームを受信します。これ

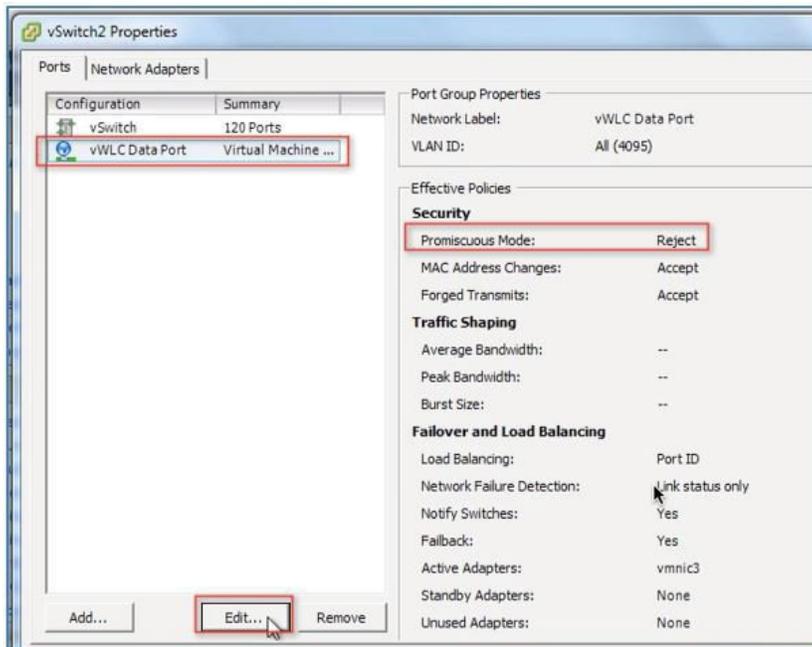
は、侵入検知モニタリングに、またはスニファがネットワークセグメントのすべてのトラフィックを分析する必要がある場合に、役立つことがあります。

vWLC データ ポートでは、割り当てられた vSwitch が正しい動作の無差別モードを受け入れる必要があります。

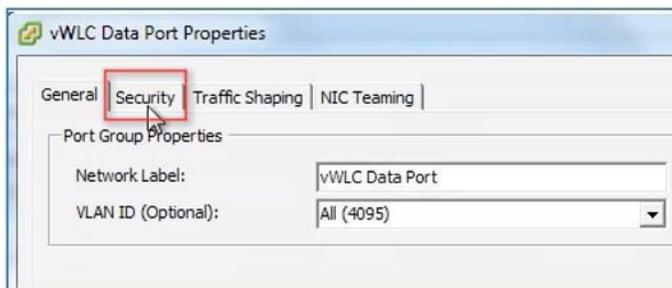
ステップ 14 (vWLC のデータ ポートに割り当てられた) vSwitch2 を配置し、[Properties] をクリックします。



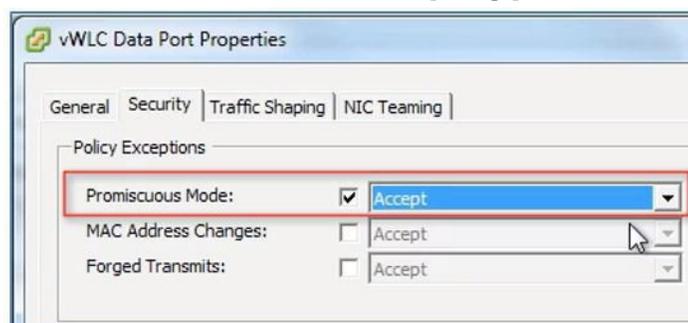
ステップ 15 vWLC データ ポートに割り当てられた VMNet を選択します。デフォルトのセキュリティ無差別モードを [Reject] に設定し、[Edit] をクリックしてください。



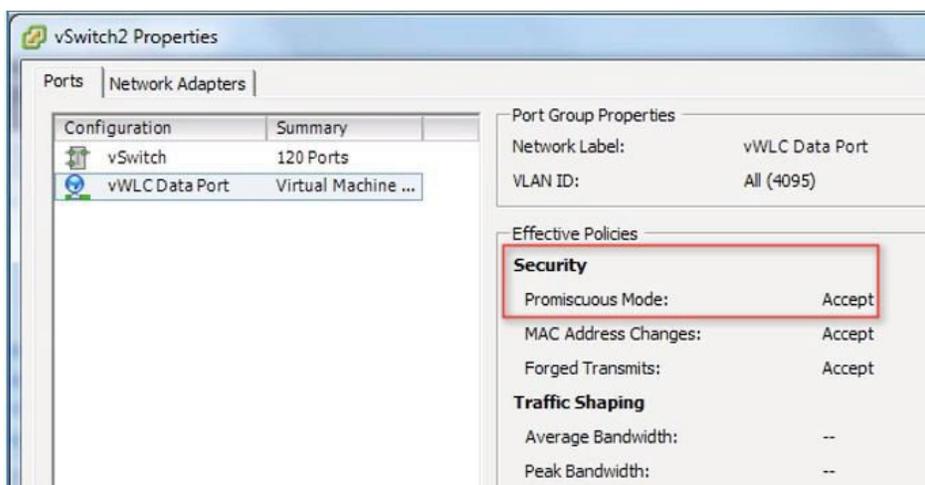
ステップ 16 プロパティでは、[Security] タブを選択します。



ステップ 17 無差別モードのボックスを確認し、[Accept] を選択します。[OK] をクリックします。



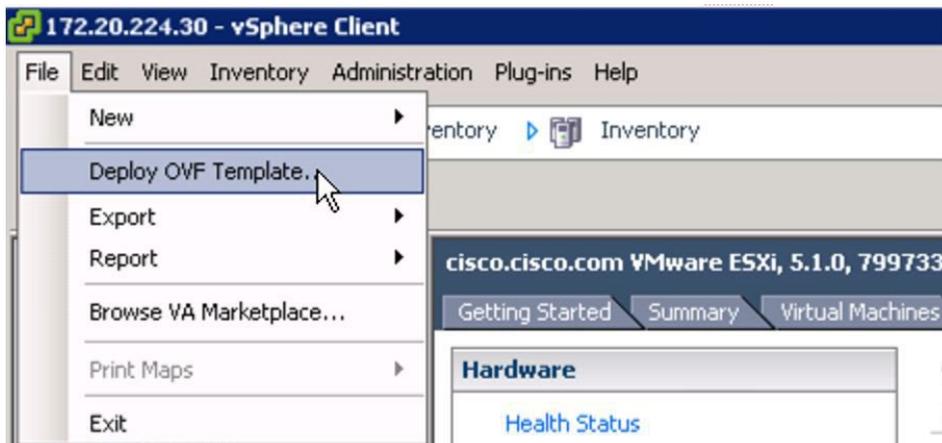
ステップ 18 変更を確認し、[Close] をクリックして続行します。



仮想コントローラのソフトウェアは Cisco Software Center に .ova パッケージとして転記されます。カスタマーは、.ova パッケージをダウンロードし、他の仮想アプリケーションと同様にインストールできます。ソフトウェアには、60 日間の評価ライセンスが付属しています。VM を起動すると、評価ライセンスを有効化し、後で、購入したライセンスを自動的にインストールして有効化することができます。

ステップ 19 ローカルディスクに、仮想コントローラ OVA イメージをダウンロードします。

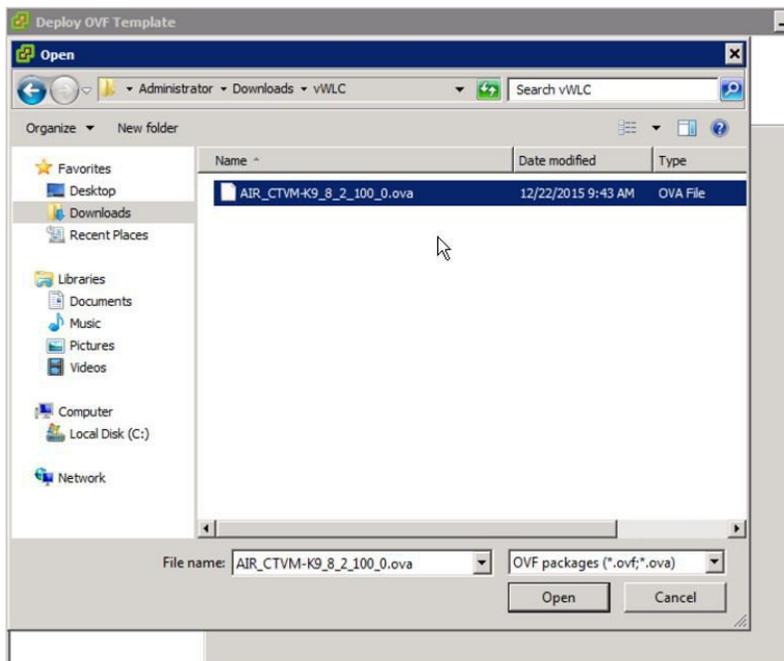
ステップ 20 [vSphere client] > [Deploy OVF Template] を使用して、vWLC を導入します。



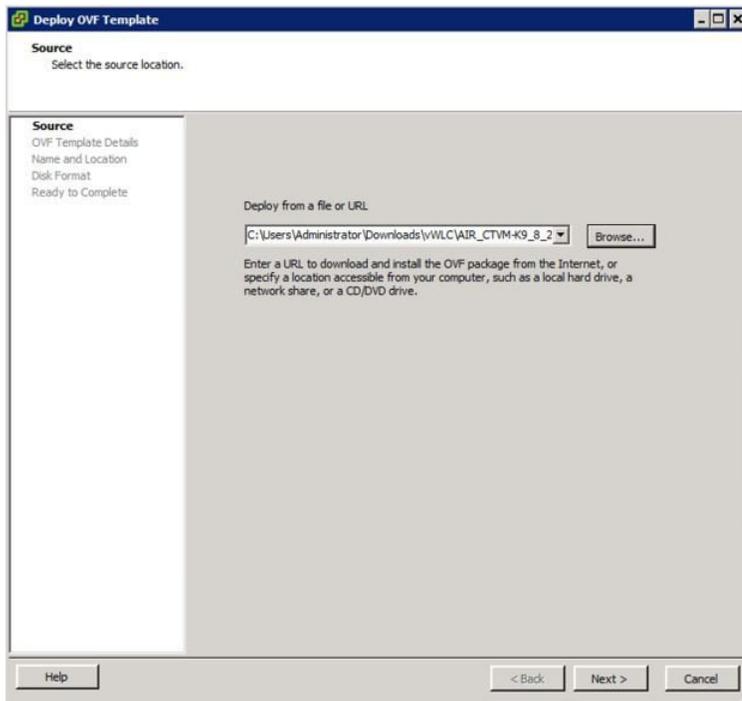
vWLC OVA の導入

手順

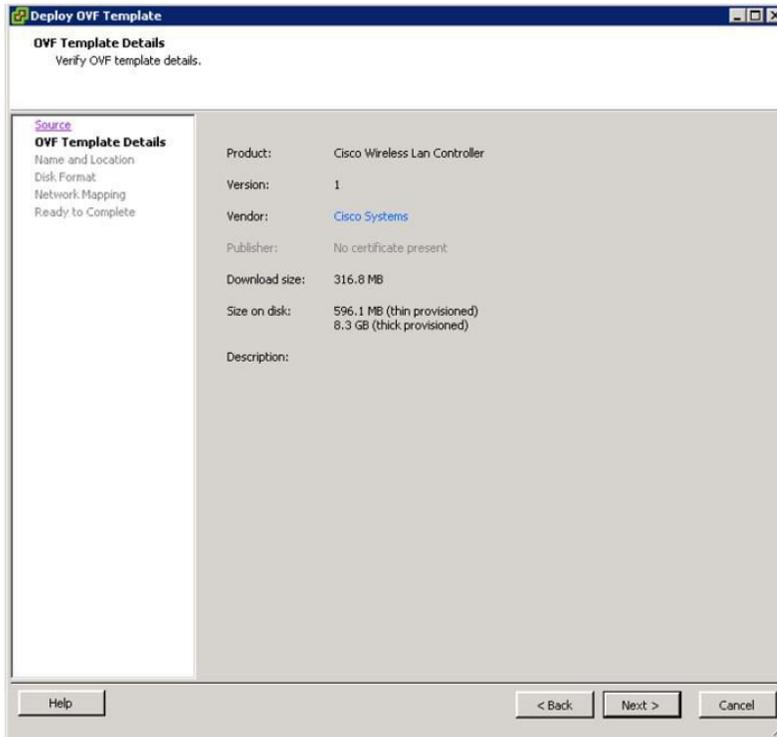
ステップ 1 ダウンロードしてローカルストレージに取得された小規模または大規模の *.ova を使用します。



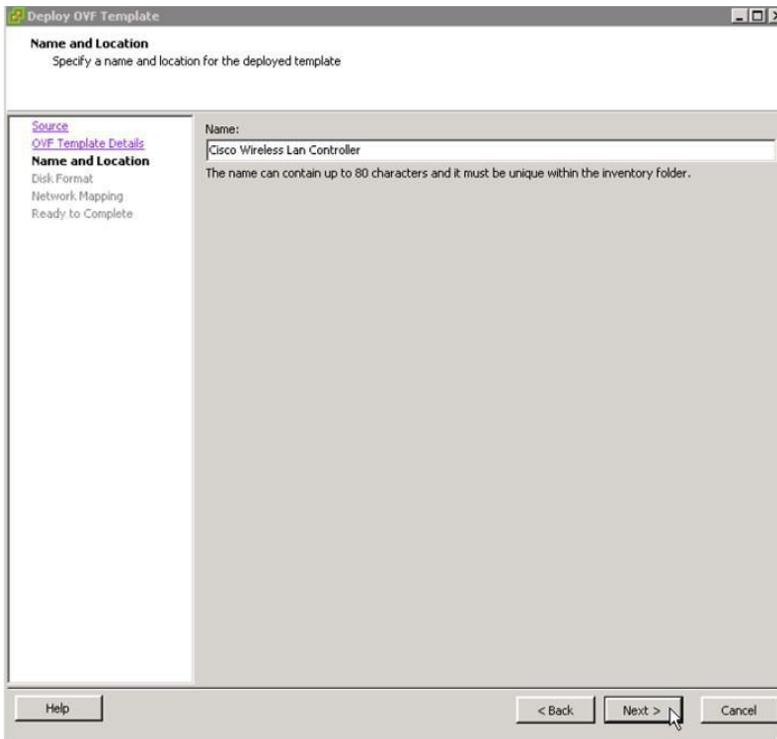
ステップ2 ターゲットの OVF ファイルを指定して、[Next] をクリックします。



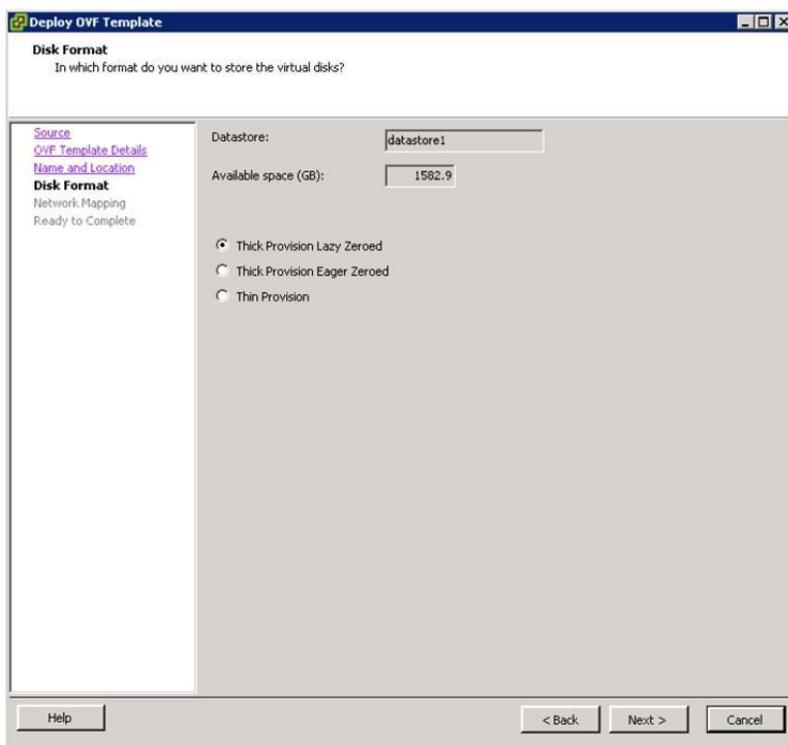
ステップ3 ターゲットの OVF に設定されている vWLC の詳細が表示されます。変更は必要ないため、[Next] をクリックします。



ステップ 4 作成される vWLC インスタンスの名前を指定し、[Next] をクリックします。

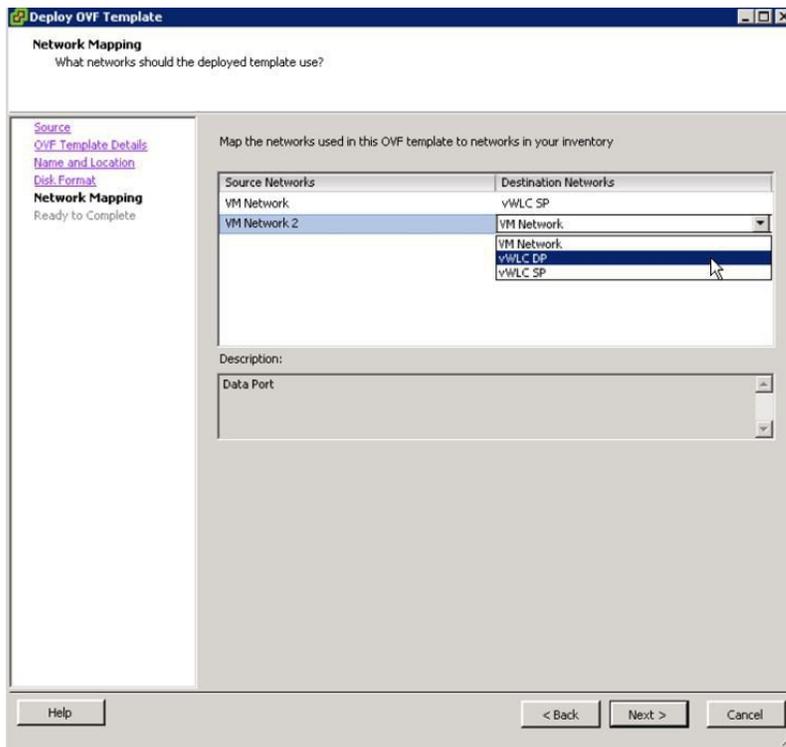


ステップ 5 ディスク形式をデフォルト、Thick Provision Lazy Zeroed、のままにしまして、[Next] をクリックします。

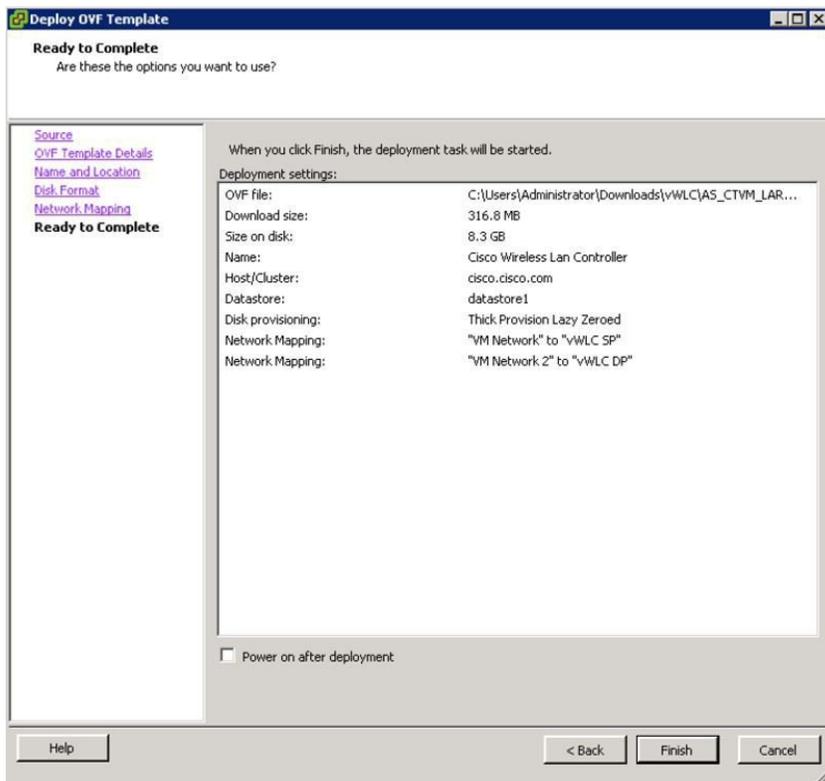


ステップ 6 ネットワーク マッピングには、サービス ポートとデータ ポートとして定義された（説明でも分類されている）2つの送信元ネットワークがあります。接続先ネットワークでこれらのインターフェイスを必要に応じてマッピングし、[Next] をクリックします。

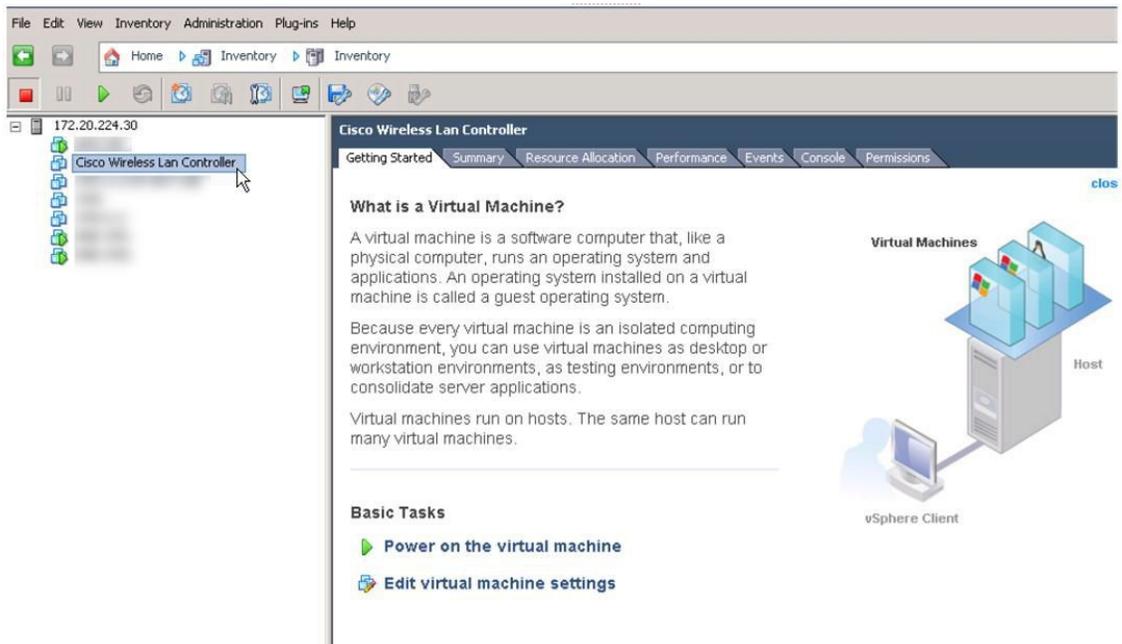
（注） 簡素化されたコントローラ プロビジョニングは、Web ブラウザを使用して、新しい vWLC で有効になります。サービス ポートのセグメントに接続されたクライアント PC は、vWLC のインストールでこの機能にアクセスできます。



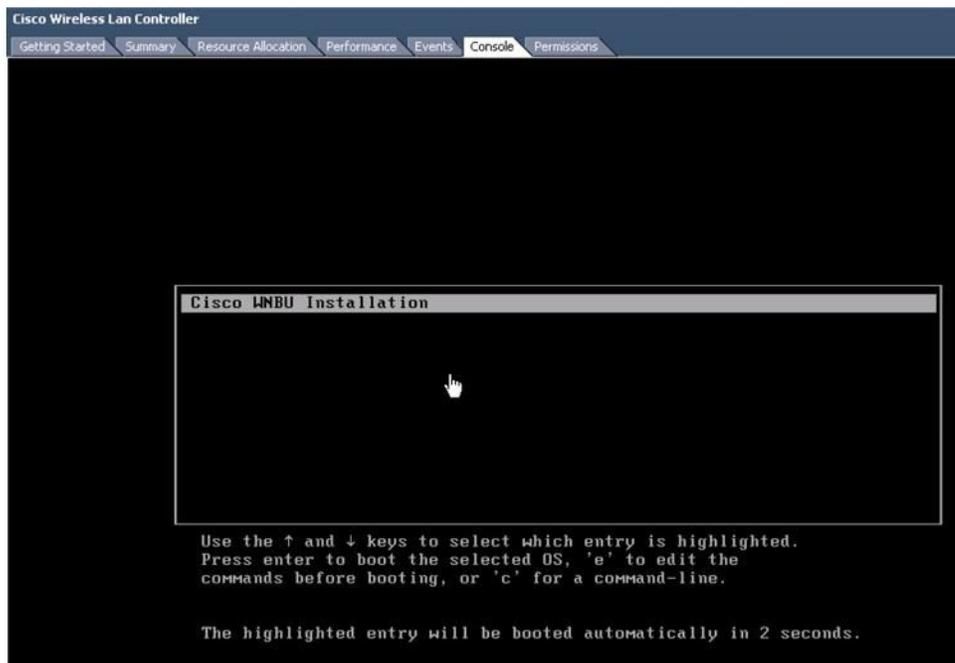
ステップ7 vWLC はインストール中に続行できます。導入設定を確認して、[Finish] をクリックします。



ステップ 8 完了したら、vWLC インスタンスを選択し、電源をオンにします。



ステップ 9 vWLC の自動インストールを完了できます。数分かかる場合があります。



ステップ 10 仮想マシンのコンソールで、インストールの完了が表示され、再起動が開始されます。

```

Cisco Wireless Lan Controller
Getting Started Summary Resource Allocation Performance Events Console Permissions

Type = 13 Length = 839
Type = 14 Length = 1245
Block 2: MAGIC2 = f00dbeef
Certs.bin verified. Real size is 11471
Copied 11471 bytes from generic2.bin to certs.bin.v2
Start appending new certs at offset 11471 in certs.bin.v2
Wrote 8 bytes file header to cert package certs.bin.v2
Wrote 8 bytes cert header to cert package certs.bin.v2
Wrote 1883 bytes (1883 reported) to cert package certs.bin.v2
Wrote 8 bytes cert header for pvt key to cert package certs.bin.v2
Wrote 1704 bytes (1704 reported) to cert package for pvt key certs.bin.v2
Wrote 4 bytes file footer to cert package for Cisoc ID cert certs.bin.v2
New cert file certs.bin.v2 is created.

certs.bin is updated.

-----
Virtual Wireless LAN Controller
Installation complete.
-----
Stage 1 boot completed, rebooting...
INIT: Switching to runlevel: 6
INIT: Sending processes the TERM signal
Sending all processes the TERM signal...

```

ステップ 11 再起動時に、VMware のコンソールで「Press any key to use this terminal as the default terminal」と表示されます。コンソールウィンドウをクリックし、任意のキーを押して端末にアクセスすることが重要です。

```

Cisco Wireless Lan Controller
Getting Started Summary Resource Allocation Performance Events Console Permissions

Cisco Bootloader Loading stage2...
Press any key to use this terminal as the default terminal.
Press any key to use this terminal as the default terminal.
Press any key to use this terminal as the default terminal.
Press any key to use this terminal as the default terminal.
Press any key to use this terminal as the default terminal.
Press any key to use this terminal as the default terminal.

Cisco Bootloader (Version 8.2.1.119)

.o00b. d000000b .d0000. .o00b. .d00b.
d0P Y0 '00' 00' YP d0P Y0 .0P Y0.
0P 00 '0bo. 0P 00 00
0b 00 'Y0b. 0b 00 00
Y0b d0 .00. db 0D Y0b d0 '0b d0'
'Y00P' Y000000P '0000Y' 'Y00P' 'Y00P'

Booting Primary Image...
Press <ESC> now for additional boot options... _

```

ステップ 12 vWLC が完全にオンラインになると、CLI によって構成ウィザードが表示されます。

```
Cisco Wireless Lan Controller
Getting Started Summary Resource Allocation Performance Events Console Permissions

Starting Hotspot Services: ok
Starting Tunnel Services New: ok
Starting Portal Server Services: ok
Starting mDNS Services: ok
Starting Management Services:
  Web Server: CLI: Secure Web: Web Authentication Certificate not found (
error). If you cannot access management interface via HTTPS please reconfigure U
irtual Interface.

Enabling Controller Provisioning
Configuring Service Port
Starting DHCP day 0 task
Starting Internal DHCP server
dhcp pool 192.168.1.3(0xc0a80103) - 192.168.1.14(0xc0a8010e), network 192.168.1
.0(0xc0a80100) netmask 255.255.255.240(0xfffff0), default gateway 192.168.1.1

Enable Service port dhcp server setup on 1
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:
```

オプションの仮想コントローラ コンソール ポート

コンソールポートは、ワイヤレス LAN コントローラのコンソールプロンプトにアクセスできます。そのため VM をこれらに接続するようにシリアルポートでプロビジョニングすることができます。シリアルポートがない場合は、vSphere クライアント コンソールが vWLC のコンソールに接続されます。

VMware ESXi は vWLC VM に追加できる仮想シリアルコンソールポートをサポートします。シリアルポートは、次の 2 通りの方法のいずれかでアクセスできます。

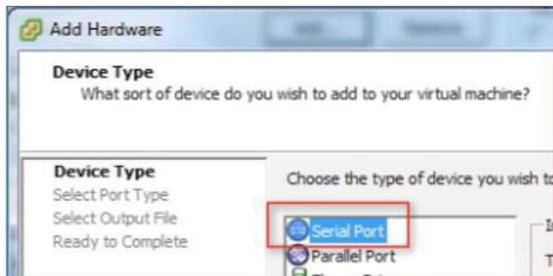
- ホスト上の物理シリアルポート：vWLC の仮想シリアルポートは、サーバ上のハードウェアシリアルポートにマッピングされます。このオプションは、マルチテナント vWLC シナリオで最適ではない可能性がある場合は、ホスト上の物理シリアルポートの番号に制限されます。
- ネットワークによる接続：vWLC の仮想シリアルポートは、リモートマシンからハイパーバイザの VM に割り当てられている特定のポートへの Telnet セッションを使用してアクセスできます。たとえば、「telnet 10.10.10.10 9090」を使用してハイパーバイザの IP アドレスが 10.10.10.10 で、vWLC VM に割り当てられているポートが 9090 である場合、Cisco ターミナルサーバを使用して物理 WLC コンソールにアクセスするように、vWLC のシリアルコンソールにアクセスできます。

手順

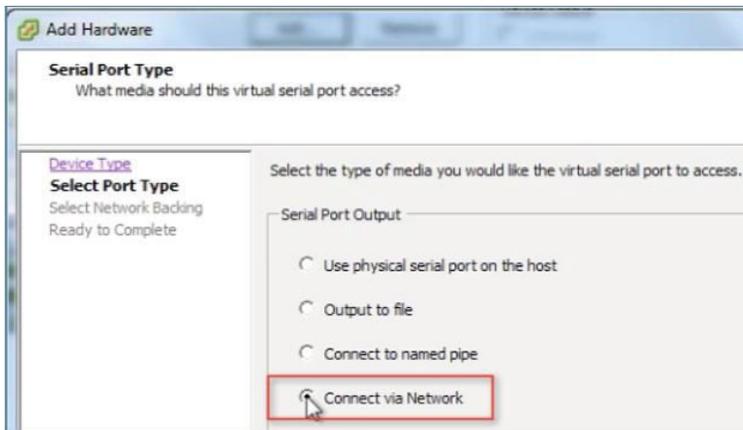
ステップ 1 [vWLC Hardware] タブで、[Add] をクリックします。



ステップ2 [Serial Port] を選択し、[Next] をクリックします。

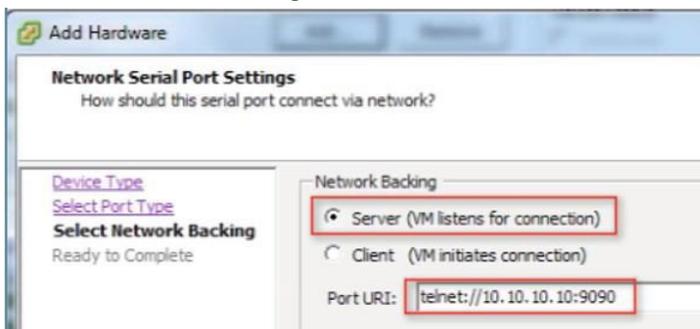


ステップ3 このシナリオでは、[Connect via Network] を選択します。[Next] をクリックします。

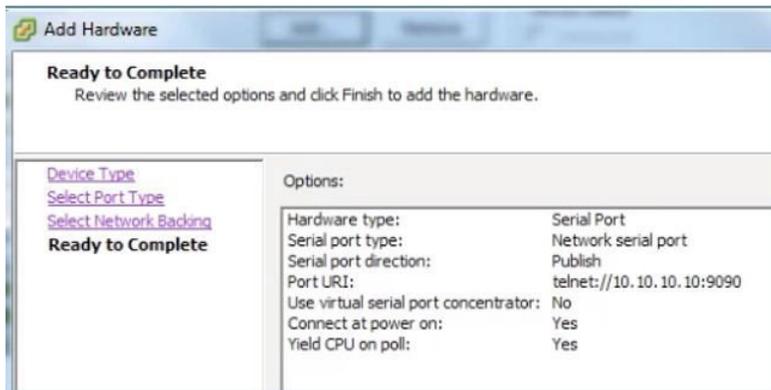


ステップ4 [Network Backing] > [Server (VM listens for connection)] を選択します。

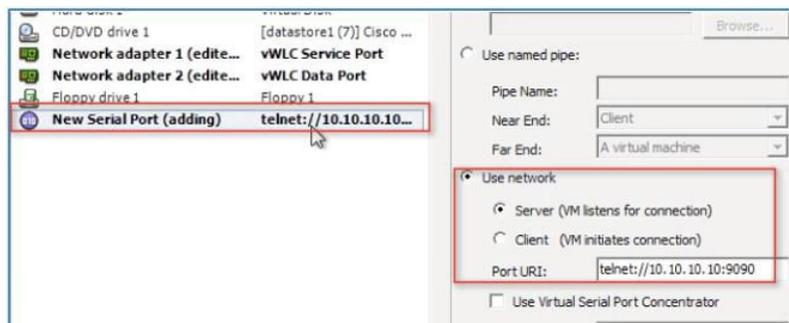
ステップ5 Port URI: telnet://<host>:<port> 例 **telnet://10.10.10.10:9090**



ステップ6 [Next] をクリックしてオプションを確認し、[Finish] をクリックします。

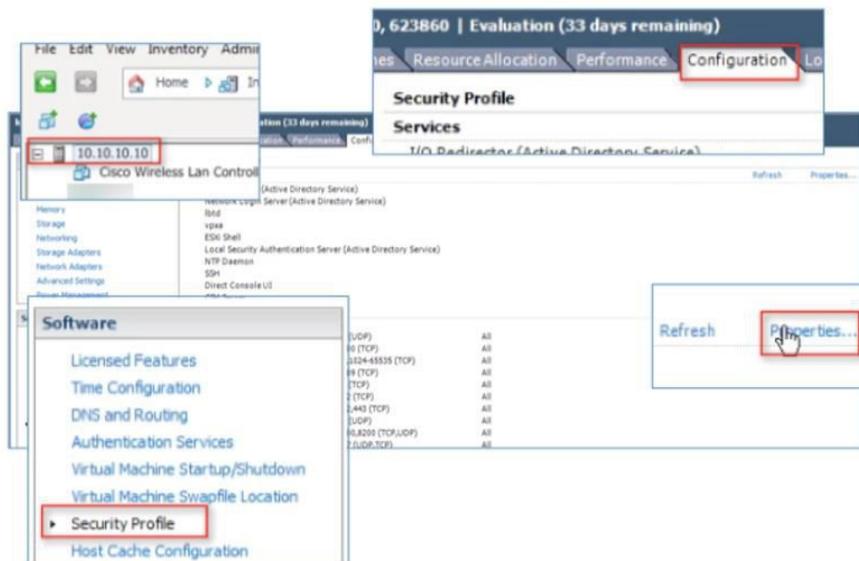


ステップ7 [OK] をクリックして設定を完了します。

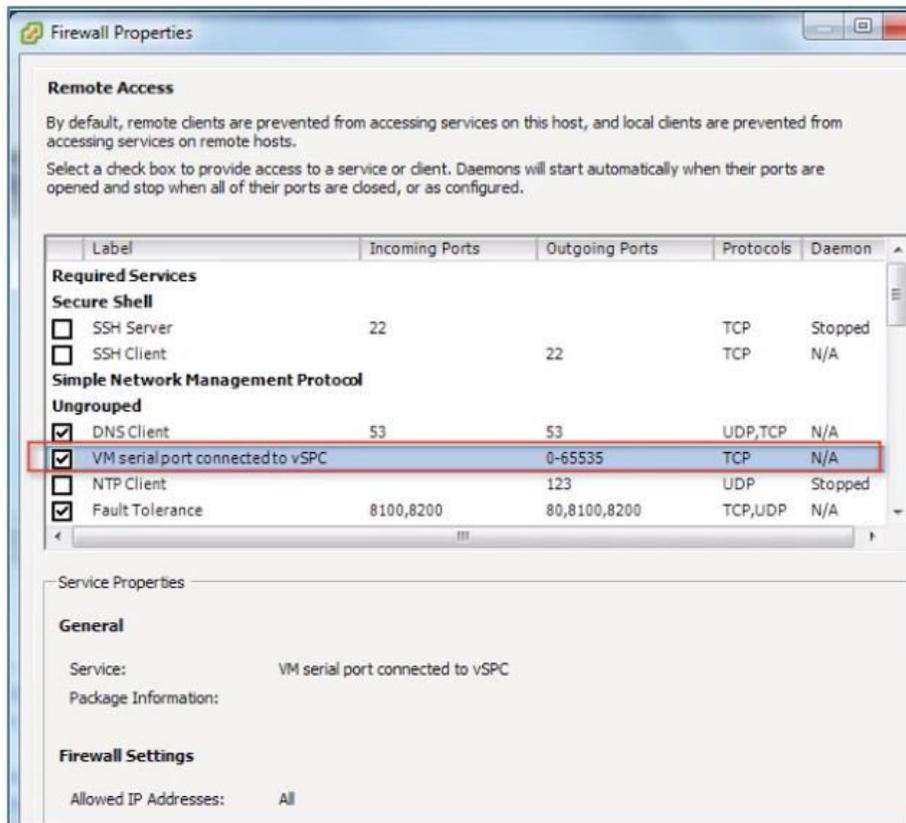


ネットワークでシリアルを有効にするには、ESX でそのような要求を許可するように設定する必要があります。

ステップ8 [ESX] > [Configuration] > [Software] > [Security Profile] に移動して、[Properties] をクリックします。

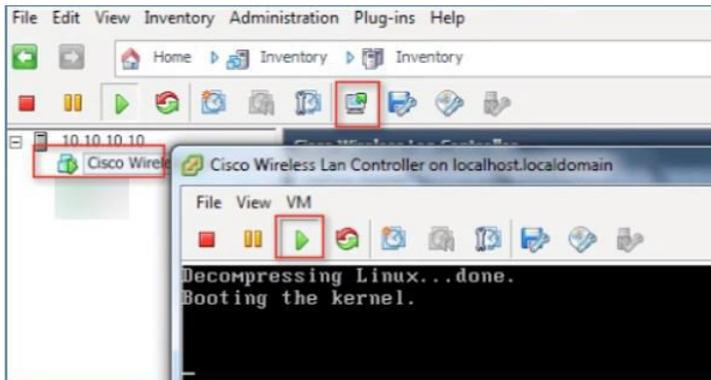


ステップ9 [Firewall Properties] で [VM serial port connected to vSPC] を選択または確認し、[OK] をクリックして設定を完了します。

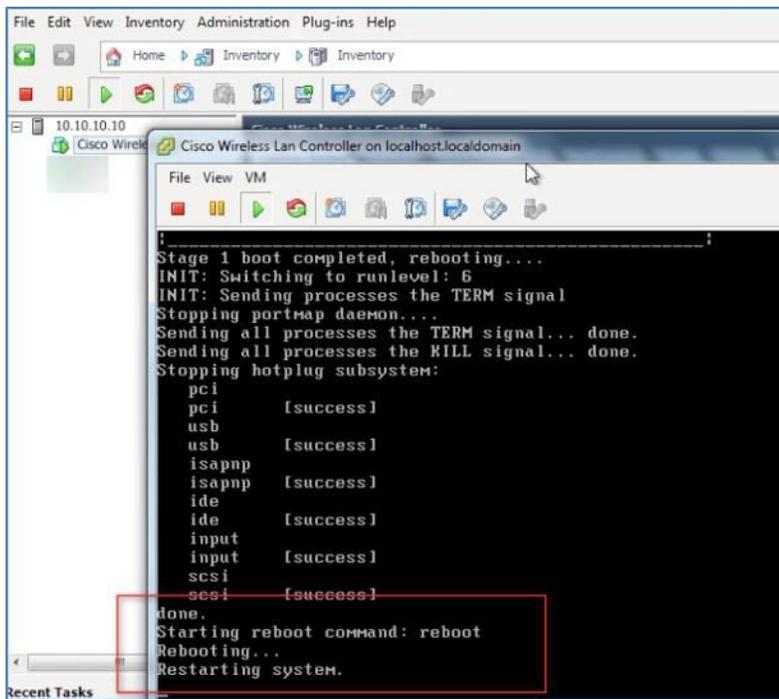


vWLC の起動

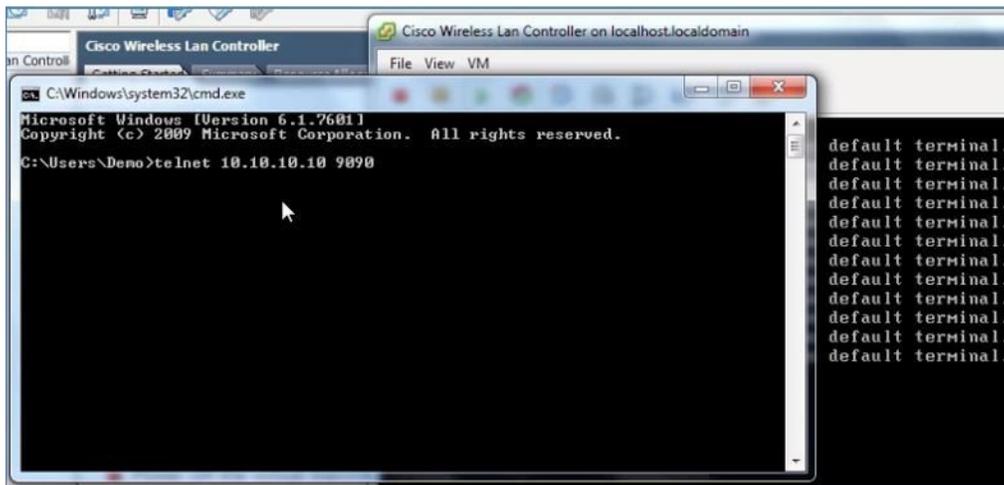
ステップ 10 仮想 WLC を起動し、コンソールを選択して最初のインストールプロセスを監視します。



ステップ 11 vWLC が再起動されたことを VM コンソールが表示するまでモニタします（これは自動です）。



ステップ 12 このとき、次の例のように、vWLC への Telnet セッションを開きます。



ステップ 13 Telnet セッションが vWLC へのコンソールを管理します。


```
Telnet 10.10.10.10
System Name [Cisco_08:5b:c2] <31 characters max>:
AUTO-INSTALL: no interfaces registered.
AUTO-INSTALL: process terminated -- no configuration loaded
vWLC
Enter Administrative User Name <24 characters max>: admin
Enter Administrative Password <3 to 24 characters>: *****
Re-enter Administrative Password : *****
Service Interface IP Address Configuration [static][DHCP]:
Management Interface IP Address: 10.10.11.20
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.11.1
Management Interface ULAN Identifier <0 = untagged>: 11
Management Interface Port Num [1 to 1]: 1
Management Interface DHCP Server IP Address: 10.10.10.1
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: demo
Network Name <SSID>:
```

ステップ 16 すべてのネットワーク デバイスと同様に、NTP を設定することは**重大で非常に重要**です。仮想コントローラは、ESX ホスト上で、または手動設定から正しくないクロックになることがあるため、正しいクロックにする必要があります。アクセス ポイントでプロセスに join しなくなる可能性があります。

```
Enter Country Code list <enter 'help' for a list of countries> [US]:
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:
Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 10.10.10.1
Enter a polling interval between 3600 and 604800 secs: _
```

ステップ 17 設定が完了したら、vWLC をリセットできます。

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Configuration saved!
Resetting system with new configuration...
Configuration saved!
Resetting system with new configuration...
```

ステップ 18 推奨事項は、オンラインであることを確認するために、vWLC の管理インターフェイスの接続を確認することです。vWLC にログインします。

```

Starting RRC Services: ok
Starting SXP Services: ok
Starting FMC HS: ok
Starting IPv6 Services: ok
Starting Config Sync Manager : ok
Starting Hotspot Services: ok
Starting Management Services:
Web Server: CLI: ok
Secure Web: ok
License Agent: ok
(Cisco Controller)
Enter User Name (or 'Recover-Config' this one-time only to
Factory defaults)
User: admin
Password:*****
Reply from 10.10.11.224: Destination host unreachable.
Reply from 10.10.11.20: bytes=32 time=42ms TTL=128
Reply from 10.10.11.20: bytes=32 time<1ms TTL=128
Reply from 10.10.11.20: bytes=32 time<1ms TTL=128
Reply from 10.10.11.20: bytes=32 time<1ms TTL=128

```

ステップ 19 「show interface summary」を実行して、vWLC からゲートウェイの接続を確認できます。

```

User:admin
Password:*****
(Cisco Controller) >show interface sum

Number of Interfaces..... 3
Interface Name          Port Ulan Id  IP Address
-----
management              1    11        10.10.11.20
service-port            N/A  N/A        0.0.0.0
virtual                  N/A  N/A        1.1.1.1

(Cisco Controller) >ping 10.10.11.1
Send count=3, Receive count=3 from 10.10.11.1
(Cisco Controller) >

```

ステップ 20 Web ブラウザを使用して vWLC 管理に接続します。

セットアップが簡単な vWLC

VMware コンソールから CLI を使用して vWLC を設定する代わりに、VMware または KVM 両方の導入に適用できる簡素化されたコントローラ プロビジョニング機能を使用します。このガイドで前述されているように、vWLC サービスポートにマッピングされたネットワークにアクセスする有線接続されたクライアント PC は、この機能を使用できません。この機能は、設定されていない vWLC から初めて起動した後、サービスポートのセグメントで一時的に DHCP サービスを提供し、PC クライアントに制限されたネットワークアドレスを割り当てます。クライアント PC は Web ブラウザを使用して vWLC に接続できます。

```
Starting Hotspot Services: ok
Starting Tunnel Services New: ok
Starting Portal Server Services: ok
Starting mDNS Services: ok
Starting Management Services:
  Web Server: CLI: Secure Web: Web Authentication Certificate not found (
error). If you cannot access management interface via HTTPS please reconfigure U
irtual Interface.

Enabling Controller Provisioning
Configuring Service Port
Starting DHCP day 0 task
Starting Internal DHCP server
dhcp pool 192.168.1.3(0xc0a80103) - 192.168.1.14(0xc0a8010e), network 192.168.1
.0(0xc0a80100) netmask 255.255.255.240(0xfffff0), default gateway 192.168.1.1

Enable Service port dhcp server setup on 1
(Cisco Controller)

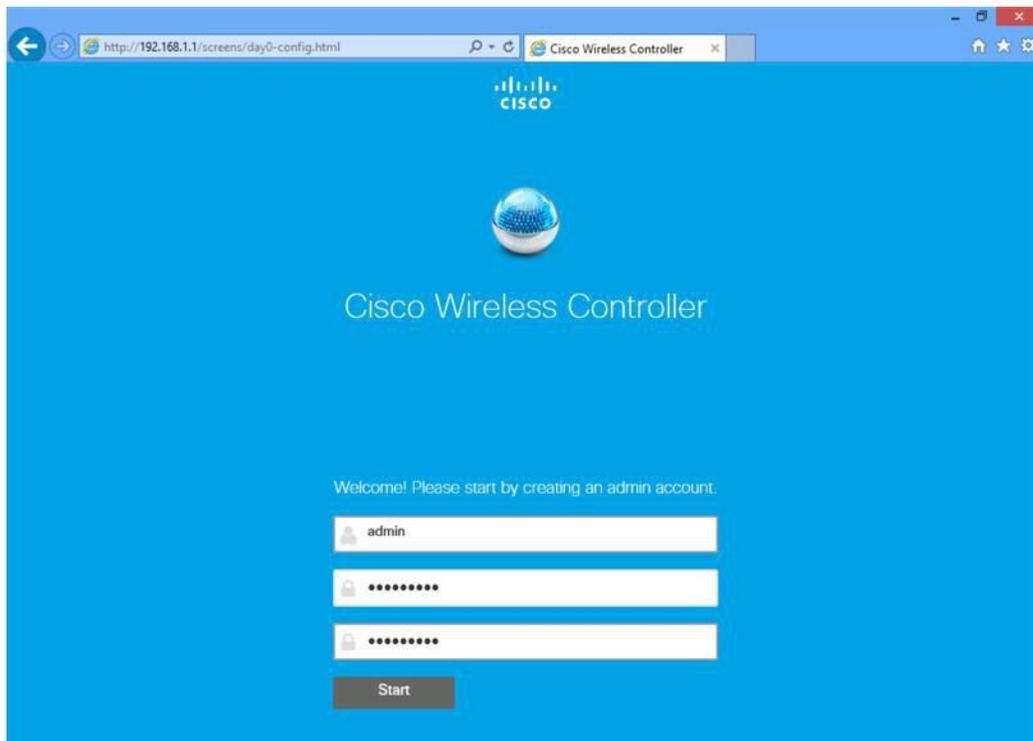
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
```

手順

- ステップ1** サービスポートにマッピングされるvWLCに接続されたクライアントPCで、192.168.1.3から192.168.1.14の限定された範囲からアドレスを使用します。vWLCは、固定の192.168.1.1が割り当てられます。



- ステップ2** クライアントPCからブラウザを開き、<http://192.168.1.1>に接続します。簡単なセットアップウィザードが、完全にvWLCを設定するために必要な最小限の手順で管理者を誘導します。最初の手順で、管理者アカウントを作成し、管理者のユーザ名とパスワードを入力し、[Start]をクリックします。



- ステップ 3** 簡単なセットアップ ウィザードの手順 1 で、システム名、国、日時（自動的にクライアント PC の時計から取得）、NTP サーバで vWLC を設定します。
- また、管理インターフェイスの管理 IP アドレス、サブネット マスク、ゲートウェイ、および VLAN を定義します。この割り当ては、ネットワーク インターフェイスの最初の VMware/KVM 設定からのデータ ポート（トランク）で設定および使用できる必要があります。[Next] をクリックします。

The screenshot shows the Cisco Wireless Controller configuration interface. The browser address bar displays 'http://192.168.1.1/screens/day0-config.html'. The page title is 'Cisco Wireless Controller' and the current step is '1 Set Up Your Controller'. The configuration fields are as follows:

System Name	vWLC
Country	United States (US)
Date & Time	12/01/2015 14:36:55
Timezone	Pacific Time (US and Canada)
NTP Server	0.0.0.0 (optional)
Management IP Address	172.20.224.50
Subnet Mask	255.255.255.0
Default Gateway	172.20.224.1
Management VLAN ID	0

At the bottom of the form, there are two buttons: 'Back' and 'Next'.

ステップ 4 手順 2 で、ワイヤレス ネットワーク (SSID)、セキュリティおよびネットワーク/VLAN の割り当てを必要に応じて作成します。オプションで、ゲストネットワーク設定、ゲスト用の個別のネットワークおよびアクセス方式のセキュアなゲスト アクセスを追加するための迅速かつ簡単な手順が含まれます。**[Next]** をクリックします。

Cisco Wireless Controller

1 Set Up Your Controller ✓

2 Create Your Wireless Networks

Employee Network

Network Name: Employee ?

Security: WPA2 Personal ?

Pass Phrase: ●●●●●●●● ?

Confirm Pass Phrase: ●●●●●●●●

VLAN: Management VLAN ?

DHCP Server Address: 0.0.0.0 (optional) ?

Guest Network

ステップ 5 簡単なセットアップの手順3では、管理者は目的のRF使用およびシスコワイヤレスLANコントローラのベストプラクティスのデフォルトを利用するためのWLC設定を最適化できます。[Next]をクリックして、設定を終了させます。

(注) シスコのベストプラクティスは、次の場所で継続的に更新されます。<http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/82463-wlc-config-best-practice.html>

Cisco Wireless Controller

1 Set Up Your Controller ✓

2 Create Your Wireless Networks

3 Advanced Setting

RF Parameter Optimization

Client Density: Low Typical High

Traffic Type: Data

Virtual IP Address: 192.0.2.1

Local Mobility Group: Default

Service Port Interface: Using DHCP (default)

Back Next

ステップ 6 簡単なセットアップウィザードは、設定の詳細を集約します。承認をクリックして、vWLCを再起動します。

Please confirm settings and apply

1 Controller Settings

Username **admin**
System Name **vWLC**
Country **United States (US)**
Date & Time **12/01/2015 14:38:20**
Timezone **Pacific Time (US and Canada)**
NTP Server **-**

Management IP Address **172.20.224.50**
Management IP Subnet **255.255.255.0**
Management IP Gateway **172.20.224.1**
Management VLAN ID **0**

2 Wireless Network Settings

✓ Employee Network

Network Name **Employee**
Security **WPA2 Personal**
Pass Phrase: *********
Employee VLAN **Management VLAN**
DHCP Server Address **-**

✗ Guest Network

Management IP Gateway 172.20.224.1
Management VLAN ID 0

2 Wireless Network Settings

Employee Network

Network Name Employee
Security WPA2 Personal
Pass Phrase: *****
Employee VLAN Management VLAN
DHCP Server Address -

Guest Network

3 Advanced Settings

RF Parameter Optimization

Client Density Typical
Traffic Type Data
Virtual IP Address 192.0.2.1
Local Mobility Group Default
Service Port Interface DHCP

Back Apply

Message from webpage

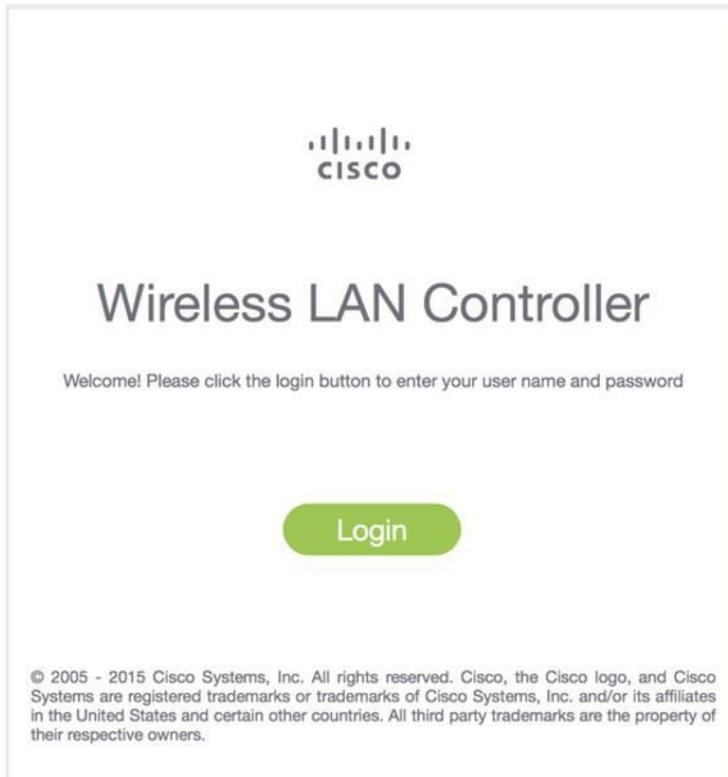
System will reboot after these settings are applied. Click OK to apply these configurations, or click Cancel to return to the setup wizard.

OK Cancel

Client Density Typical
Traffic Type Data
Virtual IP Address 192.0.2.1
Local Mobility Group Default
Service Port Interface DHCP

Back Apply

ステップ1 vWLCが再起動すると、簡単なセットアップ機能とサービスポートの使用を無効にします。操作はデータポート専用で、事実上定義された管理インターフェイスおよび動的インターフェイスを使用します。vWLCの割り当てられた管理IPアドレスでログインします。



Linux のカーネルベース仮想マシン (KVM)

このドキュメントは、CUWN 8.2 ソフトウェア リリースに基づいた vWLC および Linux のカーネルベース仮想マシン (KVM) のサポートについて更新されています。KVM は、シスコワイヤレス リリース 8.1.102.0 以降のリリースでサポートされます。



(注) KVM を導入した後、リリース 8.1.102.0 より古いシスコワイヤレスのリリースにダウングレードしないことを推奨します。

ホスティング バーチャル ワイヤレス LAN コントローラ (vWLC) の KVM 前提条件

次は、ホスティング vWLC の KVM 前提条件です。

- 最小で 2 G (小) または 8 G (大) のメモリ
- 最小で 1 つの vCPU
- 最小で 2 つのネットワーク インターフェイス

- 8 G のストレージが必要
- ネットワーク デバイス モデルは「virtio」
- Open vSwitch ブリッジに接続されている物理デバイスには IP アドレスが設定されていません。

詳細については、次を参照してください。 <http://www.linux-kvm.org/page/FAQ>

Fedora OS のインストール

Fedora OS をインストールするには、次の手順を実行します。

手順

-
- ステップ 1** Fedora 21 以降をインストールします。次のリンクをクリックして、Fedora をダウンロードします。
<https://getfedora.org/en/server/download/>
- ステップ 2** Fedora をインストールしたら、IP アドレスを設定してインターネットに移動します。
このシナリオでは、2 つの専用 Linux のインターフェイス/ポートが vWLC に使用されます。
- ステップ 3** `ifconfig{5}` を使用してインターフェイスを検索します。
例：
最初のインターフェイス：アップリンク（WLC のサービスポート）用。IP アドレスはこのインターフェイスに必要ありませんが、接続して起動する必要があります。
第 2 のインターフェイス：WLC 管理インターフェイス用。IP アドレスはこのインターフェイスに必要ありませんが、接続して起動する必要があります。
第 3 または第 4 のインターフェイス：Linux アクセシビリティ用。Linux ボックスに対するネットワークの接続性があるため、このインターフェイスに IP アドレスを指定します。
(注) デフォルトでは、KVM は vWLC 用のサービスポートとして最初のインターフェイスを使用します。
- ステップ 4** Linux にアクセスし、インターネットにアクセスして更新するには、第 3 または第 4 のインターフェイスに IP アドレスを設定します。
`vi /etc/sysconfig/network-scripts/ifcfg-enp2s0f3`
(注) BOOTPROTO を DHCP から静的に変更し、IPADDR、NETMASK、BROADCAST、および NETWORK の変数を追加する必要があります。静的 IP アドレスを選択することを推奨します。

例

```
NM_CONTROLLED="yes"
BOOTPROTO=static
DEVICE=eth1
ONBOOT=yes
IPADDR=192.168.8.248
NETMASK=255.255.255.0
BROADCAST=192.168.8.255
NETWORK=192.168.8.0
```

```
GATEWAY=192.168.8.1
TYPE=Ethernet
PEERDNS=no
```

ステップ 5 ファイルを保存します。

または

```
ifconfig <interface_name> <IP_address>
ifconfig <interface_name> netmask <netmask_address>
ifconfig <interface_name> broadcast <broadcast_address>
```

または

```
ifconfig <interface_name> <IP_address> netmask <netmask_address> broadcast <broadcast_address>
```

(注) プロキシおよび DNS 情報を必要に応じて設定します。インターネットが設定後にアクセスできることを確認します。

Fedora OS の更新

インストール後に Fedora OS を更新するには、次の手順を実行します。

手順

ステップ 1 Fedora OS の更新 :

```
yum install update
```

ステップ 2 GUI のインストール :

```
yum install @gnome-desktop -y
```

ステップ 3 VNC サーバ <http://www.namhuy.net/3134/install-vnc-server-on-fedora-20.html> のインストール :

```
yum install tigervnc-server -y
```

ステップ 4 X11 のインストール :

```
yum groupinstall "X Software Development"
```

KVM およびサポート パッケージ搭載の Open vSwitch のインストール

```
yum install -y @standard @virtualization openvswitch
systemctl enable network.service
systemctl start network.service
systemctl enable openvswitch.service
systemctl start openvswitch.service
```

KVM のインストールの確認

```
lsmod | grep kvm
```

Intel プロセッサの出力例：

```
[root@localhost system]# lsmod | grep kvm
kvm_intel 147785 0
kvm 464964 1 kvm_intel
```

ネットワーク設定

ブリッジの作成およびポートへのマッピング（イーサネット インターフェイス）

```
ovs-vsctl add-br ov_10nw
ovs-vsctl add-port ov_10nw enp2s0f0
ovs-vsctl add-br ov_9nw
ovs-vsctl add-port ov_9nw en
```

ブリッジの名前は XML ファイルで作成されるものと同じである必要があります。

ブリッジ マッピングの表示

```
ovs-vsctl show
```

例：

```
[root@localhost ~]# ovs-vsctl show
099e8b7e-bf00-4071-be62-ec55f9b543cc
Bridge "ov_9nw"
Port "ov_9nw"
Interface "ov_9nw"
type: internal
Port"enp2s0f1" Interface
"enp2s0f1"
Bridge "ov_10nw"
Port "ov_10nw"
Interface "ov_10nw"
type: internal
Port"enp2s0f0" Interface
"enp2s0f0"
ovs_version: "2.3.1-git3282e51"
```

XML ファイルの作成

2つの XML ファイル、service-nw（10nw）用と管理（9nw）用を作成します。

例：

```
10nw_eth0_ov.xml
9nw_eth1_ov.xml
```

両方の XML ファイルには、ネットワークまたは許可するものに基づいた VLAN 情報が含まれます。

例：すべての VLAN を許可する場合

```
<network>
<name>10-nw</name>
<forward mode='bridge' />
<bridge name='ov_10nw' />
<virtualport type='openvswitch' />
<portgroup name='vlan-any' default='yes'>
</portgroup>
</network>
```

ブリッジの名前は「ovs-vsctl」 コマンド中に作成されたものと同じである必要があります。

特定の VLAN だけを許可する必要がある場合は、次のフォーマットを使用します。

```
<network>
<name>ov-nw</name>
<forward mode='bridge' />
<bridge name='bridge_1' />
<virtualport type='openvswitch' />
<portgroup name='all_vlans' default='yes'>
</portgroup>
<portgroup name='vlan-152-untagged'>
<vlan>
<vlan mode='native-untagged' />
<tag id='152' />
</vlan>
</portgroup>
<portgroup name='vlan-153'>
<vlan>
<tag id='153' />
</vlan>
</portgroup>
<portgroup name='two-vlan'>
<vlan trunk='yes'>
<tag id='152' />
<tag id='153' />
</vlan>
</portgroup>
</network>
```

上記の設定の場合：

portgroup name='all_vlans' は、すべての VLAN を許可します。

portgroup name='vlan-152-untagged' は、152 のタグなし VLAN のみ許可します。

portgroup name='vlan-153' は、153 の VLAN のみ許可します。

portgroup name='two-vlan' は、2 つの VLAN、つまり 152 と 153 のみ許可します。

CDP パケットによる Open vSwitch からの転送許可

```
ovs-vsctl set bridge ov_9nw other-config:forward-bpdu=true
```

仮想ネットワークの表示

```
virsh net-list --all
```

デフォルトのネットワークの削除

```
virsh net-undefine default
```

仮想ネットワークの作成

```
virsh net-define <xml_file_name>
```

仮想ネットワークの表示

```
virsh net-list --all
```

仮想ネットワークの開始

```
virsh net-start <network_name_that is in the list>
```

例：

```
[root@localhost ~]# virsh net-list --all
Name State Autostart Persistent
-----
default inactive no yes
[root@localhost ~]# virsh net-undefine default
Network default has been undefined
[root@localhost ~]# virsh net-define 10nw_eth0_ov.xml
Network 10-nw defined from 10nw_eth0_ov.xml
[root@localhost ~]# virsh net-define 9nw_eth1_ov.xml
Network 9-nw defined from 9nw_eth1_ov.xml
[root@localhost ~]# virsh net-list --all
Name State Autostart Persistent
-----
10-nw inactive no yes
9-nw inactive no yes
[root@localhost ~]# virsh net-start 10-nw
Network 10-nw started
[root@localhost ~]#
[root@localhost ~]# virsh net-start 9-nw
Network 9-nw started
[root@localhost ~]# virsh net-list --all
Name State Autostart Persistent
-----
10-nw active no yes
9-nw active no yes
```

Fedora に仮想マシン マネージャ (VMM) を使用した vWLC のインストール

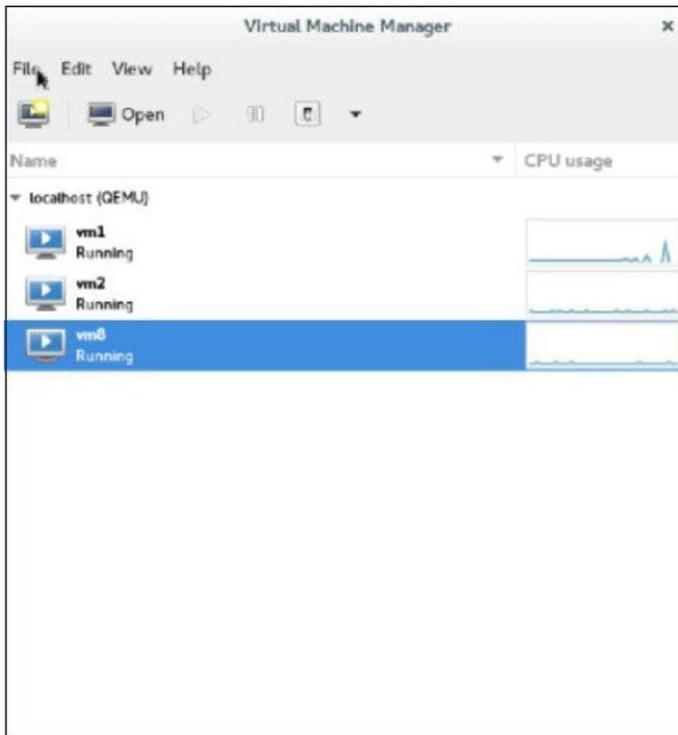
Fedora に VMM を使用して vWLC をインストールするには、次の手順を実行します。



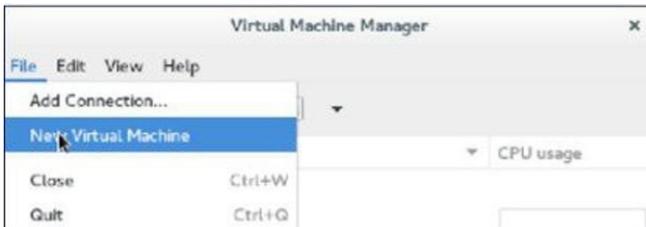
(注) Fedora へのコンソール。VMM には GUI が必要です。

手順

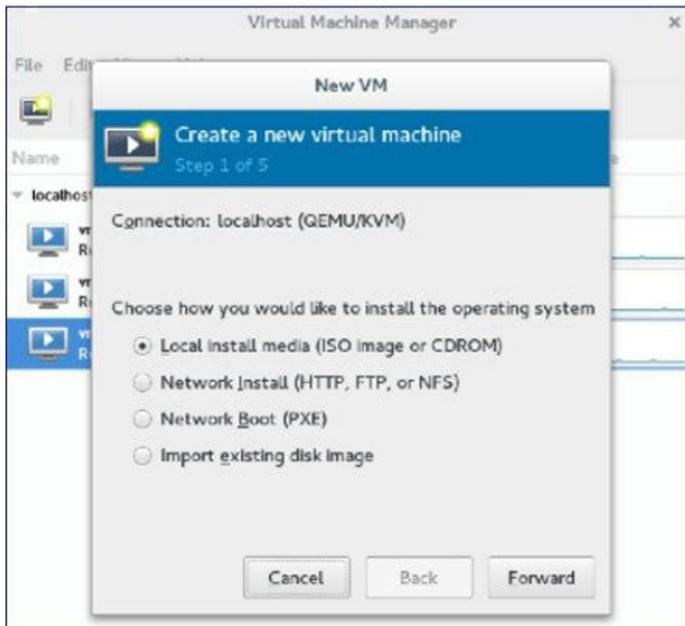
-
- ステップ1 端末を開きます (コマンドプロンプト)。
 - ステップ2 コマンド **virt-manager** を実行します。
Virt Manager (VMM) ポップアップ ウィンドウが表示されます。



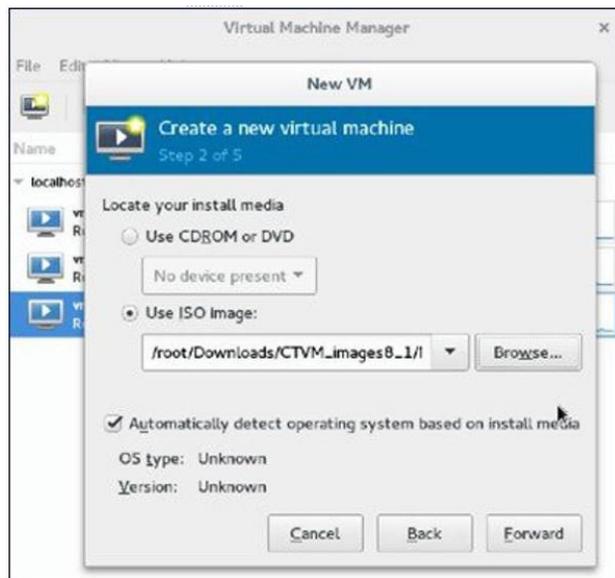
ステップ3 新しい仮想マシン (VM) を作成します。



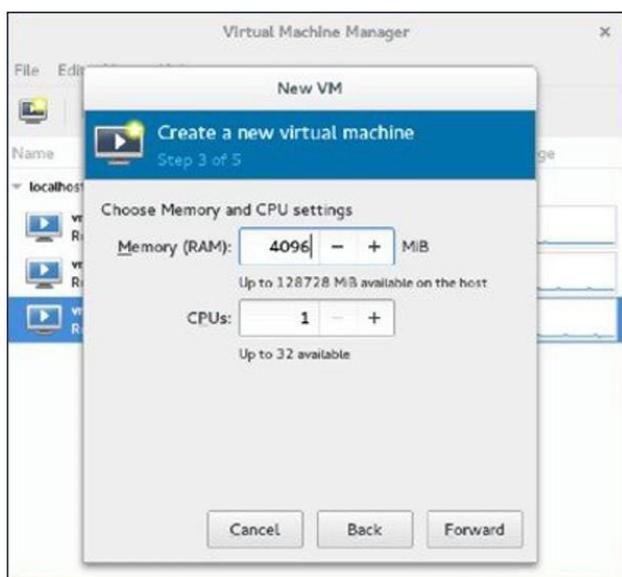
ステップ4 パスを選択します。



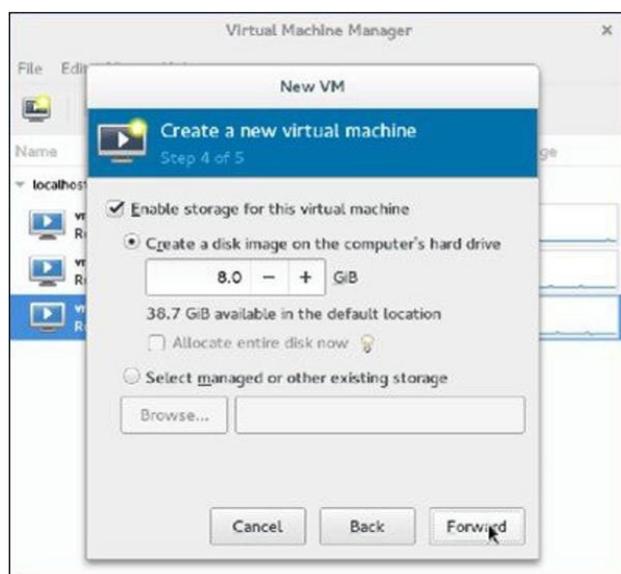
ステップ5 vWLCのISOファイルを選択します。



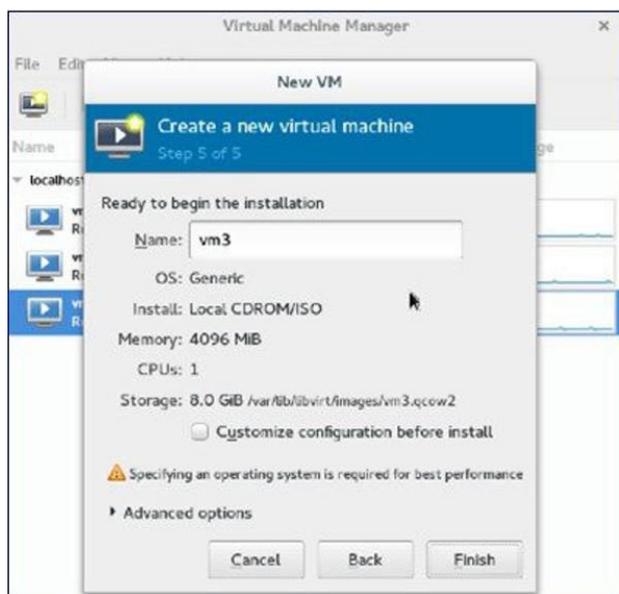
ステップ6 メモリとCPUを選択します。



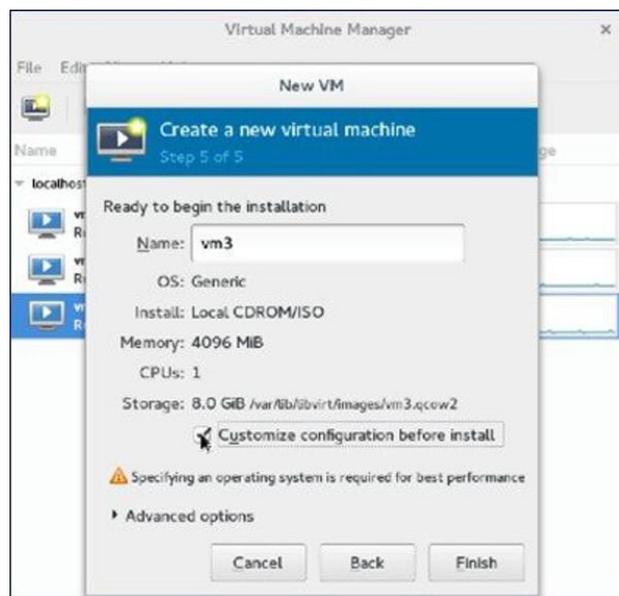
ステップ7 ディスク領域を選択します。



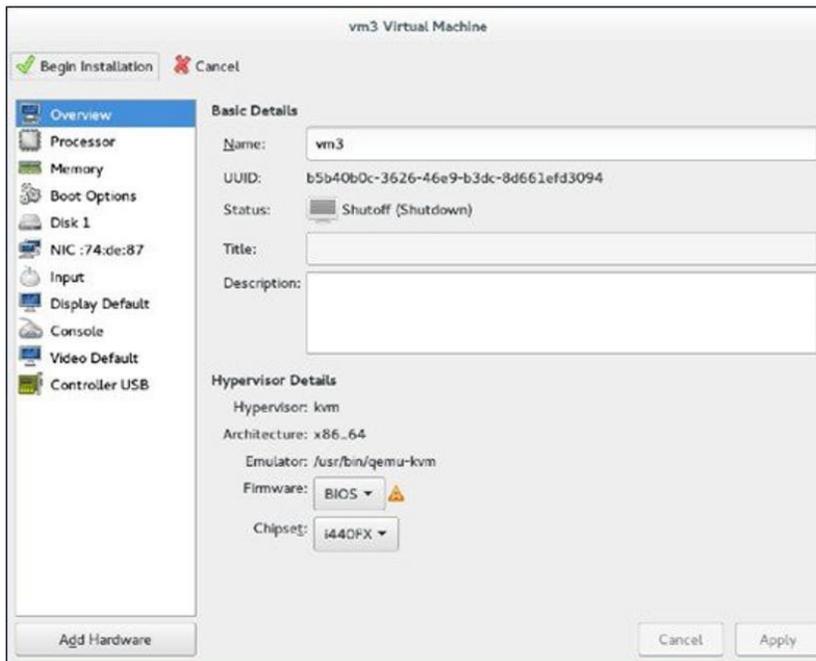
ステップ8 VMに名前を付けます。



ステップ9 [Customize configuration before install] チェック ボックスをオンにして、[Finish] をクリックします。（ここで他のオプションを設定できます）



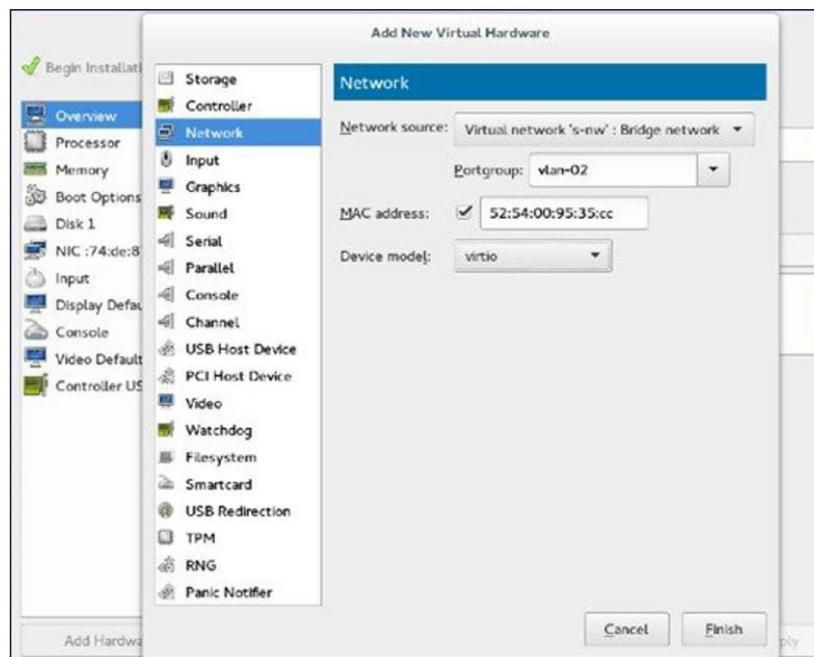
ステップ10 [Add Hardware] をクリックします。
[Add New Virtual Hardware] ウィンドウが表示されます。



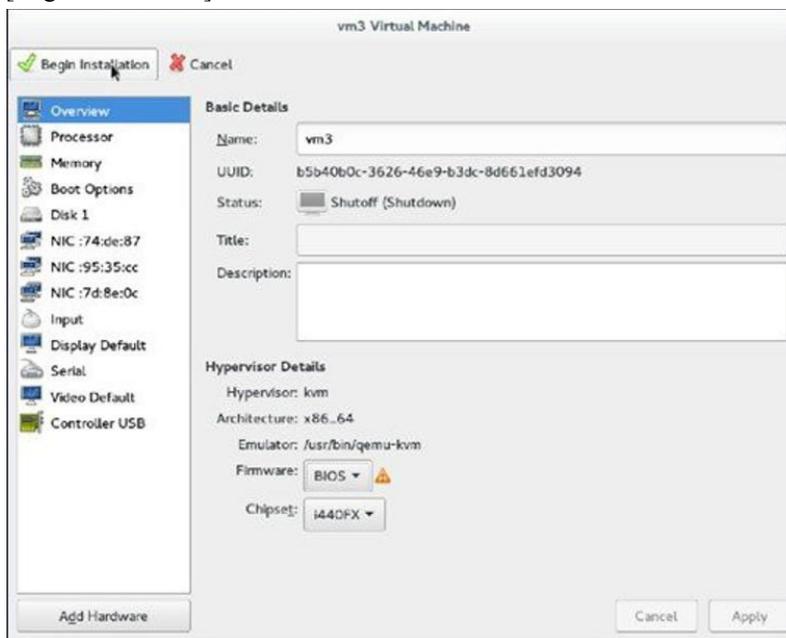
このウィンドウで、次のように、サービスポート、管理インターフェイス、シリアル接続の設定ができます。

- a) [Network] をクリックして、次の手順を実行します。
 - [Network source] ドロップダウンリストから、仮想ネットワークを選択します。（vWLC のサービスポートに仮想ネットワークを選択することを推奨します）
 - [Portgroup] ドロップダウンリストから、多数ある場合は、XML ファイルで設定されているポートグループを選択します。
 - [Device model] ドロップダウンリストから、[virtio]（現時点では、これのみがサポートされます）を選択し、[Finish] をクリックします。
- b) 管理インターフェイスの仮想ネットワークの設定には、[Add Hardware]>[Network] を選択して繰り返します。
 - (注) vWLC は 2 つの物理ポート（サービスポートと管理または動的インターフェイス）のみをサポートします。管理インターフェイスは管理または動的インターフェイスにマッピングされます。
- c) [Add Hardware]>[Serial] をクリックし、[Finish] をクリックします。

(注) Fedora 21 には「Virt-Manager」バージョン 1.1 があり、**portgroup** オプションがあります。古いバージョンにはありません。



ステップ 11 [Begin Installation] をクリックします。



ステップ 12 初期設定の WLC のプロンプトが表示されるまで待ちます。

Fedora の vWLC コンソールへのアクセス

vWLC コンソールにアクセスするには、次の手順を実行します。

手順

ステップ 1 端末から、次のコマンドを実行します。

```
virsh console <vm_name eg. vm1>
```

ステップ 2 仮想マネージャから vWLC を再起動します。

vWLC にマッピングされた vNets を見つけるには、vWLC で次のコマンドを実行します。

```
show interface detail management
```

(注) 最後の 6 オクテットを「ifconfig」出力と一致させます。

これは、複数の vWLC が設定されている場合、該当する「vNets」を取得する方法です。

vWLC および Ubuntu 搭載の KVM のインストール

Ubuntu と KVM をインストールするには、次の手順を実行します。

手順

ステップ 1 Ubuntu Server 13.10 以降をインストールして、仮想化モジュール/パッケージをインストール中に選択します。

ステップ 2 QEMU/KVM/Open vSwitch パッケージを次の手順でインストールします。

```
apt-get install qemu-kvm qemu-utils  
uml-utilities bridge-utils socat vnc4server vncviewer  
apt-get install kvm libvirt-bin virtinst  
apt-get install openvswitch-controller openvswitch-switch openvswitch-datapath-source
```

ステップ 3 Open vSwitch サービスを開始します。

```
service openvswitch-switch start
```

ステップ 4 システムをリブートします。

Ubuntu 上の 1 回限りのネットワーク設定

ホスト Linux で 1 回限りのネットワーク設定を実行するには、次の手順を実行します。

手順

ステップ1 2つの Open vSwitch ブリッジを作成し、eth0、eth1 を対応するブリッジにマッピングします。

```
ovs-vsctl add-br ovsbr0 [bridge name]
ovs-vsctl add-port ovsbr0 eth0
ovs-vsctl add-br ovsbr1[bridge name]
ovs-vsctl add-port ovsbr1 eth1
ovs-vsctl set bridge ovsbr1 other-config:forward-bpdu=true
Required for CDP packets forwarding from Open Vswitch]
```

ステップ2 管理ネットワークを定義するには、XML ファイル [mgmt.xml] を次のように作成します。

```
<network>
<name>VM-Mgmt-Nw</name>
<forward mode='bridge' />
<bridge name='ovsbr' />
<virtualport type='openvswitch' />
<!--
If the linux host port[For eg, eth1] is connected in trunk mode
to the downstream switch[which is also connected to the
openvswitch bridge ovsbr], then by choosing the following
portgroup,traffic from all vlan is passed up to the vWLC.
The management interface should be in vlan tagged mode.
And multiple interfaces can also be created with different vlans.
If the linux host port is connected in untagged mode to the
downstream switch, then on choosing this portgroup,untagged
frames are passed up to the vWLC. Hence management interface
has to be untagged.
-->
<portgroup name='default-portgroup' default='yes'>
</portgroup>
<!--
If the linux host port is connected in trunk mode to the
downstream switch [which is also connected to openvswitch
bridge ovsbr],and if only certain vlans are to be allowed,
choose this portgroup.
Uncomment the following portgroup and edit the tag ids
to the vlans allowed. You are free to add as many vlan ids as needed.
-->
<!--
<portgroup name='Management-Portgroup'>
<vlan trunk='yes'>
<tag id='4092' />
<tag id='4093' />
</vlan>
</portgroup>
-->
</network>
```

(注) 要件ごとに VLAN タグを編集します。

ステップ3 次のコマンドを実行し、管理ネットワークを作成します。

```
virsh net-define mgmt.xml
virsh net-start VM-Mgmt-Network
```

ステップ4 サービスポートネットワークを作成する場合は、手順2を繰り返します。サービスポートネットワークを定義するには、XMLファイル [service.xml] を次のように作成します。

```
<network>
<name>VM-SP-Nw</name>
<forward mode='bridge'/>
<bridge name='ovsbr'/>
<virtualport type='openvswitch'/>
<!--
If this portgroup is chosen, it is presumed that the linux host port
[For eg :eth0, connected to the openvswitch bridge "ovsbr"]
is connected in access mode to the neighboring switch.
-->
<portgroup name='default-portgroup' default='yes'>
</portgroup>
<!--
If the same linux host port[connected to the openvswitch
bridge "ovsbr"] as that of management interface is mapped
to Service interface in vWLC and if the linux host port
is in trunk mode ,then choose the following portgroup to
have untagged packets for service port access.
Uncomment the following portgroup and create the network.
Also, edit the native-vlan as per your network settings.
-->
<!--
<portgroup name='Service-portgroup'>
<vlan>
<vlan mode='native-untagged'/>
<tag id='4094'/>
</vlan>
</portgroup>
-->
</network>
```

(注) 要件ごとに VLAN タグを編集します。

ステップ5 次のコマンドを実行し、サービスネットワークを作成します。

```
virsh net-define mgmt.xml
virsh net-start VM-Service-Network
```

ステップ6 次のコマンドを使用して、仮想ネットワークのステータスを確認します。

```
virsh net-list --all
All the created networks are listed as active.
```

VMM を使用した vWLC の起動

VMM を使用して vWLC を起動するには、次の手順を実行します。



(注) これは、Fedora を使用したインストールに似ています。

手順

ステップ 1 仮想マシン マネージャ (VMM) を次のように起動します。

- a) GUI から VMM を起動するか、シェルから **virt-manager** と入力します。
GUI で、次の手順で vWLC インスタンスを簡単に作成することができます。
- b) ISO イメージを選択します。
- c) メモリに 4 GB を選択します。
- d) CPU に 1 を選択します。
- e) qcow2 イメージまたは raw イメージを指定します。
- f) インストールする前にカスタマイズ設定をクリックします。
- g) [NIC] をクリックし、デバイス モデルを **virtio** に変更し、ホスト デバイスを **VM-Service-Network** に変更します。
- h) [Add hardware] をクリックします。
- i) 新しいウィンドウで、[Network] をクリックし、ホスト デバイスを **VM-Mgmt-network** に、デバイス モデルを **virtio** に変更します。
- j) [Begin installation] をクリックします。

ステップ 2 コマンドプロンプトから、vWLC は次のコマンドで同様にシェルからインスタンス化できます (必要に応じてファイル名とパスを変更します)。

```
virt-install --connect=qemu:///system
--network=network:VM-Service-network,model=virtio
--network=network:VM-Mgmt-network,model=virtio --name=vm1
--cdrom=/home/user/vWLC/images/<AS_CTVM_8_1_xx_xx.iso>
--disk path=/var/lib/libvirt/images/4.img,size=8
--ram 2048 --vcpus=1 --vnc --vncport=5926
```

VMM の vWLC へのアクセス

バーチャル WLC (vWLC) は、次の方法でアクセスできます。

手順

- ステップ1 `virsh console <Virtual Machinename>` を開きます。
 - ステップ2 VNCviewer : たとえば、「`virsh vncviewer <VirtualMachine name>`」から vWLC の VNC の詳細を確認し、その VNC 接続の詳細を使用して「`vncviewer 127.0.0.1:11`」として vWLC にアクセスします。
 - ステップ3 VMM からコンソールにアクセスします。
-

vWLC および Suse Linux 搭載のホスト Linux のインストール

SLEs 12 - <https://www.suse.com> をダウンロードします。(ログインの作成が必要です)

- `eth0` : アップリンク (WLC のサービスポート) 用。IP アドレスはこのインターフェイスに必要ありませんが、接続して起動する必要があります。
- `eth1` : WLC 管理インターフェイス用。IP アドレスはこのインターフェイスに必要ありませんが、接続して起動する必要があります。
- `eth2` または `3` : Linux アクセシビリティ用。Linux ボックスおよびそこからインターネットに対するネットワークの接続性があるため、このインターフェイスに IP アドレスを指定します。



(注) その他のパッケージまたは KVM/vSwitch で作業する前に、Linux カーネルを確認します。カーネルバージョンが 3.12.36-38 以降であることを確認します。

カーネルバージョンが 3.12.36-38 以降でない場合は、次の手順を実行してアップグレードします。

手順

- ステップ1 SLES 12 をサーバにインストールします。
 - ステップ2 サーバが起動したら、マシンにカーネル RPM をコピーします。
 - ステップ3 端末で、`rpm --ivh <kernel>.rpm` を実行します。
RPM がインストールされます。設定には時間がかかります。
 - ステップ4 インストールが完了したらマシンを再起動し、最新のカーネルが `uname --a` を使用してロードされたことを確認します。
-

Suse での KVM およびサポート パッケージのインストール

次のコマンドを使用して、KVM およびサポート パッケージをインストールします。

```
zypper install openvswitch openvswitch-switch
zypper install kvm libvirt libvirt-python qemu virt-manager
```

SSH の有効化

次のコマンドを実行します。

```
systemctl enable sshd.service → enabling sshd daemon
systemctl start sshd.service → starting ssh
netstat -an | grep :22 → to see if port# 22 is listening
```

ネットワーク設定

ブリッジの作成およびポートへのマッピング（イーサネット インターフェイス）

```
ovs-vsctl add-br ov_10nw
ovs-vsctl add-port ov_10nw eth0 ovs-vsctl add-br ov_9nw
ovs-vsctl add-port ov_9nw eth1
```

ブリッジの名前は XML ファイルで作成されるものと同じである必要があります。

ブリッジ マッピングの表示

```
ovs-vsctl show
```

例：

```
linux-f8es:~ # ovs-vsctl show
51600b63-b508-45b0-9d0c-9f74036114c5
Bridge "ov_9nw"
Port "ov_9nw"
Interface "ov_9nw"
type: internal
Port "eth1"
Interface "eth1"
Bridge "ov_10nw"
Port "ov_10nw"
Interface "ov_10nw"
type: internal
Port "eth0"
Interface "eth0"
ovs_version: "2.1.2"
```

XML ファイルの作成

2 つの XML ファイル、service-nw（10nw）用と管理（9nw）用を作成します。

```
10nw_eth0_ov.xml
9nw_eth1_ov.xml
```

両方の XML ファイルには、ネットワークまたは許可するものに基づいた VLAN 情報が含まれます。

例：すべての VLAN を許可する場合

```
<network>
<name>10-nw</name>
<forward mode='bridge' />
<bridge name='ov_10nw' />
<virtualport type='openvswitch' />
<portgroup name='vlan-any' default='yes'>
</portgroup>
</network>
```

ブリッジの名前は「ovs-vsctl」コマンド中に作成されたものと同じである必要があります。

Open vSwitch の開始

```
service openvswitch-switch start
```

システム起動時に開始する Open vSwitch の設定

```
chkconfig openvswitch-switch on
```



(注) vSwitch は、上記のコマンドを使用してブリッジを作成する前に開始する必要があります。

libvirt の開始

```
service libvirtd restart
```

CDP パケットによる Open vSwitch からの転送許可

```
ovs-vsctl set bridge ov_9nw other-config:forward-bpdu=true
```

仮想ネットワークの表示

```
virsh net-list --all
```

デフォルトのネットワークの削除

```
virsh net-undefine default
```

仮想ネットワークの作成

```
virsh net-define <xml_file_name>
```

仮想ネットワークの表示

```
virsh net-list --all
```

仮想ネットワークの開始

```
virsh net-start <network_name_that is in the list>
```

例：

```
linux-f8es:~ # virsh net-list --all
Name          State      Autostart   Persistent
-----
default      inactive  no          yes
linux-f8es:~ # virsh net-undefine default
Network default has been undefined
linux-f8es:~ # virsh net-define 10nw_eth0_ov.xml
Network 10-nw defined from 10nw_eth0_ov.xml
linux-f8es:~ # virsh net-define 9nw_eth1_ov.xml
Network 9-nw defined from 9nw_eth1_ov.xml
linux-f8es:~ # virsh net-list --all
Name          State      Autostart   Persistent
-----
10-nw        inactive  no          yes
9-nw         inactive  no          yes
linux-f8es:~ # virsh net-start 10-nw Network 10-nw started
linux-f8es:~ #
linux-f8es:~ # virsh net-start 9-nw Network 9-nw started
linux-f8es:~ # virsh net-list --all
Name          State      Autostart   Persistent
-----
10-nw        active    no          yes
9-nw         active    no          yes
```

VMM を使用した vWLC のインストール

SUSE Linux に VMM を使用して vWLC をインストールするには、次の手順を実行します。

手順

-
- ステップ 1** Fedora と同様、端末に移動して、「virt-manager」と入力します。
仮想マシンマネージャ（VMM）が表示されます。
 - ステップ 2** 仮想マシン マネージャ（VMM）を使用して vWLC をインストールする手順を実行します。
-

RTU ライセンス

手順

-
- ステップ 1** AP Adder ライセンスをインストールするには、[Management] > [Software Activation] > [Licenses] をクリックします。
 - ステップ 2** [Adder License] 領域の [License Count] フィールドで、ライセンス タスクを [Add] に設定し、vWLC 用に購入した AP ライセンス数を入力して [Set Count] をクリックします。

Licenses

Adder License

License Count

License	Type	Time(expires)	RTU Count	Status
ap_count	Evaluation	12 weeks, 5 days	200	Active, Not-In-Use

ステップ3 エンドユーザライセンス (EULA) を読み、[I Accept] をクリックします。

End User License Agreement (EULA) ✕

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

Enabling additional access points supported by this controller product may require the purchase of supplemental or "adder" licenses. You may remove supplemental licenses from one controller and transfer to another controller in the same product family. NOTE: licenses embedded in the controller at time of shipment are not transferrable.

By clicking "I AGREE" (or "I ACCEPT") below, you warrant and represent that you have purchased sufficient supplemental licenses for the access points to be enabled.

All supplemental licenses are subject to the terms and conditions of the Cisco end user license agreement (http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), together with any applicable supplemental end user license agreements, or SEULA's.

Pursuant to such terms, Cisco is entitled to confirm that your access point enablement is properly licensed.

If you do not agree with any of the above, do not proceed further and CLICK DECLINE below.

AP Adder ライセンスが vWLC にインストールされて有効化されます。

Licenses

Adder License

License Count

License	Type	Time(expires)	RTU Count	Status
ap_count	Evaluation	12 weeks, 5 days	200	Inactive
ap_count (adder)	Permanent	No Expiry	200	Active, Not-In-Use

CLI を使用した RTU ライセンス

手順

ステップ 1 CLI を使用して AP Adder ライセンスをインストールするには、次のコマンドを入力します。
(Cisco Controller) > **license add ap-count<1-200>**

ステップ 2 エンドユーザ ライセンス (EULA) を読み、**Y** を入力し、[Enter] を押下して承認します。
機能名 : ap-count

```
Right to Use
```

```
Enabling additional access points supported by this controller product may require the purchase of supplemental or "adder" licenses. You may remove supplemental licenses from one controller and transfer to another controller in the same product family. NOTE: licenses embedded in the controller at time of shipment are not transferrable. By clicking "I AGREE" (or "I ACCEPT") below, you warrant and represent that you have purchased sufficient supplemental licenses for the access points to be enabled. All supplemental licenses are subject to the terms and conditions of the Cisco end user license agreement (http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\_.html), together with any applicable supplemental end user license agreements, or SEULA's. Pursuant to such terms, Cisco is entitled to confirm that your access point enablement is properly licensed. If you do not agree with any of the above, do not proceed further and CLICK "DECLINE" below. ACCEPT? [y/n]: Y Successfully added the license.
```

ステップ 3 AP Adder ライセンスが vWLC にインストールされて有効化されます。次のように、**show license summary** コマンドを入力して、インストール済みのライセンスを確認できます。
(Cisco Controller) > **show license summary**

```
Feature name:
ap_count License type:
Evaluation License Eula:
Not Accepted
Evaluation total period: 12
weeks 6 days License state:
Inactive, Not-In-Use
RTU License Count: 200
```

```
Feature name:
ap_count (adder)
License type:
Permanent
```

```
License state:  
Active, Not-In-Use  
RTU License Count:  
200
```

ステップ 4 機能ライセンスをアクティブ化または非アクティブ化するには、次のコマンドを入力します。
license {activate | deactivate} featurelicense_name

スマートライセンス

シスコスマートソフトウェアライセンスにより、現在のエンタイトルメント障壁を削除し、ソフトウェアのインストールベースに関する情報を提供することで、シスコソフトウェアの購入、展開、追跡、および更新が容易になります。これは、PAK ベース モデルから柔軟性と拡張ユーザーベースのモデルを有効にする新しいアプローチに移動する、シスコのソフトウェア戦略に対する大きな変更です。

シスコスマートソフトウェアライセンスは、次の特長を持ちます。

- 購入および導入したデバイスとソフトウェアの可視性
- 自動ライセンス有効化
- 標準ソフトウェア、ライセンス プラットフォーム、およびポリシーによる製品の簡素化
- 運用コストの削減可能性

お客様、お客様の選択したパートナー、およびシスコは、ハードウェア、ソフトウェア エンタイトルメント、およびサービスを Cisco Smart Software Manager インターフェイスで確認できます。

すべてのスマートソフトウェアライセンス製品は、シングルトークンで設定および有効化するとき自己登録されるため、Web サイトにアクセスして PAK 製品の後で製品を登録する必要がありません。PAK またはライセンス ファイルを使用する代わりに、スマートソフトウェアライセンスでは、柔軟かつ自動化された方法でポートフォリオ全体で使用できるソフトウェアライセンスまたはエンタイトルメントのプールを設定します。プーリングによりライセンスを再ホストする必要がなくなるため、RMA で特に役立ちます。Cisco Smart Software Manager で会社全体のライセンス導入を簡単かつ迅速に自己管理できます。

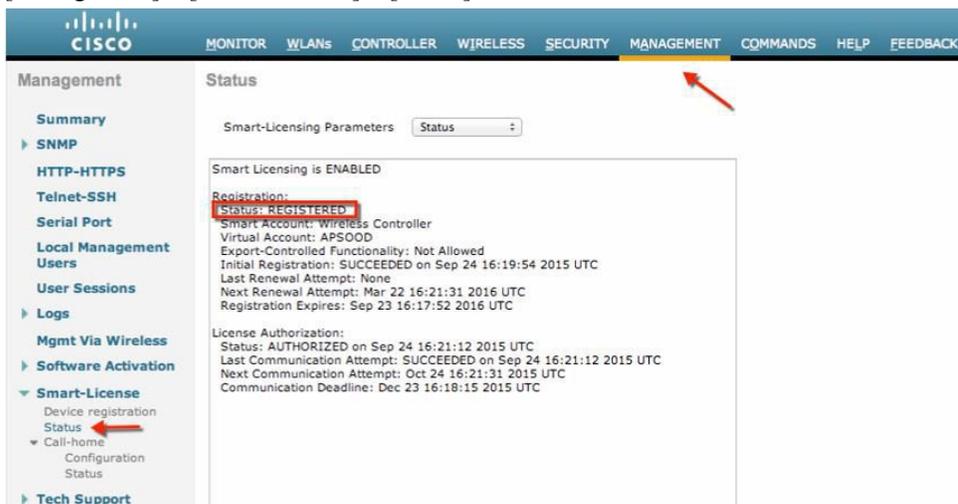
標準製品、標準ライセンスプラットフォーム、および柔軟な契約を通じて、シスコソフトウェアによるシンプルかつ生産性の高い経験が得られます。

Web GUI を使用したスマートライセンス

次の手順は、ダイレクトクラウドアクセス向けの、最も一般的な導入モードです。このガイドは、スマートライセンスを詳細に説明するものではありません。ユーザは、すでにアクセス権を持ち、完全にスマートライセンス機能と管理を理解していることが期待されます。

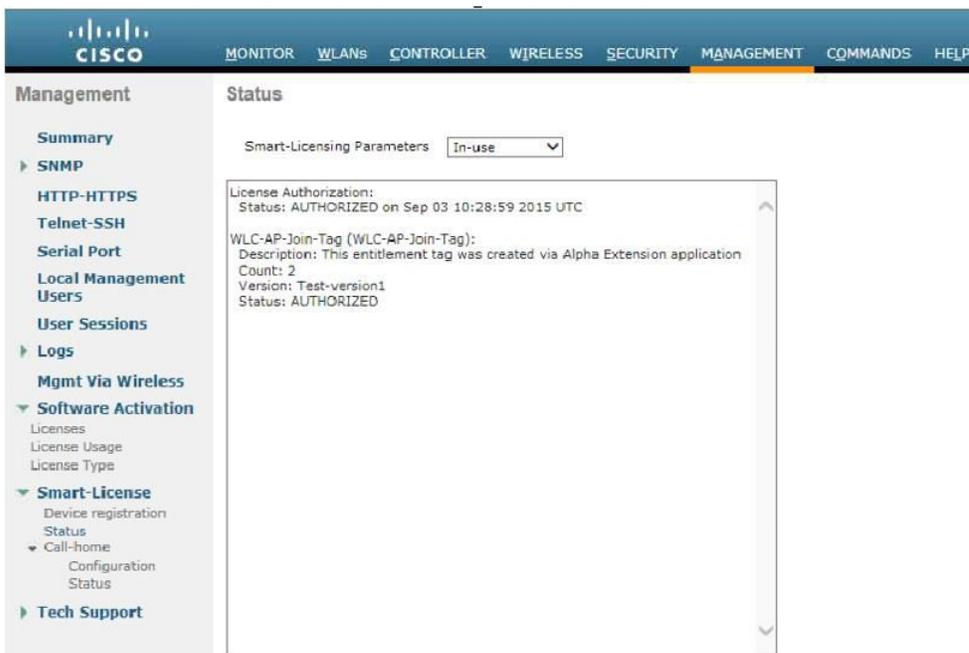
ユーザには、vWLC を登録するために必要なトークン ID を作成する能力が必要です。スマートライセンスに関する詳細については、必要に応じて導入ガイドを参照してください。

ステップ4 [Management] > [Smart-License] > [Status] で、登録と認証のステータスを確認します。



CSSM ポータルで、デバイスが登録された対応する仮想アカウントの [Product Instances] タブにデバイスが表示されます。

ステップ5 AP が WLC に join すると、エンタイトルメントが 24 時間に 1 回要求されます。エンタイトルメントのステータスは、[Management] > [Smart-license] > [Status] で確認できます。



The screenshot shows the Cisco Prime Infrastructure Management console. The left sidebar contains a 'Management' menu with options like Summary, SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, Smart-License, and Tech Support. The main content area is titled 'Status' and shows 'Smart-Licensing Parameters' with a 'Summary' dropdown menu. Below this, it states 'Smart Licensing is ENABLED' and provides details for 'Registration' and 'License Authorization'. A table titled 'License Usage' shows the following data:

License	Entitlement tag	Count	Status
WLC-AP-Join-Tag	(WLC-AP-Join-Tag)	2	AUTHORIZED

Cisco Prime 3.0 搭載の仮想コントローラ管理

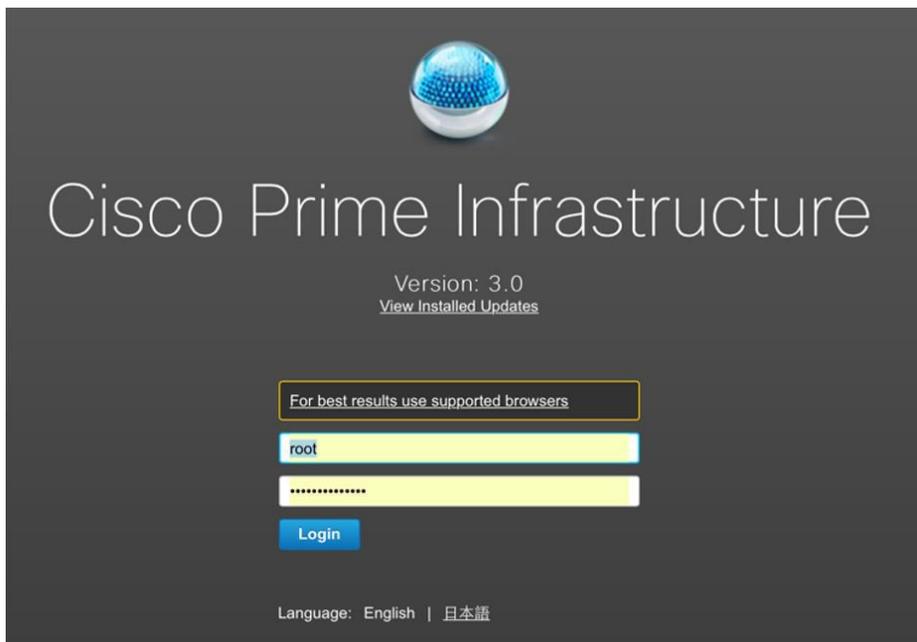
Cisco Prime Infrastructure バージョン 3.0 では、1 つ以上のシスコ仮想コントローラを中央管理するために必要な最小リリースです。CPI 3.0 は、仮想コントローラの設定、ソフトウェア管理、モニタリング、レポート、およびトラブルシューティングを提供します。管理および管理サポートに関する Cisco Prime Infrastructure ドキュメントを必要に応じて参照してください。

Cisco Prime 互換性対応表：

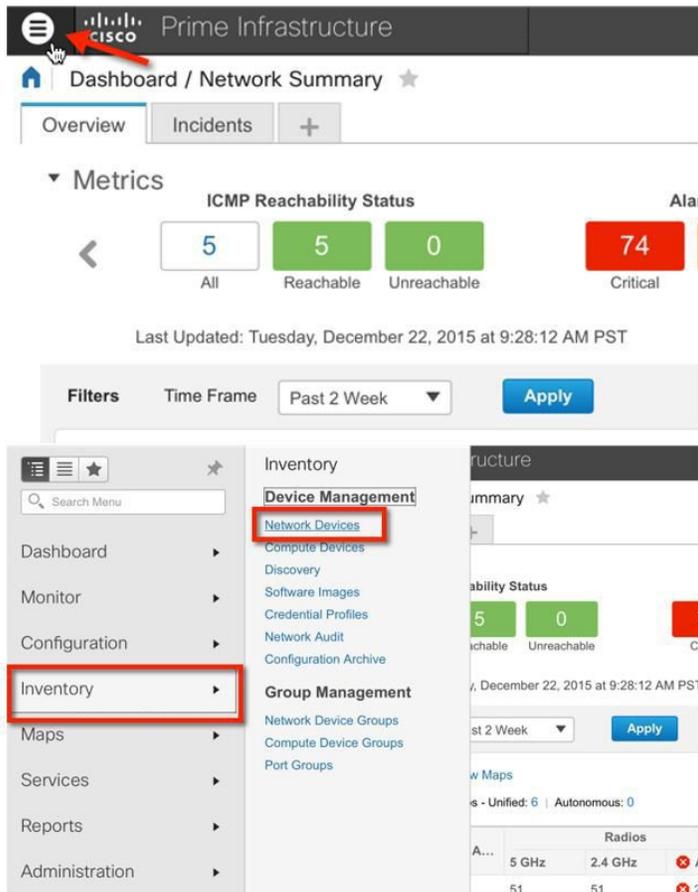
<http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html#52734>

手順

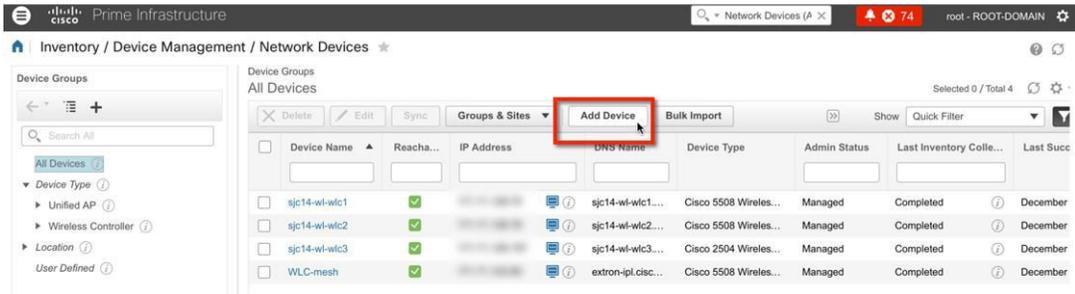
ステップ 1 ルートとして Cisco Prime Infrastructure サーバにログインします。



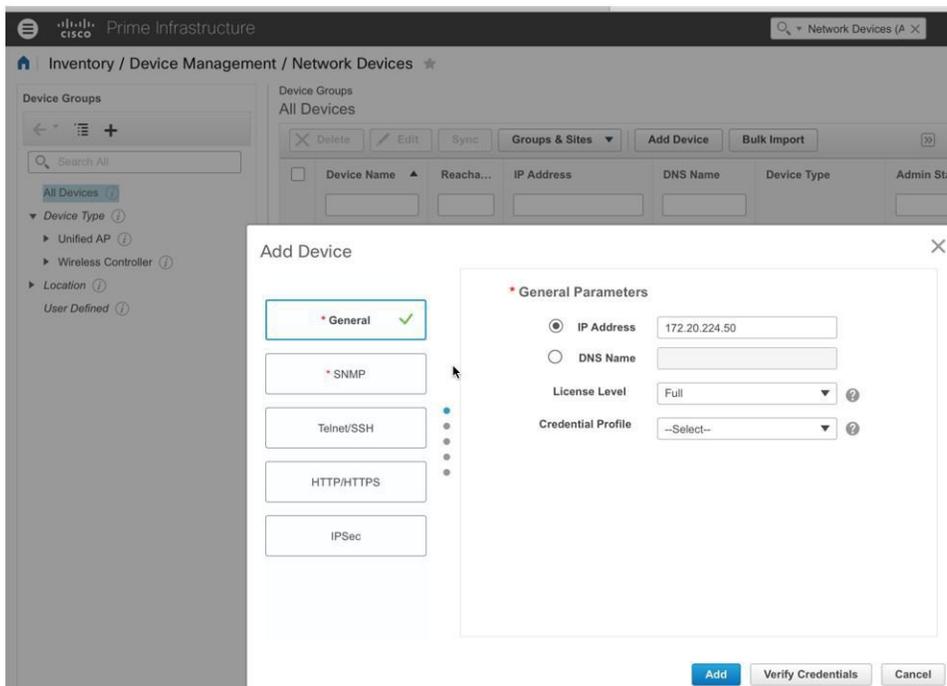
ステップ2 [Inventory]、[Device Management] > [Network Devices] に移動します。

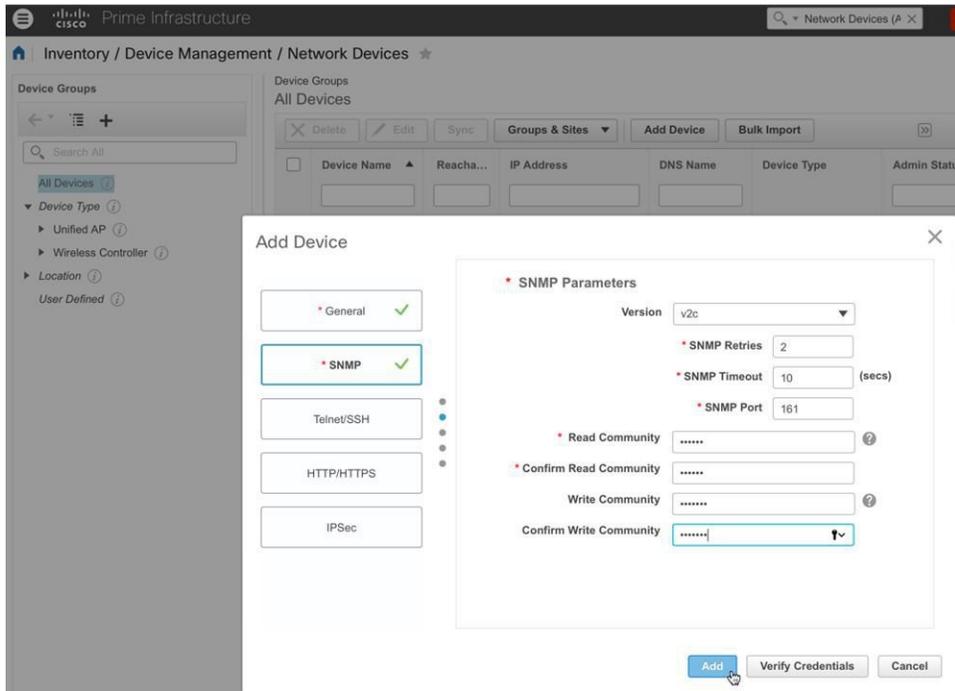


ステップ3 ネットワークデバイスで [Add Device] をクリックします。

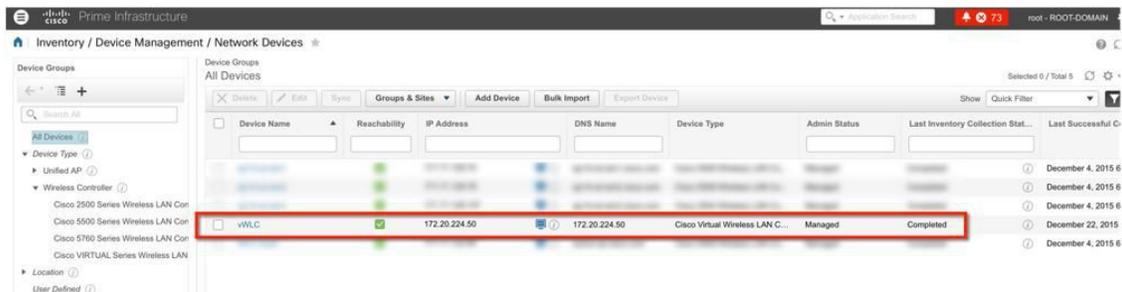


ステップ4 IP アドレスと SNMP コミュニティ文字列を入力します (読み取り/書き込み)。デフォルトでは、コントローラの SNMP RW は [Private] です。[Add] をクリックします。

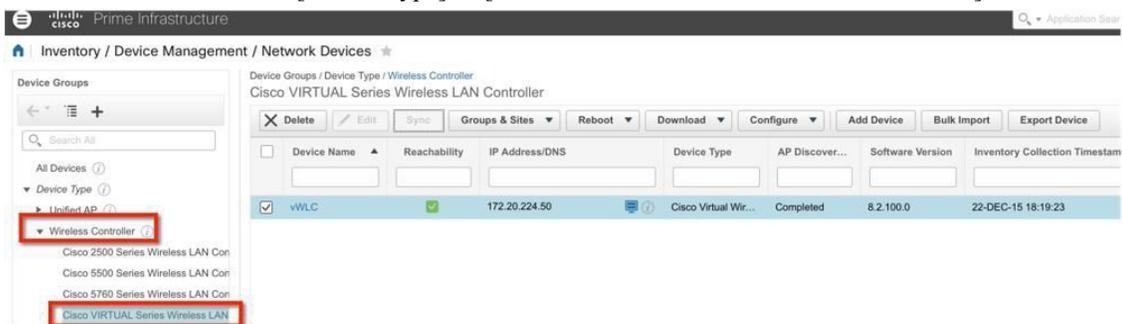




ステップ5 Cisco Prime Infrastructure は仮想コントローラで検出と同期を行います。画面を更新するには、更新ボタンをクリックします。仮想コントローラが検出されると、到達可能性が緑色で表示され、[Managed]（管理対象）としてリストされます。他の仮想コントローラを使用する可能性がある場合、この時点で追加します。



ステップ6 新しいコントローラは、[Device Type] の [Cisco Virtual Series Wireless LAN Controller] にリストされます。



仮想コントローラのアップグレード

インストールの以前の手順では、シスコ仮想コントローラには新しい仮想アプライアンスを作成するには最初に OVA ファイルが必要でした。ただし、仮想コントローラ機能の管理およびソフトウェアアップグレードには Cisco のサイトからダウンロード可能な共通の AES ファイルが必要です。

手順

ステップ 1 アップグレードソフトウェアの *aes ファイルを、ターゲットホスト (TFTP/FTP など) にダウンロードするか HTTP ファイル転送を使用します。

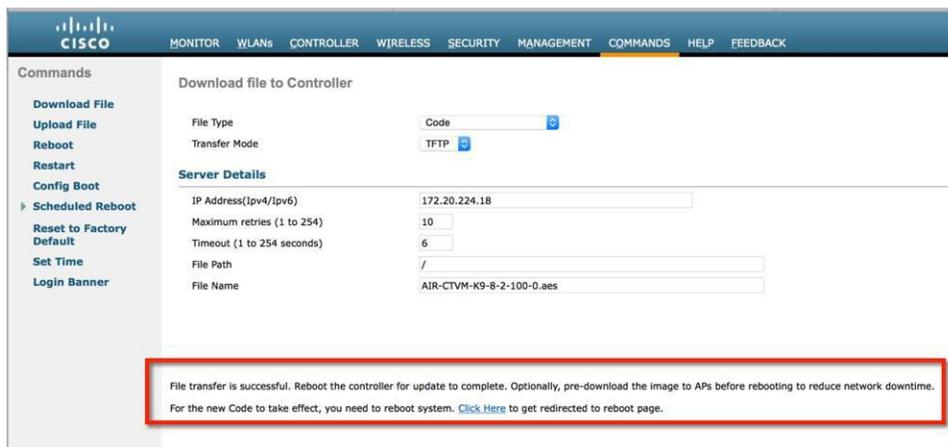
ステップ 2 従来のコントローラと同様に、コントローラの Web GUI で、[COMMANDS] > [Download File] に移動します。ファイルタイプ、転送モード、IP アドレス、パスとファイル名 (aes ファイル) を選択します。[Download] ボタンをクリックしてプロセスを開始します。



The screenshot shows the Cisco Web GUI interface for downloading a file to the controller. The left sidebar contains a 'Commands' menu with 'Download File' highlighted. The main content area is titled 'Download file to Controller' and contains the following fields:

Field	Value
File Type	Code
Transfer Mode	TFTP
IP Address(Ipv4/Ipv6)	172.20.224.18
Maximum retries (1 to 254)	10
Timeout (1 to 254 seconds)	6
File Path	/
File Name	AIR-CTVM-K9-8-2-100-0.aes

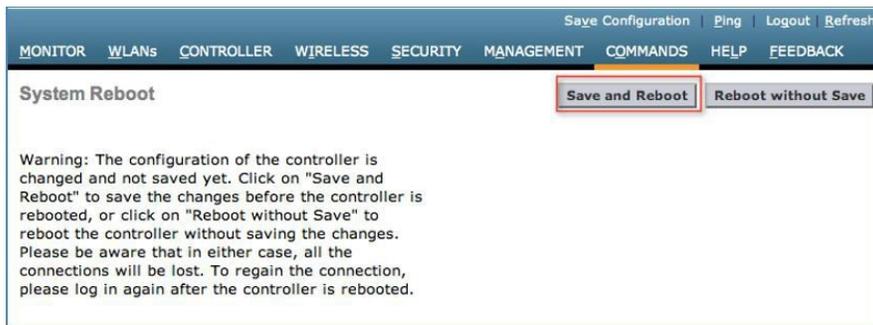
ステップ 3 プロセスが正常に完了すると、ユーザは新しいソフトウェアイメージの影響を伝送するために再起動するように求められます。続行するには、再起動ページへのリンクをクリックします。



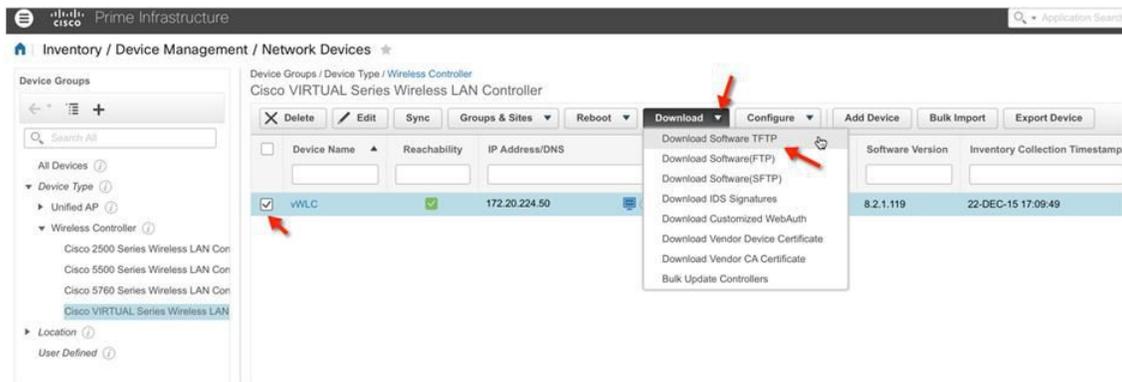
The screenshot shows the same 'Download file to Controller' page as in Step 2, but with a success message displayed at the bottom, highlighted with a red box:

File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to APs before rebooting to reduce network downtime. For the new Code to take effect, you need to reboot system. [Click Here](#) to get redirected to reboot page.

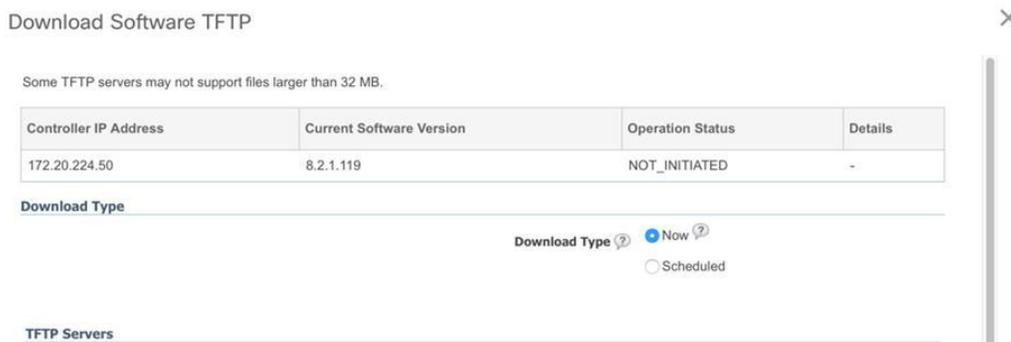
ステップ 4 [Save and Reboot] をクリックします。



ステップ 5 また、Cisco Prime Infrastructure 3.0 は、1 つの仮想コントローラまたは同時に多数の仮想コントローラのアップグレードに役立つことがあります。[Network Device] に移動します。1 つ以上の仮想コントローラを選択（チェック ボックスをオンに）し、コマンドプルダウンから [Download (TFTP/TFTP)] を選択します。この例では、イメージのアップグレードの TFTP モードを使用します。



ステップ 6 ダウンロードタイプ（Now / Scheduled）から [New]、または既存サーバの IP アドレス、パスとサーバファイル名（*.aes アップグレード ソフトウェア）を指定します。[Download] をクリックして、開始します。



TFTP Servers

File is located on Local machine TFTP server

Server Name

Server IP Address

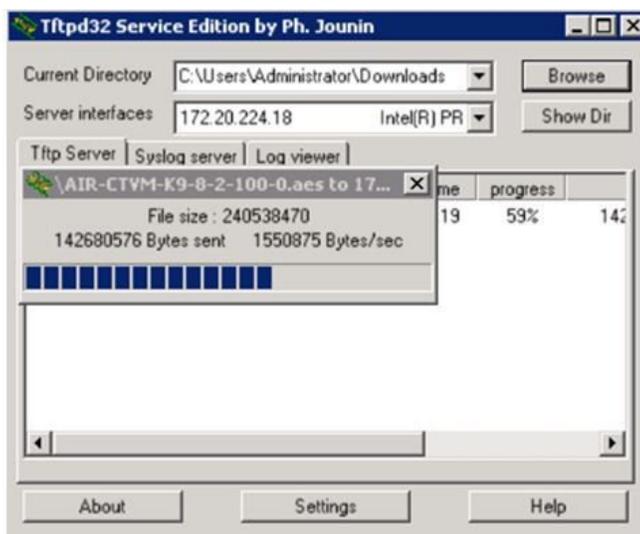
Maximum Retries

Time Out (secs)

File Path

Server File Name

ステップ 7 次の画面は TFTP サーバから仮想コントローラに転送される AES イメージの例です。



ステップ 8 Cisco Prime Infrastructure は、ソフトウェアが正常に転送されるまで、ステータスを更新します。

Download Software TFTP



Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version	Operation Status	Details
172.20.224.50	8.2.1.119	WRITING_TO_FLASH	Executing fini script.

Download Software TFTP

Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version	Operation Status	Details
172.20.224.50	8.2.1.119	TRANSFER_SUCCESSFUL	File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to APs before rebooting to reduce network downtime.

- ステップ 9** コントローラからの直接のエクスペリエンスと同様に、転送が完了したら再起動が必要です。仮想コントローラを選択して Cisco Prime Infrastructure に移動し、コマンドプルダウンから、[Reboot]>[Reboot Controllers] を選択します。



- ステップ 10** Cisco Prime Infrastructure は、保存の設定など、再起動パラメータのプロンプトが表示されます。続行するには、[OK] をクリックします。

Reboot Controllers



- ステップ 11** Cisco Prime Infrastructure は、仮想コントローラが再起動されていることを管理者に通知します。

Reboot Controllers



ステップ 12 完了すると、Cisco Prime Infrastructure は、プロセスの結果を示します。
Reboot Controllers

IP Address	Reboot Controller	Save Config to Flash	Reboot APs	Swap AP Image
172.20.224.50	✓	✓	✗	✗

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2016 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2016年5月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先