Cisco Network Function Virtualization Infrastructure Software スタートアップガイド

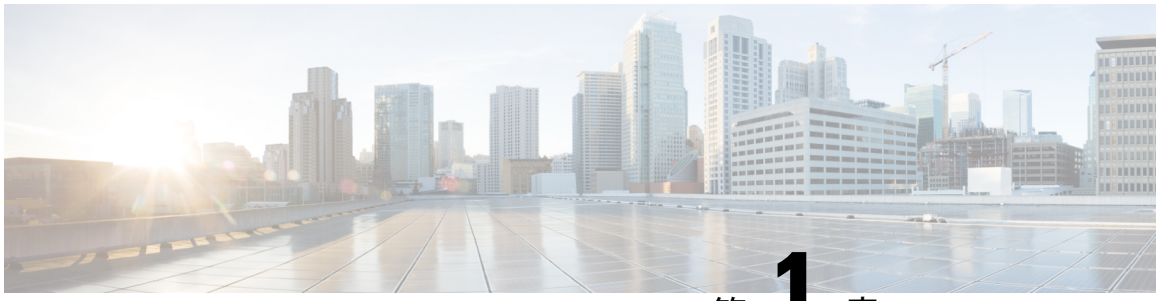
初版：2020 年 9 月 1 日

最終更新：2023 年 9 月 14 日

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：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

目 次



第 1 章

Cisco Enterprise NFVIS について

Cisco Enterprise Network Function Virtualization Infrastructure Software（Cisco Enterprise NFVIS）は、サービスプロバイダーや企業がネットワークサービスを設計、導入、管理できるように設計された、Linux ベースのインフラストラクチャ ソフトウェアです。Cisco Enterprise NFVIS は、サポートされているシスコのデバイスに、仮想ルータ、ファイアウォール、WAN アクセラレータなどの仮想ネットワーク機能を動的に展開するのに役立ちます。このような VNF の仮想化展開は、デバイスの統合にもつながります。個別のデバイスは必要なくなるのです。自動化されたプロビジョニングと中央管理により、コストのかかるトラックロールも不要になります。

Cisco Enterprise NFVIS は、Cisco Enterprise Network Function Virtualization（ENFV）ソリューションに Linux ベースの仮想化レイヤを提供します。

Cisco ENFV ソリューションの概要

Cisco ENFV ソリューションによって、重要なネットワーク機能をソフトウェアに変換し、ネットワークサービスをさまざまな場所に数分で展開することができます。このソリューションは次のような主要コンポーネントを備えており、仮想と物理の両方のデバイスによる多様なネットワークの上部で実行できる、完全に統合されたプラットフォームを実現します。

- Cisco Enterprise NFVIS
- VNF
- ユニファイド コンピューティング システム（UCS）およびエンタープライズ ネットワーク コンピューティング システム（ENCS）のハードウェア プラットフォーム
- Digital Network Architecture Center

Cisco Enterprise NFVIS の利点

- 複数の物理ネットワークアプライアンスを、複数の仮想ネットワーク機能を実行する単一のサーバーに統合。
- サービスを迅速かつタイムリーに展開。
- クラウドベースの VM ライフサイクル管理とプロビジョニング。
- プラットフォーム上で VM を動的に展開およびチェーン化するためのライフサイクル管理。
- プログラム可能な API。

サポートされているハードウェア プラットフォーム

要件に応じて、次のシスコ ハードウェア プラットフォームに Cisco Enterprise NFVIS をインストールできます。

- Cisco 5100 シリーズエンタープライズネットワーク コンピューティング システム（ENCS）
- Cisco 5400 シリーズエンタープライズネットワーク コンピューティング システム（ENCS）
- Cisco Catalyst 8200 シリーズ エッジ ユニバーサル CPE
- Cisco UCS C220 M4 ラック サーバ
- Cisco UCS C220 M5 ラックサーバー
- Cisco Cloud Services Platform 2100（CSP 2100）
- Cisco Cloud Services Platform 5228（CSP-5228）、5436（CSP-5436）、および 5444（CSP-5444 ベータ版）
- UCS-E140S-M2/K9 を搭載した Cisco ISR4331
- UCS-E160D-M2/K9 を搭載した Cisco ISR4351
- UCS-E180D-M2/K9 を搭載した Cisco ISR4451-X
- Cisco UCS-E160S-M3/K9 サーバー
- Cisco UCS-E180D-M3/K9
- Cisco UCS-E1120D-M3/K9

Cisco ENCS

Cisco 5100 および 5400 シリーズのエンタープライズ ネットワーク コンピューティング システムは、ルーティング、スイッチング、ストレージ、処理、およびその他のコンピューティング

やネットワーキングのアクティビティのホストを、小型の 1 つのラックユニット（RU） ボックス内に統合します。この高性能ユニットは、仮想化されたネットワーク機能を導入するためのインフラストラクチャを提供し、処理、ワークロード、およびストレージに関する課題に対処するサーバとして機能することで、この目標を実現します。

Cisco Catalyst 8200 シリーズ エッジ ユニバーサル CPE

Cisco Catalyst 8200 Edge uCPE は、中小規模の仮想化ブランチ向けに、ルーティング、スイッチング、アプリケーションホスティングをコンパクトな1ラックユニットデバイスに統合した次世代のシスコ エンタープライズ ネットワーク コンピューティング システム 5100 シリーズです。これらのプラットフォームは、Cisco NFVIS ハイパーバイザソフトウェアを搭載した同じハードウェア プラットフォーム上で、仮想化されたネットワーク機能やその他のアプリケーションを仮想マシンとして実行できるように設計されています。これらのデバイスは、より多くの WAN ポートを備えた IPSec 暗号化トラフィック用の HW アクセラレーションを搭載した 8 コア x86 CPU です。ブランチ用に異なる WAN、LAN、および LTE/5G モジュールを選択するための NIM スロットと PIM スロットがあります。

Cisco UCS C220 M4/M5 ラックサーバー

Cisco UCS C220 M4 ラックサーバーは、高密度の汎用企業インフラストラクチャおよびアプリケーションサーバーであり、仮想化、コラボレーション、ベアメタルアプリケーションなど、企業の幅広いワークロードに世界クラスのパフォーマンスをもたらします。

Cisco CSP 2100-X1、5228、5436 および 5444（ベータ版）

Cisco Cloud Services Platform は、データセンターのネットワーク機能を仮想化するためのソフトウェアおよびハードウェア プラットフォームです。このオープンなカーネル仮想マシン（KVM）プラットフォームは、ネットワーク仮想サービスをホストするように設計されています。Cisco Cloud Services Platform デバイスを使用すると、ネットワーク、セキュリティ、およびロードバランサのチームが、シスコまたはサードパーティのネットワーク仮想サービスを迅速に展開できます。

（注） CSP 5000 シリーズ デバイスは ixgbe ドライバをサポートしています。

注意 CSP プラットフォームが NFVIS を実行している場合、返品許可（RMA）はサポートされません。

Cisco UCS E シリーズ サーバ モジュール

Cisco UCS E シリーズ サーバ（E シリーズ サーバ）は、Cisco UCS Express サーバの次世代製品です。E シリーズ サーバーは、サイズ、重量、電源効率の点で優れたブレードサーバーファミリであり、第 2 世代のシスコサービス統合型ルータ（ISR G2）、および Cisco 4400、Cisco 4300 シリーズのサービス統合型ルータに格納されています。これらのサーバーは、オペレーティン

グシステム（Microsoft Windows や Linux など）上でベアメタルとして、あるいはハイパーバイザ上で仮想マシンとして導入される分散拠点アプリケーション向けの汎用コンピューティングプラットフォームを提供します。

サポート対象の VM

Cisco Enterprise NFVIS は現在、次の Cisco VM および他社製 VM をサポートしています。

- Cisco Catalyst 8000V Edge ソフトウェア
- シスコサービス統合型仮想（ISRv）
- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）
- 『Cisco Virtual Wide Area Application Services (vWAAS)』
- Linux Server VM
- Windows Server 2012 VM
- Cisco Firepower Next-Generation Firewall Virtual (NGFWv)
- Cisco vEdge
- Cisco XE SD-WAN
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- ThousandEyes
- Fortinet
- Palo Alto
- CTERA
- InfoVista

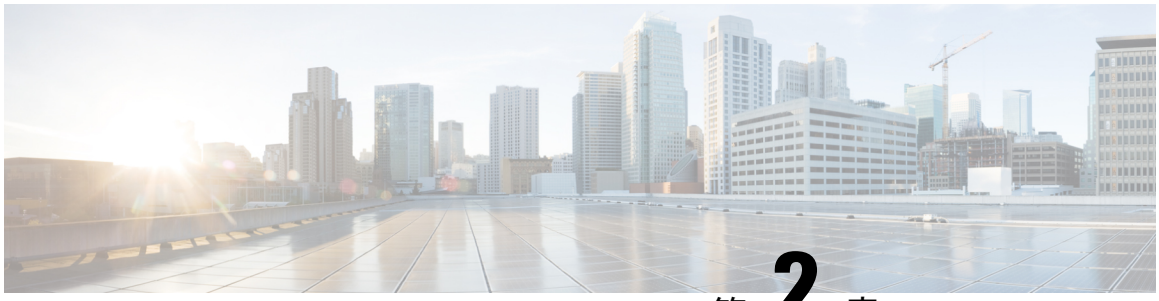
Cisco Enterprise NFVIS で実行できる主なタスク

- VM イメージの登録と展開の実行
- 新しいネットワークとブリッジの作成、およびブリッジへのポートの割り当て
- VM のサービスチェーン化の実行
- VM 操作の実行
- CPU、ポート、メモリ、ディスク統計などのシステム情報の確認
- UCS-E バックプレーン インターフェイスを除く、すべてのプラットフォームのすべてのインターフェイスでの SR-IOV サポート

これらのタスクを実行するための API については、『API Reference for Cisco Enterprise NFVIS』で説明されています。

（注） NFVIS は、すべての設定が YANG モデルを通じて公開されるため、Netconf インターフェイス、REST API、およびコマンド ライン インターフェイスを介して設定できます。

Cisco Enterprise NFVIS コマンド ライン インターフェイスから、SSH クライアントを使用して別のサーバーおよび VM にリモート接続できます。



第 2 章

Cisco Enterprise NFVIS のセットアップ

この章では、エンタープライズ ネットワーク コンピューティング システム（ENCS）5400 シリーズ のプラットフォームデバイスを開梱し、WAN 経由でリモートアクセスできるように設定する方法について説明します。ルータ VNF（仮想ネットワーク機能）インスタンスをプロビジョニングし、LAN から WAN へのトラフィックフローを有効にするよう設定します。

この章では、初期設定のセットアップについて次の導入例を取り上げます。

- コンソールシリアルケーブルを使用したセットアップ
- イーサネットケーブルを使用したセットアップ

60 分でセットアップ全体を完了することができます。

ENCS 5400 プラットフォームデバイスの概要

シスコ エンタープライズ ネットワーク コンピューティング システム（ENCS）5000 シリーズは、仮想化されたソフトウェア定義型ブランチ ネットワーク アーキテクチャ向けに設計されたコンピューティング アプライアンス ファミリです。ENCS は、従来のルータの機能と従来のサーバーを組み合わせた小型のインフラストラクチャ フットプリントを備えた、目的に特化したハイブリッド プラットフォームです。ネットワークサービスや仮想ネットワーク機能（VNF）を数分で展開できます。ENCS の機能の詳細やデータシートについては、「Cisco 5000 シリーズ エンタープライズ ネットワーク コンピューティング システム」を参照してください。

この章では、ENCS 5400 シリーズのデバイスとその主要コンポーネントについて説明します。このシリーズには、次のモデルが含まれます。

- ENCS 5406

- ENCS 5408
- ENCS 5412

インストールの前提条件

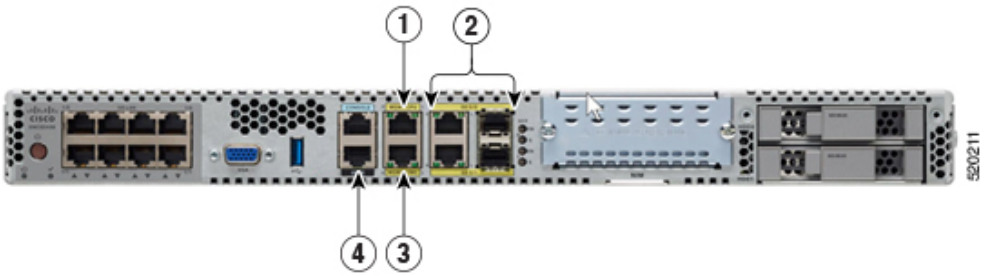
前提条件として、デバイスのセットアップを開始する前に、次のものが揃っていることを確認してください。

- ENCS 5400 デバイスとサポート電源ケーブル
- 1 本のコンソールシリアルケーブル、または適切な長さの 2 本のイーサネットケーブル
- シリアルポート接続をサポートするターミナルソフトウェアを搭載した Windows または Mac のラップトップ
- 管理を目的としてこのアドレスの LAN 上の ENCS デバイスにアクセスするための 1 つの使用可能な LAN IP アドレス（**10.29.43.84** ）。
- LAN 上の ENCS デバイスを管理するためのサブネットマスク（**255.255.255.0**）とゲートウェイ IP アドレス（**10.29.43.1**）。ご使用の環境については、ローカル LAN 管理者にお問い合わせください。

ENCS 5400 シリーズのコンポーネント

ハードウェア

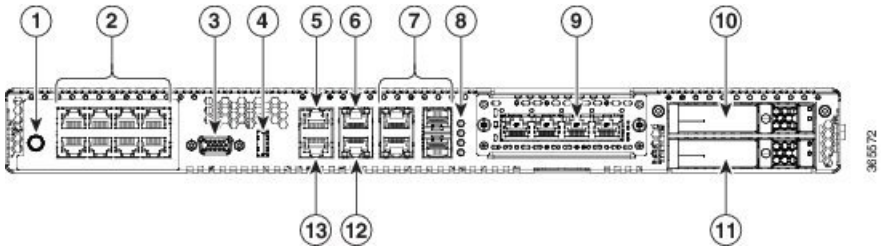
図 *1:* ハードウェアポートのインストール



1	イーサネット管理ポート VNF へのネットワークハイパーバイザ（NFVIS）IP/仮想シリアルコンソールアクセスの管理	2	銅線または光ファイバ WAN ポートを介した NFVIS および VNF の管理 NFVIS と VNF サービスの間で共有される物理ポート

3	CIMC イーサネット接続 CIMC-KVM を介した NFVIS への CLI アクセス	4	CIMC シリアル接続 CIMC を介した NFVIS への CLI アクセス

図 *2 : Cisco 5400 ENCS* の前面パネル



1.	電源オン/オフ スイッチ	2	統合 LAN ポート：一部のモデルではオプションの PoE サポートを利用可能
3	VGA コネクタ	4	USB ポート
5	CPU のシリアルコンソールポート	6	CPU のイーサネット管理ポート
7	前面パネルのギガビット イーサネット ポート	8	前面パネルのギガビット イーサネット ポートの LED
9	ネットワーク インターフェイス モジュール（NIM）	10	ドライブ ベイ 0
11	ドライブ ベイ 1	12	CIMC のイーサネット管理ポート
13	CPU のシリアルコンソールポート		

Cisco IMC

Cisco Integrated Management Controller（CIMC）は、デバイス上でネイティブに実行されるアウトオブバンドの組み込み型管理サービスです。Cisco IMC コンソールには、シリアルコンソールケーブルまたはイーサネットケーブルを通じてアクセスできます。Web ユーザーインターフェイス、コマンド ライン インターフェイス（CLI）、XML API など、複数のインターフェイスをサポートしています。

Cisco IMC から、ファームウェアのアップグレード、BIOS のアップグレード、オペレーティングシステムのインストールとアップグレードなどを実行できます。詳細については、「CIMC アクセス制御」を参照してください。

（注） このガイドでは、Cisco IMC を使用せずに最小限のセットアップを完了させます。

NFVIS

Cisco Network Function Virtualization Infrastructure Software（NFVIS）は、ソフトウェア定義型ブランチネットワーク仮想化展開用のオペレーティング システム ソフトウェアです。NFVIS は、すべての ENCS シリーズのデバイスのオペレーティングシステムです。NFVIS は、オープンソースであるカーネルベースの仮想マシン（KVM）ハイパーバイザを基盤としています。

NFVIS を使用すると、ルータ、ファイアウォールなどの 1 つ以上のネットワークサービスを、単一のハードウェアプラットフォームで仮想ネットワーク機能（VNF）とも呼ばれる仮想マシン（VM）として実行できます。

次の方法で NFVIS にアクセスできます。

- シリアルコンソールケーブルを使用したシリアルコンソールポート
- Web ベースの GUI コンソールにアクセスできる、専用の NFVIS 管理イーサネットポート
- Cisco IMC

この章では、GUI コンソールを使用して ENCS デバイスをセットアップする手順について説明します。

NFVIS の詳細については、「Enterprise NFV Infrastructure Software」を参照してください。

VNF

仮想ネットワーク機能（VNF）とは、仮想ルータ、仮想ファイアウォール、仮想ロードバランサなどの仮想化されたネットワークサービスについて述べるときに使用する総称です。VNF は仮想マシン（VM）と同義です。

すべての ENCS デバイスには、シスコサービス統合型仮想ルータ（ISRv）の仮想アプライアンス イメージ ファイルがプレインストールされています。この章では、このイメージファイルを使用してルータ VNF インスタンスを作成し、LAN 上のトラフィックを WAN に流せるように設定する方法を説明します。

ENCS 5400 の開梱とケーブル接続

デバイスの開梱

デバイス、アクセサリキット、マニュアル、およびオプションの機器は、複数の箱で納品されることがあります。開梱するときは、納品書を確認し、リストのアイテムがすべて揃っていることを確認してください。

インストールする準備が完了してから製品を開梱します。これは、偶発的な損傷を防ぐためです。

ENCS デバイスを梱包箱から取り出し、箱の指示に従ってラックに取り付けます。

ケーブル接続

電源ケーブルをデバイスに接続すると、デバイスの電源が自動的にオンになります。LAN を介してリモートで管理できるように、デバイスで NFVIS 管理 IP アドレスを設定します。

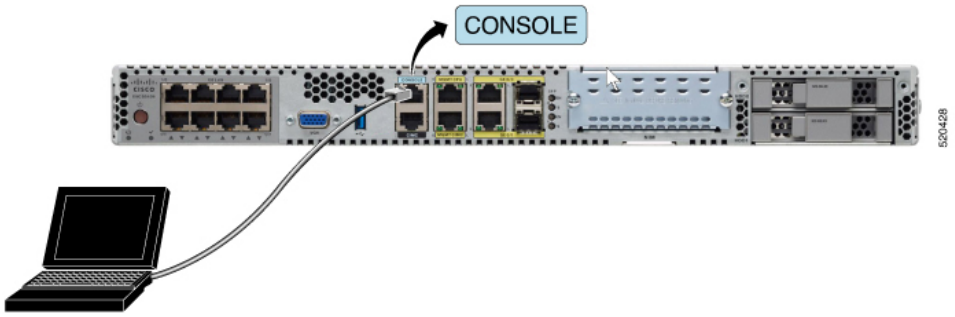
下記を使用して、デバイスで NFVIS 管理 IP アドレスを設定できます。

- シリアルコンソールケーブル：シリアルコンソールケーブルを使用してラップトップをデバイスのシリアルポートに接続し、NFVIS IP アドレスを設定します。さらに、イーサネットケーブルを使用してデバイス管理イーサネットポートをローカル管理ネットワークに接続し、デバイスにリモートアクセスして詳細な設定を行います。

  専用の管理イーサネットポートを介してデバイスにアクセスするには、シリアルコンソールケーブルを使用してデバイス管理 IP アドレスを設定します。その後、インストール手順用に設定されたデバイス管理 IP アドレスを使用して NFVIS ポータルにアクセスできます。

  シリアルコンソールケーブルの一方の端を ENCS デバイスの **CONSOLE** というラベルの付いたポートに接続し、もう一方の端をラップトップのシリアルポートまたは USB ポートに接続します。

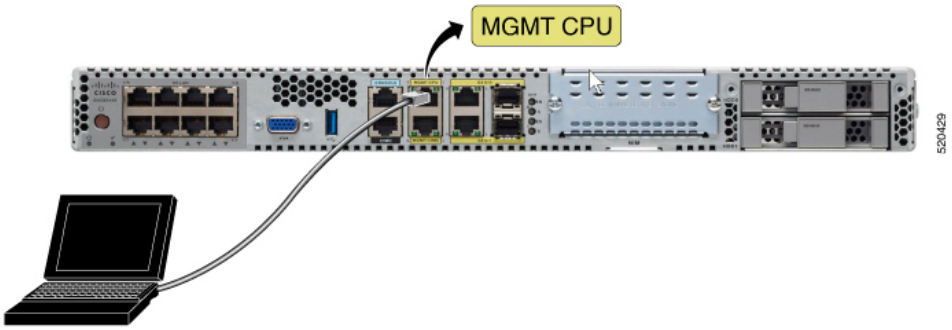
  図 *3:* シリアルコンソールケーブルの接続



- イーサネットケーブル：イーサネットケーブルを使用してラップトップをデバイスの管理イーサネットポートに接続し、NFVIS IP アドレスを設定します。管理ネットワークを介してデバイスをリモートで管理するには、管理ポートをローカル管理ネットワークに再接続します。

  イーサネットケーブルの一方の端を ENCS デバイスの **MGMT CPU** ポートに接続し、もう一方の端をラップトップのイーサネットポートまたはローカルスイッチに接続します。

図 *4:* イーサネットケーブルの接続



ENCS 5400 プラットフォームへの NFVIS のインストール

ENCS デバイスを開梱してケーブル接続した後、次の手順を実行します。

1. LAN 経由でデバイスにリモートアクセスするための NFVIS 管理 IP アドレスを設定します。
2. NFVIS Web ベース GUI コンソールで Cisco ISRv ルータを使用して VNF インスタンスを作成します。
3. LAN から WAN への接続を有効にするように ISRv ルータを設定します。
4. LAN から WAN への接続を検証します。

NFVIS へのアクセス

1. NFVIS への最初のログインでは、デフォルトのユーザー名が **admin** で、デフォルトのパスワードが **Admin123#** です。

```
NFVIS Version: 3.12.3

Copyright (c) 2015-2020 by Cisco Systems, Inc.
Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco
Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

The copyrights to certain works contained in this software are owned by other
third parties and used and distributed under third party license agreements.
Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0,
LGPL 2.1, LGPL 3.0 and AGPL 3.0.
```

2. 最初のログインの直後に、デフォルトのパスワードを変更するように求められます。他のすべての操作は、デフォルトのパスワードが変更されるまでブロックされます。

   パスワードは、以下の規則に従う必要があります。

   - 少なくとも 1 つの大文字と 1 つの小文字を含める必要があります。

- 少なくとも 1 つの数字と 1 つの特殊文字（# _ - * ?）を含める必要があります。
- 7 文字以上にする必要があります。長さは 7 ー 128 文字にする必要があります。

3. パスワードを変更すると、nfvis プロンプトが表示されます。

```
admin connected from ::1 using ssh on nfvis
admin logged with default credentials
Setting admin password will disable zero touch deployment
Do you wish to proceed? [y or n]y
Please provide a password which satisfies the following c
        1.At least one lowercase character
        2.At least one uppercase character
        3.At least one number
        4.At least one special character from # _ - * ?
        5.Length should be between 7 and 128 characters
Please reset the password :
Please reenter the password :


 Resetting admin password


New admin password is set

nfvis#
System message at 2020-01-08 03:10:10...
Commit performed by system via system using system.
nfvis#
```

4. NFVIS にログインすると、NFVIS バージョンに関する情報を確認できます。その後、新しいバージョンのインストールやアップグレードを行うかどうかを決定できます。

```
nfvis#
nfvis# show ver
Cisco NFV Infrastructure Software
Version 4.4.1-FC2
Build date Friday, December 04, 2020 [15:06:41 PST]
Last Reboot Friday, December 04 [22:46]
nfvis#
```

デバイス管理 IP アドレスの設定

1. デバイス管理 IP アドレスを設定します。

```
configure terminal
system settings mgmt ip address 10.29.43.84 255.255.255.0
bridges bridge wan-br no dhcp
bridges bridge wan2-br no dhcp
system settings default-gw 10.29.43.1
commit
end
```

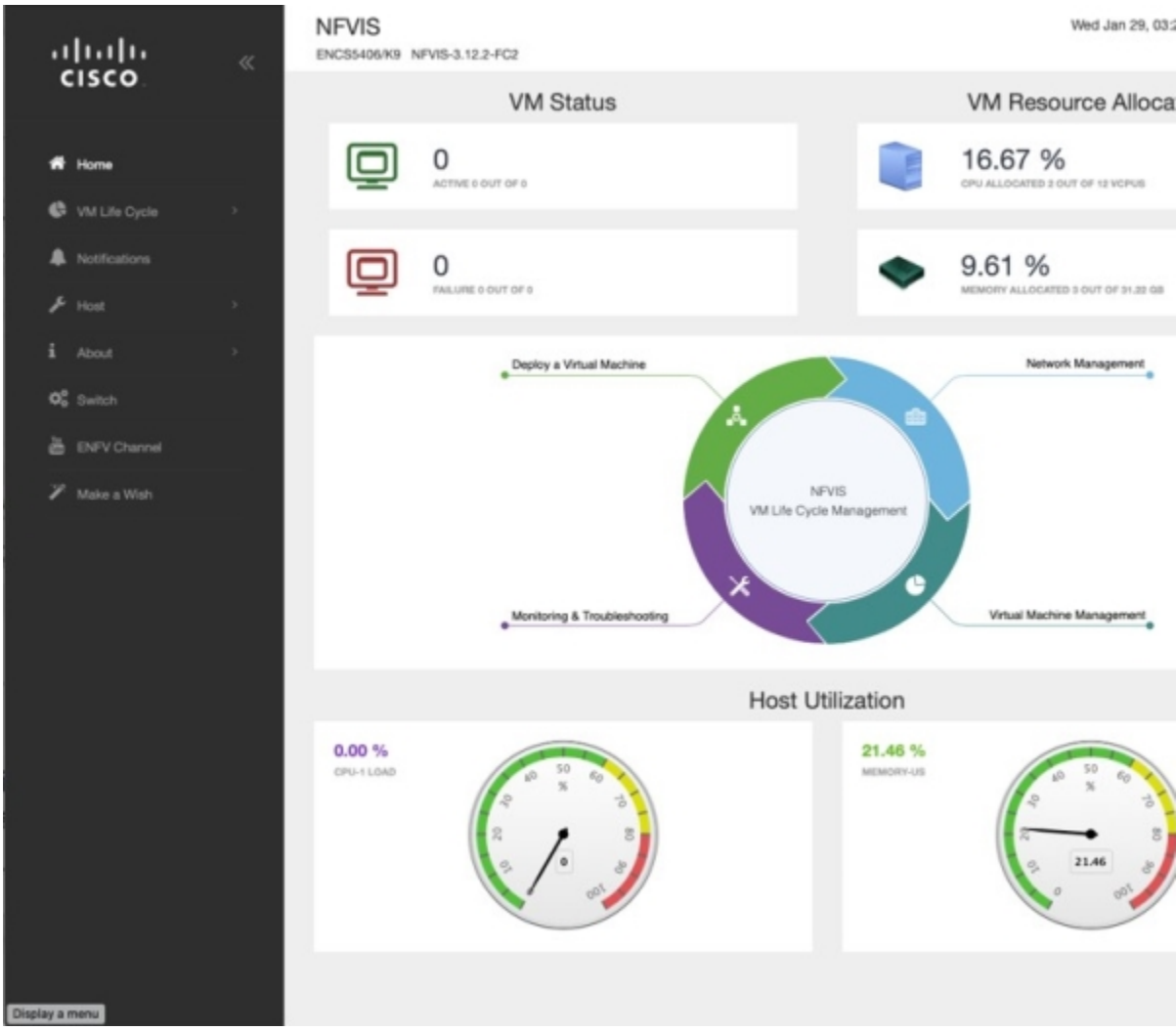
2. これでデバイス管理 IP アドレスが 10.29.43.84 に設定され、このアドレスで NFVIS にリモートでアクセスできます。
3. **show system settings-native** コマンドを使用して設定を確認し、現在の値を表示します。
4. システムからログアウトするには、**Exit** と入力します。

NFVIS ポータルへのアクセス

NFVIS ポータルにアクセスするには、次の手順を実行します。

1. ラップトップをローカルのイーサネット管理ネットワークに接続します。Web ブラウザのアドレスバーに https://10.29.43.84 と入力します。Google Chrome の使用をお勧めします。

2. NFVIS ポータルにログインするためのユーザー名は**admin**、パスワードは新しく生成したパスワードです。デバイスのアクティビティの概要を示すNFVIS ダッシュボードが表示されます。

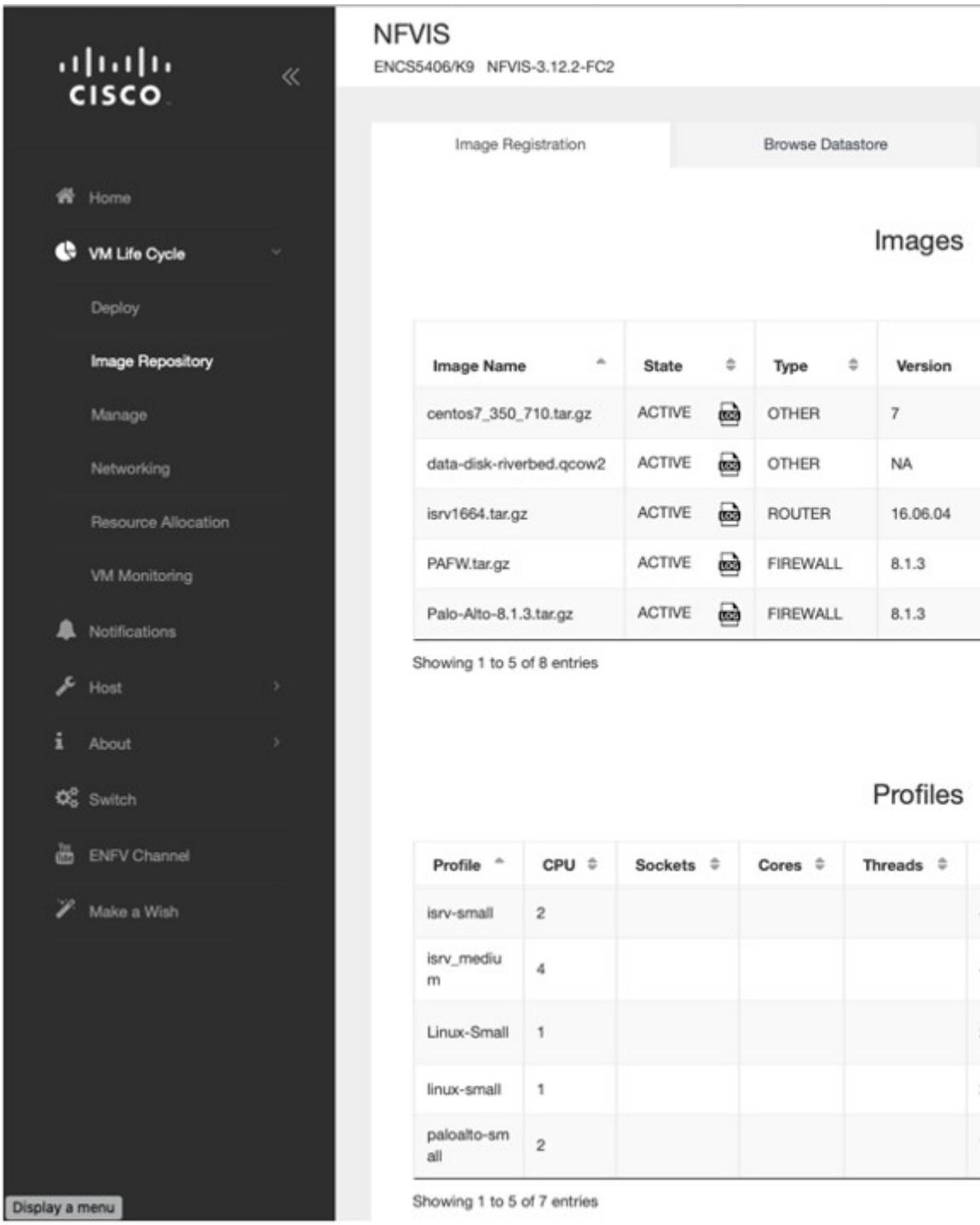


仮想ルータの作成と展開

工場出荷時の ENCS 5400 デバイスに仮想ルータを展開するには、次の手順を実行します。

1. インターフェイスの左側にあるナビゲーションツリーから、**[VMライフサイクル（VM Life Cycle）]>[イメージリポジトリ（Image Repository）]** を選択します。ここには、デバイスにこれまでアップロードされたすべての画像が表示されます。

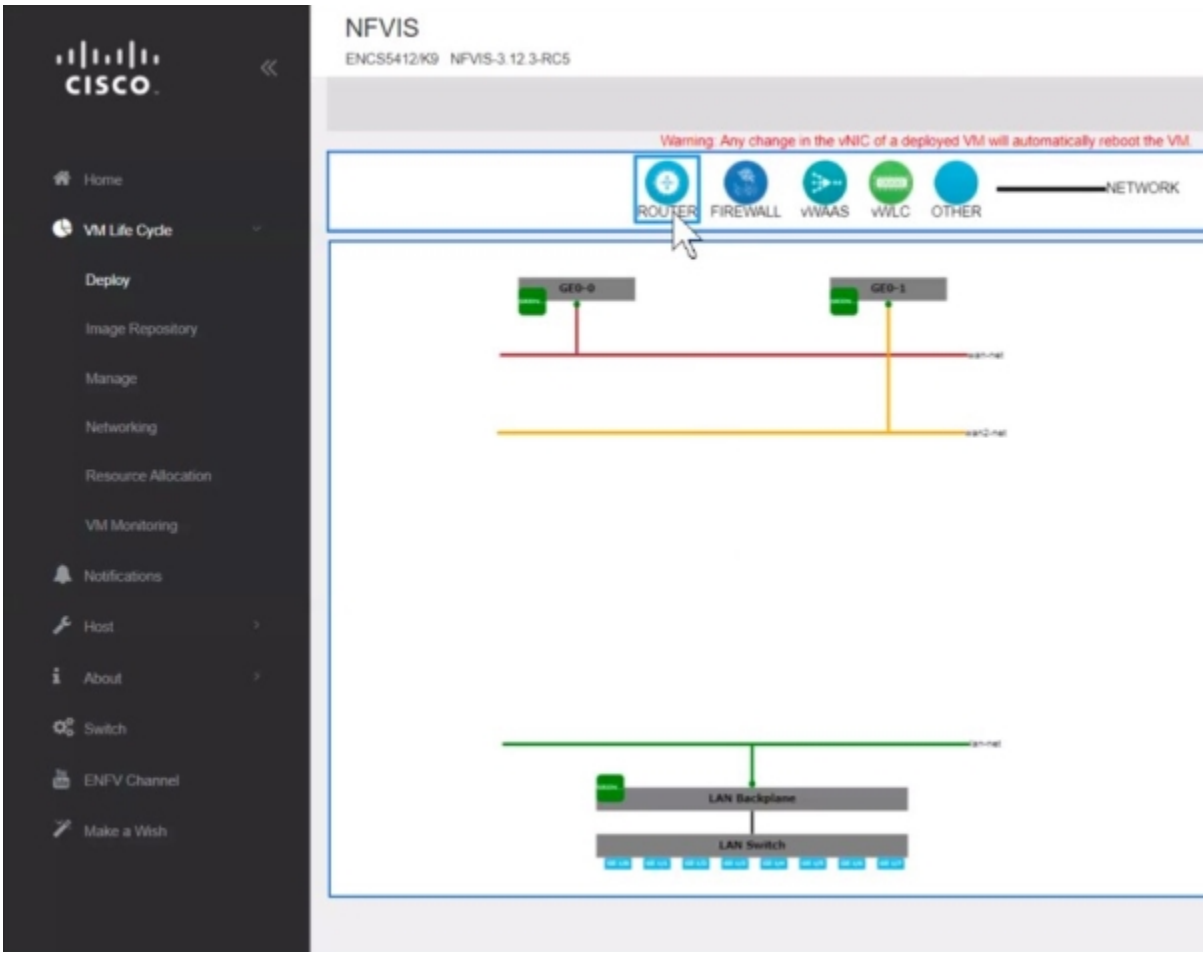
   工場出荷時の ENCS 5400 デバイスの場合、**[イメージ（Images）]** で使用できるイメージは **`isrv.tar.gz`** のみで、**[プロファイル（Profiles）]** には、**`isrv-mini`**、**`isrv-small`**、および**`isrv-medium`**、または **`C8000V-mini`**、**`C8000V-small`**、および **`C8000V-medium`** が表示されます。



[イメージ（Images）] では、使用可能なイメージに関する情報を確認し、必要に応じてアップグレードするためにそのバージョンのメモを取ることができます。イメージの **ACTIVE** 状態は、イメージが登録され、展開の準備ができていることを示します。

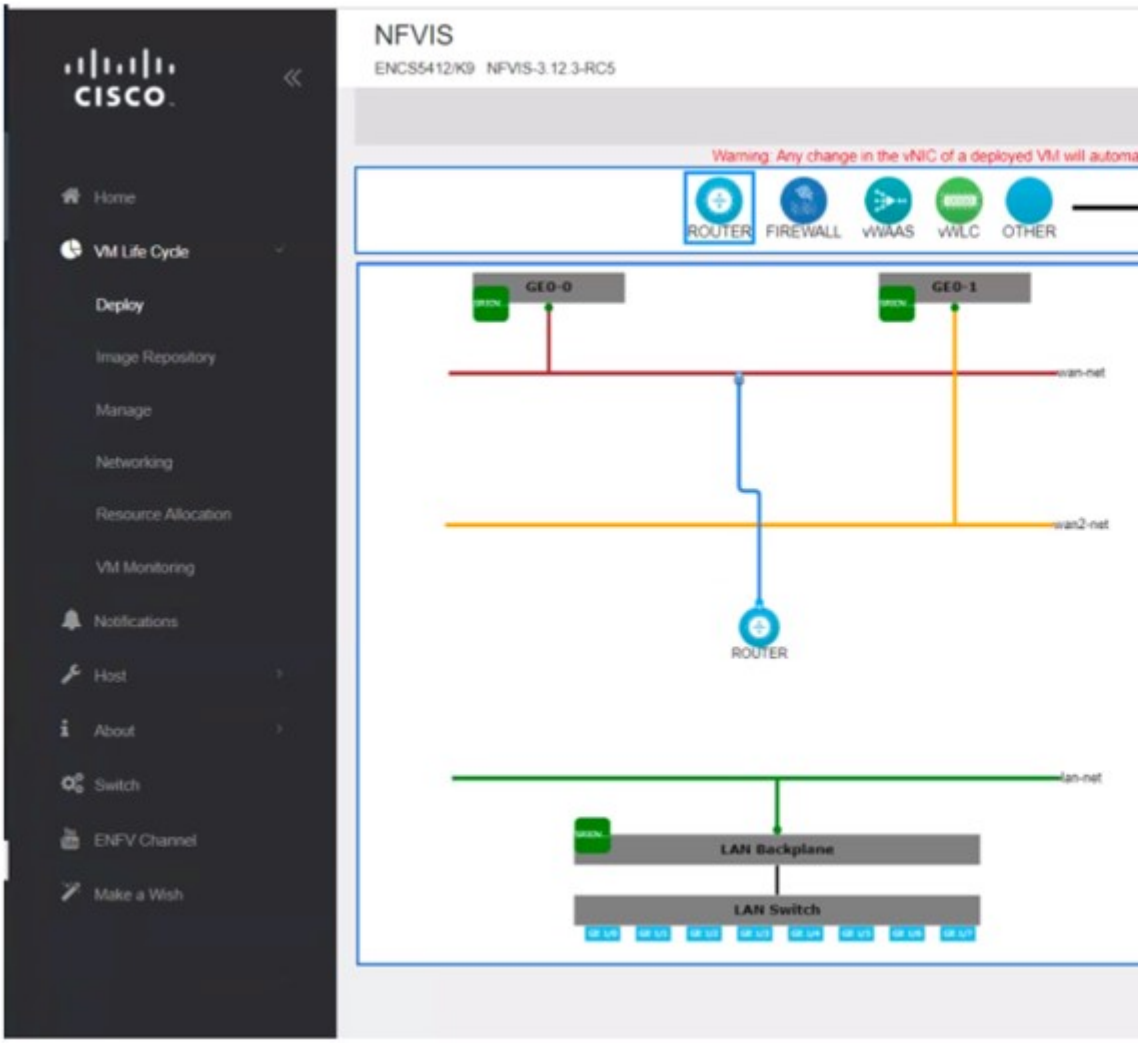
2. **[VMライフサイクル（VM Life Cycle）]** > **[展開（Deploy）]** を選択します。

ページの上部に、さまざまな VNF のカタログを表示できます。ページの中央にあるデバイスのデフォルト設定には、LAN、WAN、および WAN2 ネットワークがあります。



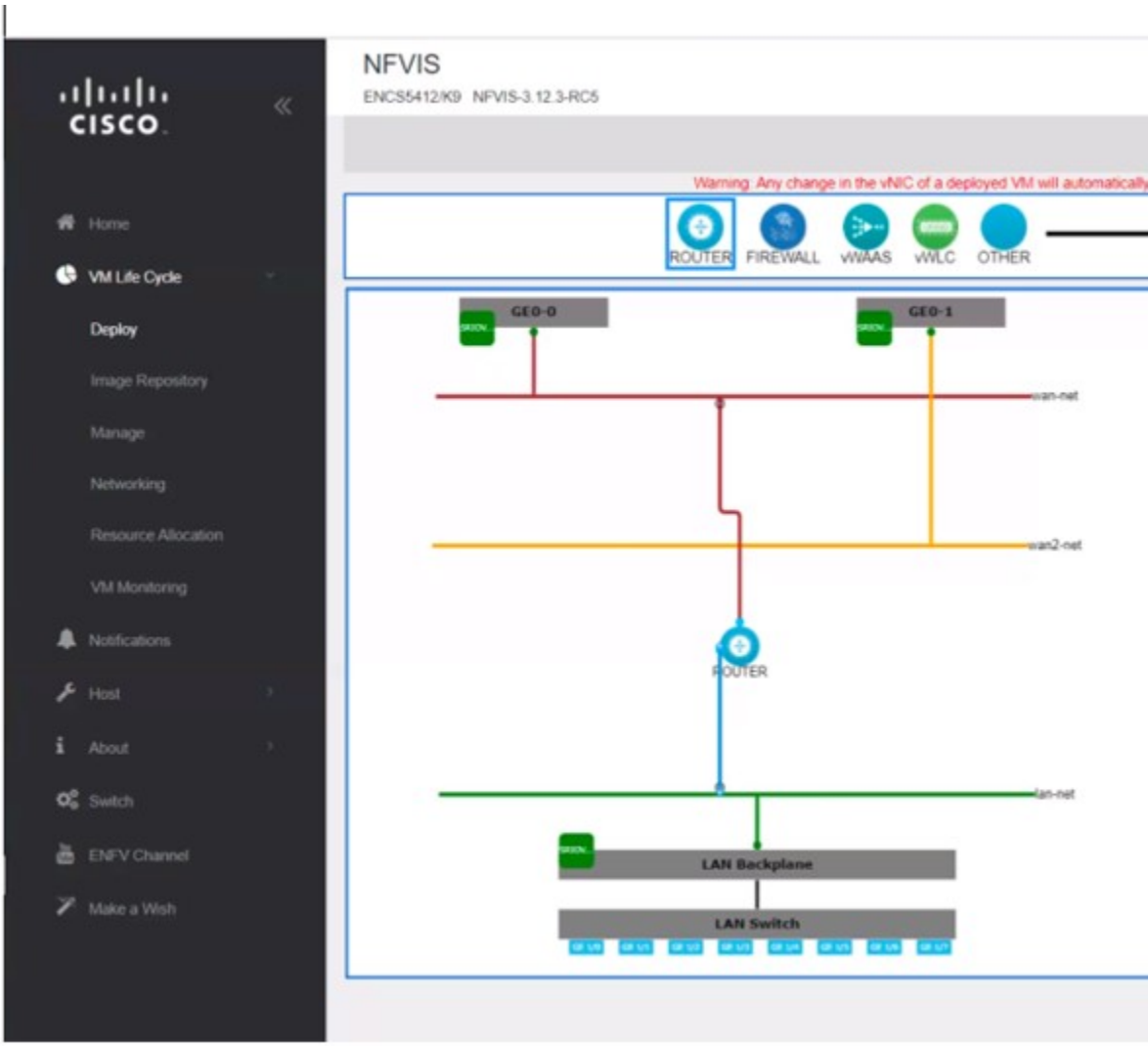
3. LAN および WAN 接続でルータインスタンスを作成するには、**[ルータ（ROUTER）]** をクリックし、ページの中央にドラッグします。WAN への接続を設定するには、ページの **[ルータ（ROUTER）]** をクリックし、**wan-net** 回線にドラッグします。

   接続した回線を選択して詳細を表示します。[vNICの詳細（vNIC details）]ペインで、インターフェイス **GigabitEthernet2** が WAN（**wan-net**）に関連付けられていることを確認できます。後で WAN サブネットを設定するときに同じ名前を使用するため、このインターフェイス名を記録します。



LAN 接続を設定するには、**[ルータ（ROUTER）]** を再度クリックし、今度は **lan-net** 回線にドラッグします。

接続した回線を選択して詳細を表示します。[vNICの詳細（vNIC details）]ペインで、インターフェイス **GigabitEthernet3** が LAN（**lan-net**）に関連付けられていることを確認できます。後でローカルサブネットを設定するときに同じ名前を使用するため、このインターフェイス名を記録します。

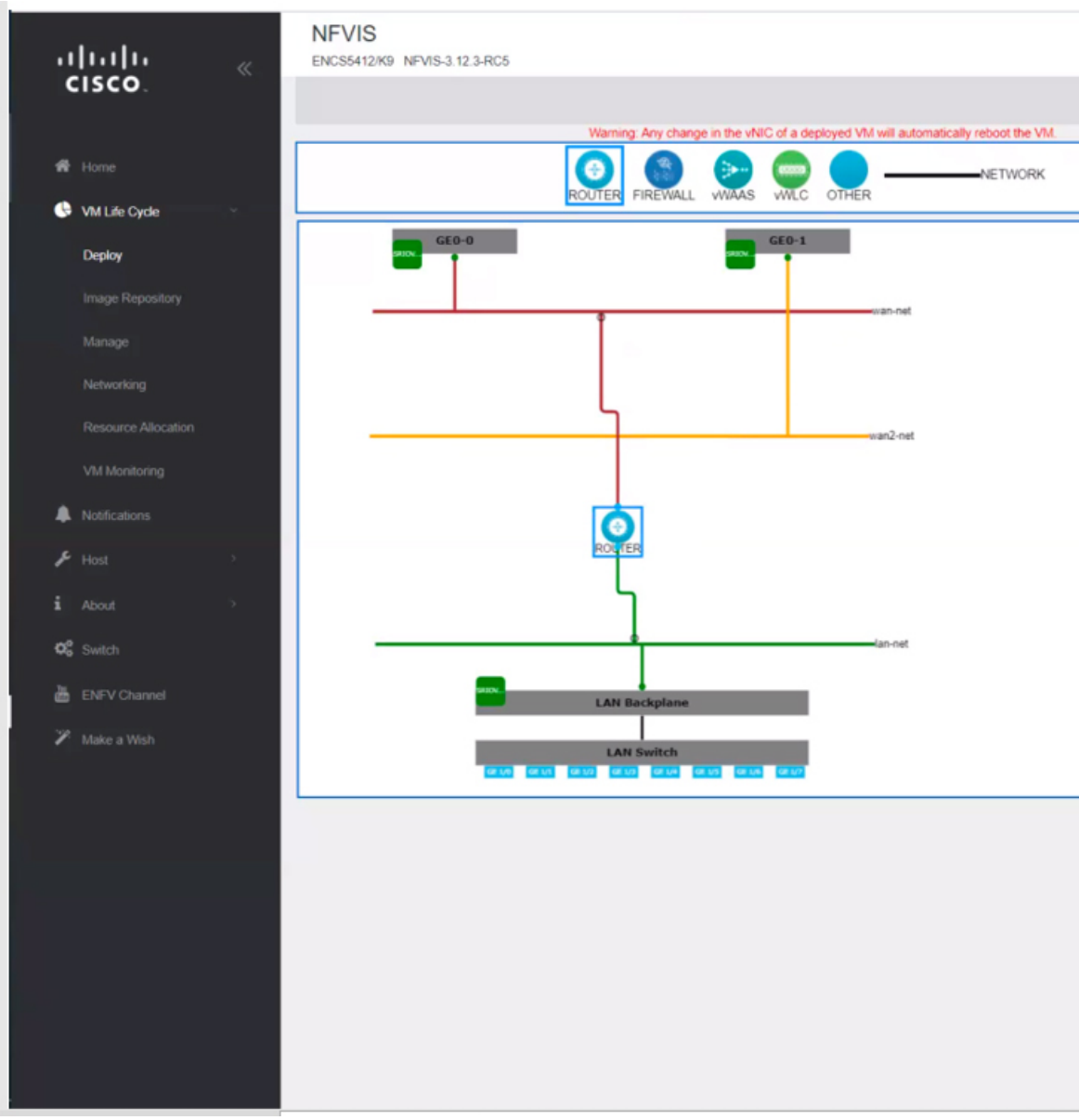


4. **[ルータ（ROUTER）]** をクリックし、**VM の詳細**を入力します。

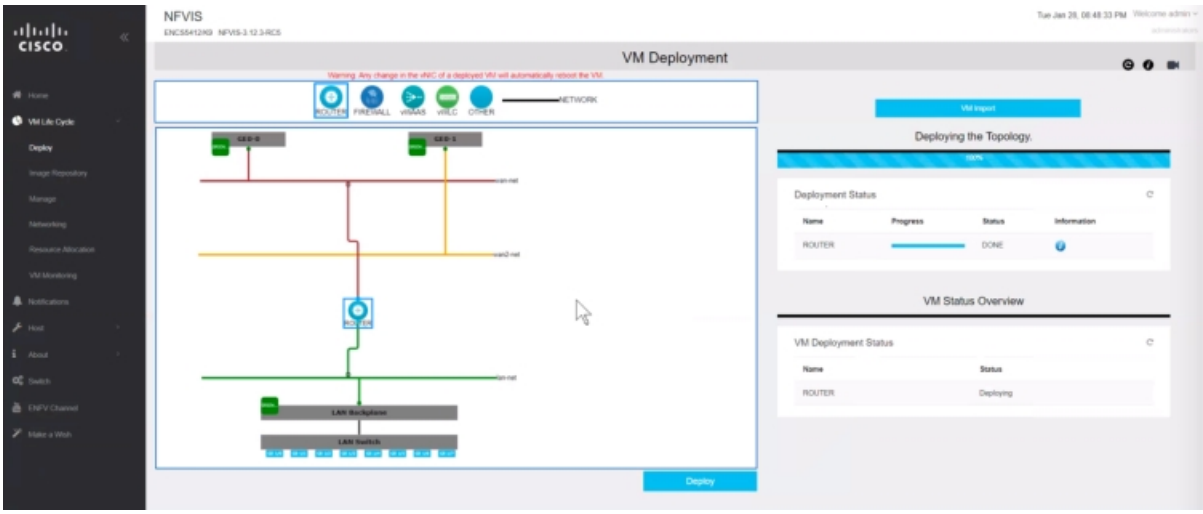
```
Profile: isrv-small
SSH USERNAME: admin
SSH PASSWORD: time44Fun
Port Number: 22
External Port Range: 2001
Source Bridge: MGMT
Deployment Disk: datastore1(internal)
```

これらの値は、VM が 2 つの CPU、4 GB のメモリ、および 8 GB のディスク容量を持つ **isrv-small** プロファイルを使用していることを示しています。**[SSHユーザー名（SSH USERNAME）]** と **[SSHパスワード（SSH PASSWORD）]** で指定したログイン情報を使用して、SSH 経由でこの VM にリモートでログインできます。**[ポート番号（Port Number）]** と **[外部ポート範囲（External Port Range）]** の値は、管理ネットワーク（ソースブリッジ = MGMT）を介した VM への SSH 接続に必要であるため、管理ネットワーク IP アドレス

のポート 2001 を VM のポート番号 22 にマッピングします。この VNF は、datastore1（internal）という名前のデフォルトのデータストアに保存されます。

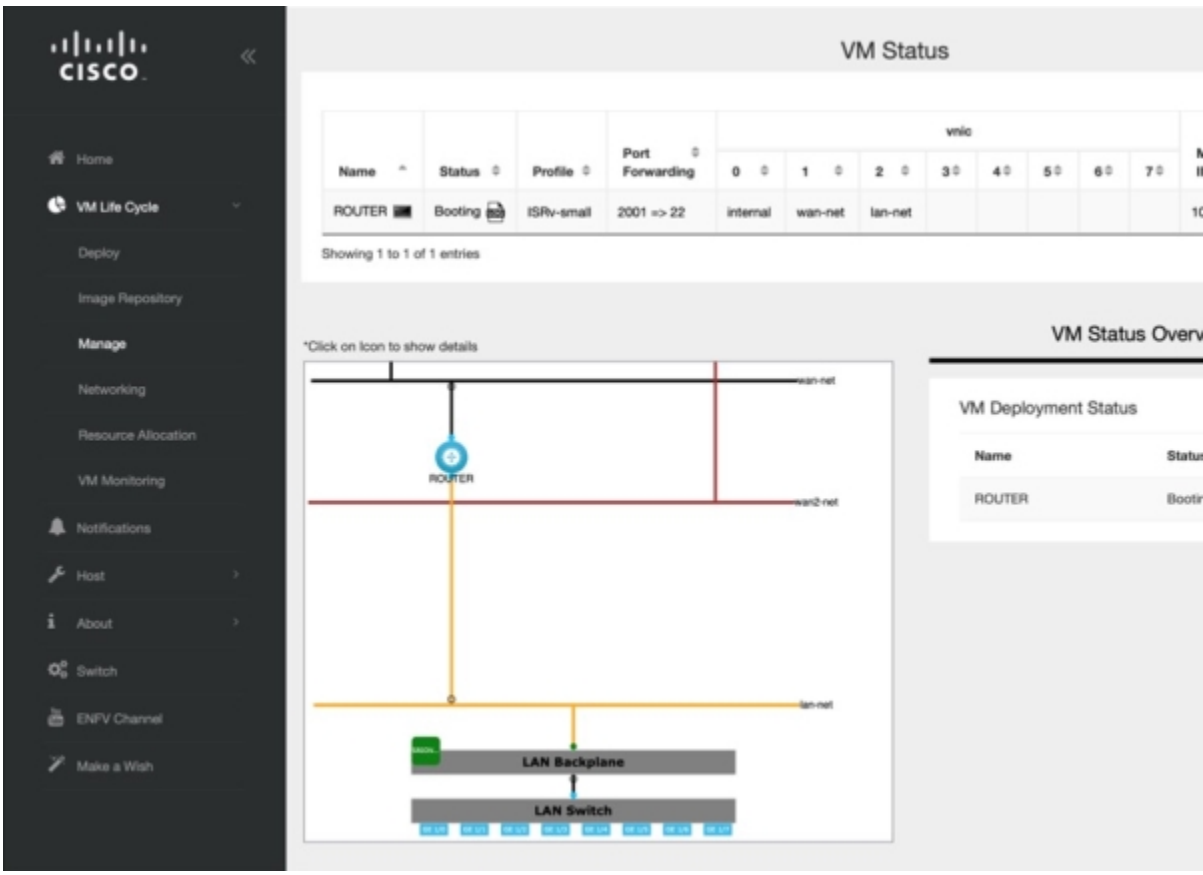


5. **[展開（Deploy）]** をクリックして VM を展開し、ページの右側で展開の進行状況を確認します。展開が成功すると、ページの隅にポップアップメッセージが表示されます。

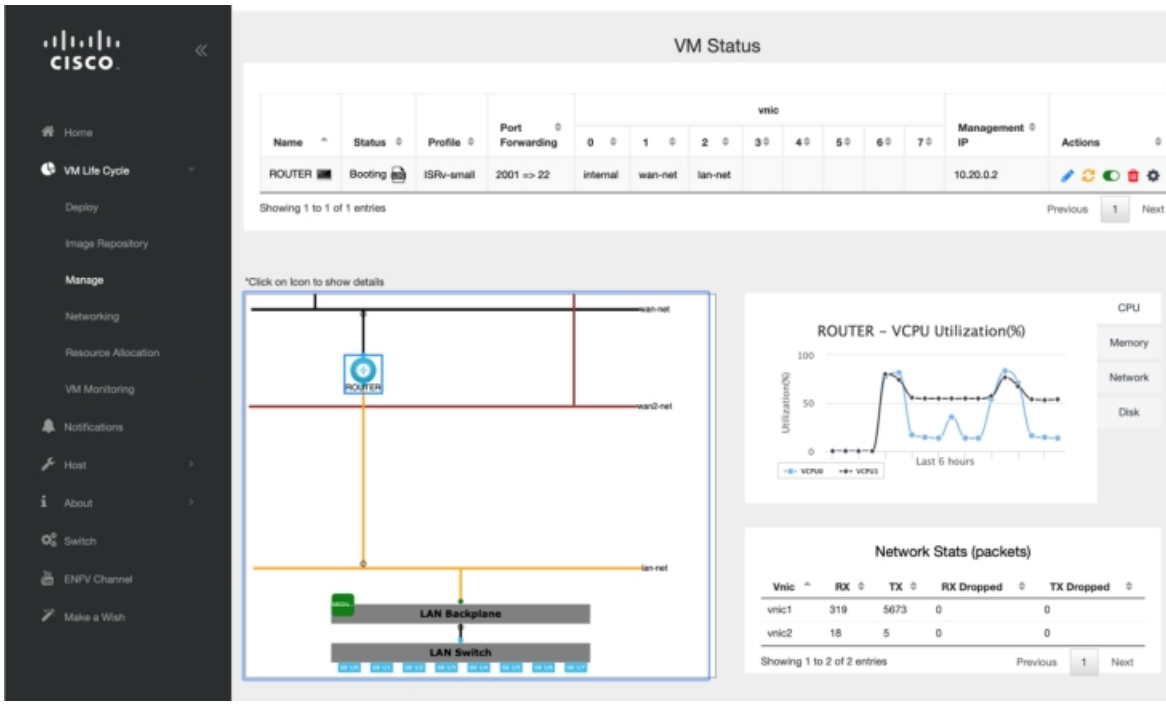


6. ルータ VNF 起動の進行状況をモニターするには、**[VMライフサイクル（VM Life Cycle）]** > **[管理（Manage）]** を選択します。

   展開のステータスは、**[VMステータスの概要（VM Status Overview）]** に表示されます。最新の状態を表示するには、[更新（Refresh）] をクリックします。



7. ルータ VNF の準備ができると、それに関連するすべてのデータを表示できます。

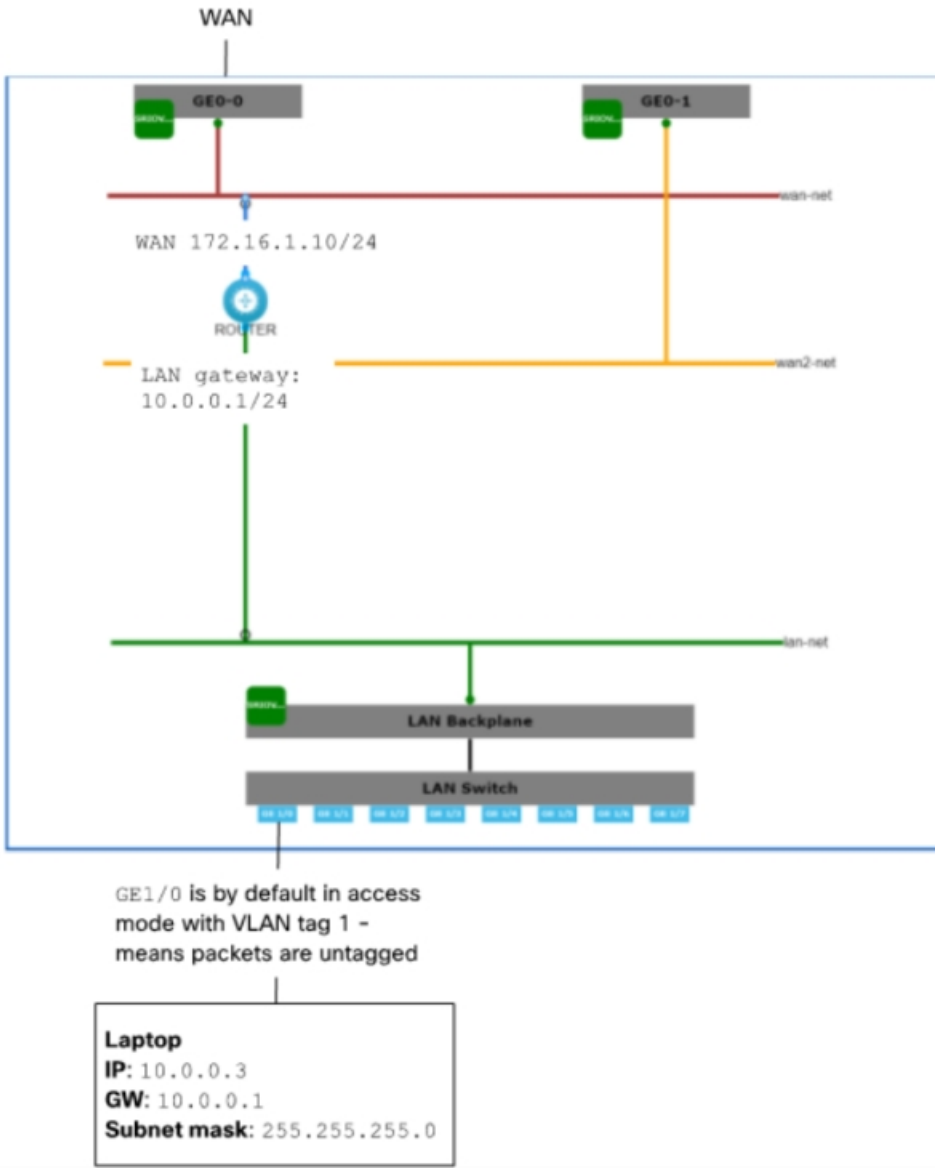


これで、ISRv ルータ VNF インスタンスの作成と展開が完了しました。

LAN と WAN の接続

仮想ルータの作成と展開が正常に完了したら、LAN ネットワークから WAN へのトラフィックフローを有効にするように仮想ルータを設定します。次の図は、仮想ルータを介した LAN から WAN への接続を示しています。

図 *5*: 仮想ルータを介した *LAN* と *WAN* の接続



ラップトップから WAN へのトラフィックフローは、ENCS の物理 8 ポート組み込みスイッチと OVS 仮想スイッチ lan-net を通過します。ラップトップは、イーサネットケーブルで組み込み 8 ポートスイッチのポート GE1/0 に接続されます。ラップトップの静的 IP アドレスは **10.0.0.3**、ゲートウェイ IP アドレスは **10.0.0.1**、サブネットマスクは **255.255.255.0** です。

デフォルトでは、GE1/0 ポートは VLAN タグ 1 でアクセスモードに設定され、内部仮想 lan-net OVS スイッチはトランクモードになり、仮想ルータはタグなしトラフィックを受け入れるように設定されます。

ゲートウェイ IP アドレス **10.0.0.1** は仮想ルータに設定されます。仮想ルータは、WAN への、および WAN からのフロートラフィックを可能にする外部 WAN ポートに接続されます。

ルータ VNF の展開中に、外部ポートと、wan-br や lan-br など、システムへのアクセスを可能にするために使用される同じブリッジを指す source-bridge を設定する必要があります。これで、管理ネットワーク上のラップトップからこのルータ VNF に SSH できるようになります。ログインするには、次の手順を実行します。

```
ssh admin@10.29.43.84:2001
```

VNF インスタンスの作成時に指定したものと同じパスワードを使用します。

```
time44Fun
```

ルータの LAN 側インターフェイスを 10.0.0.1/24 サブネットに設定します。

```
interface GigabitEthernet3
ip address 10.0.0.1 255.255.255.0
```

ルータの WAN 側を設定します。

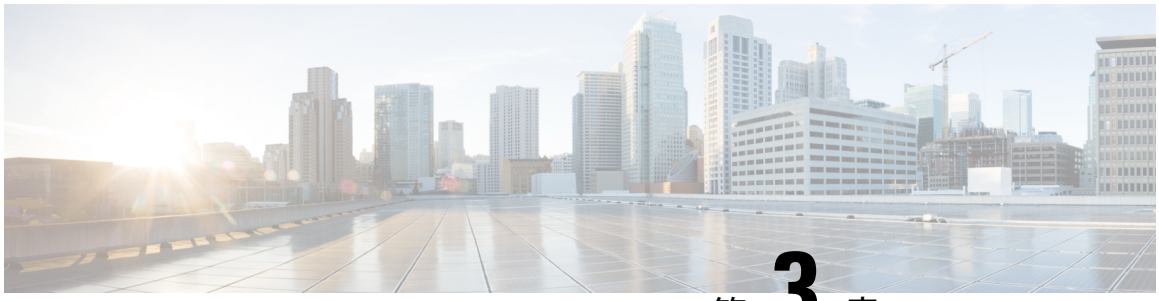
```
interface GigabitEthernet2
ip address 172.16.1.10 255.255.255.0
```

デフォルトルートを設定します。

```
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

これで、ラップトップから WAN 上の任意の接続先に到達できるようになります。

これで、工場出荷時の ENCS 5400 デバイスに仮想ルータが正常に展開されました。詳細設定については、『Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide』を参照してください。



第 3 章

Cisco Enterprise NFVIS のインストール

この章では、サポートされているハードウェア プラットフォームの Cisco IMC および USB を使用して Cisco NFVIS をインストールする方法について説明します。

CIMC を介した NFVIS のインストール

ENCS 5400 プラットフォームへの NFVIS のインストール

ソフトウェアまたはハードウェア RAID コントローラのセットアップは、Cisco ENCS 5400 プラットフォームデバイスではサポートされていません。NFVIS は RAID ディスクグループにインストールされていません。ENCS 5400 プラットフォームデバイスの RAID ディスクグループは、extdatastore にのみ使用されます。

ステップ 1 CIMC にログインします。

ENCS 5400 プラットフォームの推奨 CIMC バージョンは、3.2(7) 以降です。

ステップ 2 KVM コンソールを起動するには、CIMC ホームページから **[KVMの起動（Launch KVM）]** を選択します。

Java または HTML ベースの KVM を選択できます。HTML ベースの KVM の使用をお勧めします。KVM コンソールは別のウィンドウで開くため、ポップアップブロッカーが無効になっていることを確認します。

ステップ 3 KVM コンソールから仮想メディアをマッピングするには、次の手順を実行します。

a) ダウンロードしたファイルを安全にインストールできるかどうかを確認するには、ファイルのチェックサムを比較してから使用する必要があります。チェックサムを確認することで、ネットワーク送信中にファイルが破損したり、ダウンロード前にファイルが悪意のある第三者によって変更されたりしていないことを確認できます。詳細については、「仮想マシンのセキュリティ」を参照してください。

b) **[仮想メディア（Virtual Media）]** を選択し、**[仮想デバイスのアクティブ化（Activate Virtual Devices）]** を選択します。

c) **[仮想メディア（Virtual Media）]** を再度選択し、**[CD/DVDのマッピング（Map CD/DVD）]** を選択します。画面を参照し、Cisco Enterprise NFVIS ISO イメージを選択します。**[ドライブを開いてマッピングする（Open and Map Drive）]** をクリックしてイメージをマウントします。

d) **[仮想メディア（Virtual Media）]** を再度選択し、NFVIS ISO イメージが CD/DVD にマッピングされたことを確認します。

ステップ 4 起動順序を設定するには、次の手順を実行します。

a) **[CIMCコンピューティング（CIMC Compute）]** から、**[BIOS]** を選択します。

b) **[起動順序の設定（Configure Boot Order）]** を選択すると、**[起動順序の設定（Configure Boot Order）]** ダイアログボックスが表示されます。

c) **[CD/DVD]** ページで、**[Cisco vKVMにマッピングされたvDVD（Cisco vKVM-Mapped vDVD）]** を選択し、**[追加（Add）]** を選択します。

d) **[HDD]** から **[RAIDアダプタ（RAID Adapter）]** を選択し、**[追加（Add）]** をクリックします。

a) [Up] および [Down] オプションを使用して、起動の順序を設定します。**Cisco vKVM にマッピングされた vDVD** の起動順序を最初に選択する必要があります。**[変更を保存（Save Changes）]** をクリックして、起動順序の設定を完了します。

（注） CIMC を介して UEFI の起動順序を設定する場合、サポートされる BIOS バージョンは 2.10 以降です。他の BIOS バージョンを使用する場合は、BIOS セットアップメニューで UEFI 起動順序を設定し、**[BootOrderRules]** を **[Loose]** に設定する必要があります。

UEFI の起動順序を設定するには、次の手順を実行します。

a) **[CIMCコンピューティング（CIMC Compute）]** から、**[BIOS]** を選択します。

b) **[起動順序の設定（Configure Boot Order）]** を選択すると、**[起動順序の設定（Configure Boot Order）]** ダイアログボックスが表示されます。

c) **>>**、**<<**、**[上（up）]**、および **[下（down）]** ボタンを使用して、**UEFI イメージマップ**をユーザーインターフェイスの右側の列の最初のオプションにします。

d) **>>**、**<<**、**[上（up）]**、および **[下（down）]** ボタンを再度使用して、**UEFI OS** をユーザーインターフェイスの右側の列の 2 番目のオプションにします。

e) [変更の保存（Save Changes）] をクリックします。

CLI を使用して UEFI の起動順序を設定することもできます。下記に、CLI を使用して UEFI の起動順序を設定する例を示します。

```
Server# scope bios
Server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
  from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
  The configured list will be appended by the additional device types
  seen by the BIOS
Server /bios *# commit
Server /bios #
Server /bios # show detail
BIOS:
    BIOS Version:"UCSEDM3.2.10b5 (Build Date:02/27/2020)"
    Boot Order: UEFIMAP,UEFIOS
```

```
FW Update/Recovery Status: None, OK
Active BIOS on next reboot: main
UEFI Secure Boot: enabled
```

ステップ 5 サーバーの電源を再投入して、インストールを開始します。

CIMC ホームページから、**[ホスト電源（Host Power）]** を選択します。**[電源オフ（Power Off）]** オプションを選択して、サーバーを再起動します。サーバーの電源が切れたら、**[電源オン（Power On）]** オプションを選択します。

サーバーが再起動すると、KVM コンソールによって、仮想 CD/DVD ドライブから Cisco Enterprise NFVIS が自動的にインストールされます。インストールが完了するまで 30 分～ 1 時間ほどかかることがあります。

ステップ 6 ENCS 5400 プラットフォームでは、ファームウェアが自動アップグレードされます。

NFVIS 3.8.x リリース以降、ファームウェアの自動アップグレードがサポートされています。NFVIS のインストールが完了すると、BIOS または CIMC は対応するバージョンに自動的にアップグレードされます。CIMC と NFVIS は複数回再起動されます。ファームウェアのアップグレードが完了するまで 30 分～ 1 時間ほどかかることがあります。ファームウェアのアップグレード中は、システムを使用しないでください。

ステップ 7 インストールが完了すると、システムはハードドライブから自動的に再起動されます。再起動後にコマンドプロンプト **nfvis login** が表示されたら、システムにログインします。

ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123＃** を使用します。

（注） 初めてログイン試行すると、デフォルトのパスワードを変更するように求められます。アプリケーションを続行するには、画面の指示に従って強力なパスワードを設定する必要があります。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。デフォルトのパスワードがリセットされていない場合、API は 401 未承認エラーを返します。

ステップ 8 システム API または CLI を使用するか、Cisco Enterprise NFV ポータルからシステム情報を表示して、インストールを確認します。

ステップ 9 ホスト名を設定し、NFVIS にアクセスするための管理 IP アドレスを割り当てます。

管理アクセス用にイーサネット管理ポートをネットワークに接続します。NFVIS のイーサネットを介した IP アドレスベースのアクセスを有効にするには、シリアルコンソール接続ポートを使用します。

Cisco ENCS のデフォルトのシステム設定

次の図は、Cisco ENCS を搭載した Cisco Enterprise NFVIS のデフォルトのネットワーク設定を示しています。

図 *6 : Cisco ENCS 5400* を搭載した *Cisco Enterprise NFVIS* のデフォルトのネットワーク設定

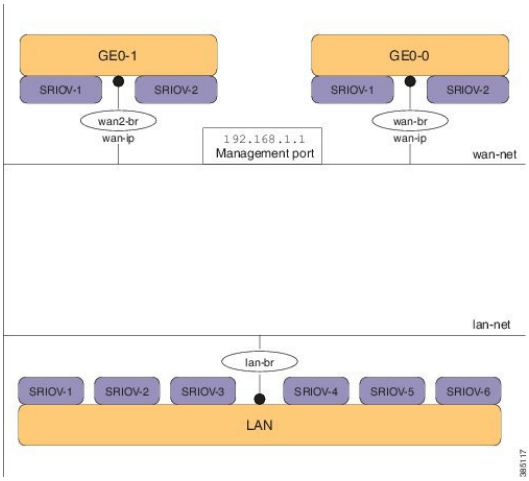
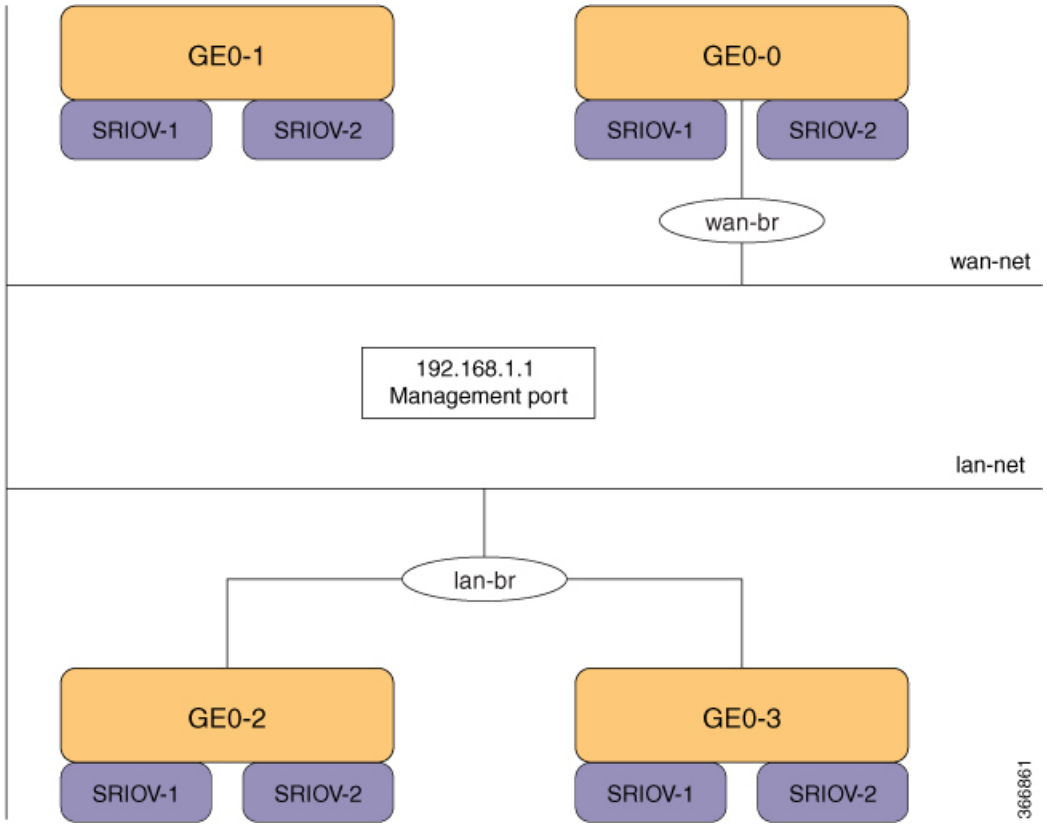


図 *7 : Cisco ENCS 5100* を搭載した *Cisco Enterprise NFVIS* のデフォルトのネットワーク設定



- LAN ポート：インバウンドおよびアウトバウンドのトラフィック用の 8 個の物理ギガビット イーサネット ポート。
- WAN ポート：デュアル メディア イーサネット ポート（wan-br および wan2-br）の 1 つを DHCP 接続に使用できます。

- ブリッジ：VM の仮想ネットワーク インターフェイス コントローラ（vNIC）間でレイヤ 2 ドメインを形成します。vNIC は仮想マシンが使用し、MAC アドレスの範囲を定義することによって仮想ネットワーク インターフェイスを提供します。NFVIS ホストのデフォルトの管理 IP アドレス（192.168.1.1）は、管理ポートで設定されます。複数の VM がローカル接続に同じ LAN ポートを使用できます。
- ネットワーク：特定の VLAN トラフィックのみが許可されるセグメントレイヤ 2 ブリッジドメインです。
- ENCS 5400 プラットフォーム上の LAN ネットワークの予約済み VLAN：VLAN 範囲 2350 ～ 2449 は内部使用のために予約されているため、外部スイッチポートおよび LAN ポートの仮想マシンには使用できません。この制限は WAN ポートには適用されないことに注意してください。
- 内部 192.168.10.00/24 および 192.168.50.0/24 ネットワーク：IP サブネット 192.168.10.0/24 および 192.168.50.0/24 は ENCS-5400 内部ネットワークに使用されます。ユーザーは、NFVIS 管理ネットワークでこの IP サブネットを使用しないでください。今後の NFVIS リリースでは、ユーザーが NFVIS 管理に使用できるように、この内部サブネットが分離されます。

（注） 次のネットワークとブリッジは自動的に設定されます。必要に応じてさらに設定できます。

- LAN ネットワーク（lan-net）および LAN ブリッジ（lan-br）
- WAN ネットワーク（wan-net）および WAN ブリッジ（wan-br）

wan2-net および wan2-br は、ENCS 5400 および ENCS 5100 のデフォルト設定です。

デフォルトのネットワークとブリッジは削除できません。

USC C シリーズ サーバーおよび CSP プラットフォームへの NFVIS のインストール

UCS-C シリーズのデバイスでは、NFVIS をインストールする前に RAID ディスクグループを設定する必要があります。UCS-C は、新規インストール用の単一の RAID ディスクグループのみをサポートしています。

（注） NFVIS 4.6 リリース以降、USC C シリーズ サーバーおよび CSP プラットフォームは最大 3 つの RAID グループをサポートしています。最初の RAID グループは OS のインストール用に予約されており、他の RAID グループは外部ストレージドライブとして使用できます。

ステップ 1 CIMC にログインします。

USC-C シリーズ サーバーおよび Cisco CSP プラットフォームの推奨 CIMC バージョンは、3.0(3c) 以降のバージョンです。

ステップ 2 KVM コンソールを起動するには、CIMC ホームページから **[KVMの起動（Launch KVM）]** を選択します。

Java または HTML ベースの KVM を選択できます。HTML ベースの KVM の使用をお勧めします。KVM コンソールは別のウィンドウで開くため、ポップアップブロッカーが無効になっていることを確認します。

ステップ 3 KVM コンソールから仮想デバイスをマッピングするには、次の手順を実行します。

a) ダウンロードしたファイルを安全にインストールできるかどうかを確認するには、ファイルのチェックサムを比較してから使用する必要があります。チェックサムを確認することで、ネットワーク送信中にファイルが破損したり、ダウンロード前にファイルが悪意のある第三者によって変更されたりしていないことを確認できます。詳細については、「仮想マシンのセキュリティ」を参照してください。

b) **[仮想メディア（Virtual Media）]** を選択し、**[仮想デバイスのアクティブ化（Activate Virtual Devices）]** を選択します。

c) **[仮想メディア（Virtual Media）]** を再度選択し、**[CD/DVDのマッピング（Map CD/DVD）]** を選択します。画面を参照し、Cisco Enterprise NFVIS ISO イメージを選択します。**[ドライブを開いてマッピングする（Open and Map Drive）]** をクリックしてイメージをマウントします。

d) **[仮想メディア（Virtual Media）]** を再度選択し、NFVIS ISO イメージが CD/DVD にマッピングされたことを確認します。

ステップ 4 起動順序を設定するには、次の手順を実行します。

a) **[CIMCコンピューティング（CIMC Compute）]** から、**[BIOS]** を選択します。

b) **[起動順序の設定（Configure Boot Order）]** を選択すると、**[起動順序の設定（Configure Boot Order）]** ダイアログボックスが表示されます。

c) [詳細設定（Advanced）] を選択します。

d) **[起動デバイスの追加（Add Boot Device）]** ページが表示されます。**[仮想メディアの追加（Add Virtual Media）]** を選択すると、**[仮想メディアの追加（Add Virtual Media）]** ダイアログボックスが表示されます。

e) 名前を入力し、**[KVMにマッピングするDVD（KVM Mapped DVD）]** を選択します。状態を **[有効（Enabled）]**、順序を 1 に設定し、**[変更を保存（Save Changes）]** を選択します。

f) **[起動デバイスの追加（Add Boot Device）]** ページが再度表示されるので、**[ローカルHDDの追加（Add Local HDD）]** を選択すると、**[仮想メディアの追加（Add Virtual Media）]** ダイアログボックスが表示されます。

g) 名前を入力し、状態を **[有効（Enabled）]**、順序を 2 に設定し、**[変更を保存（Save Changes）]** を選択します。

h) [**閉じる（Close）**] をクリックします。

ステップ 5 サーバーの電源を再投入して、インストールを開始します。

CIMC ホームページから、**[ホスト電源（Host Power）]** を選択します。**[電源オフ（Power Off）]** オプションを選択して、サーバーを再起動します。サーバーの電源が切れたら、**[電源オン（Power On）]** オプションを選択します。

サーバーが再起動すると、KVM コンソールによって、仮想 CD/DVD ドライブから Cisco Enterprise NFVIS が自動的にインストールされます。インストールが完了するまで 30 分～ 1 時間ほどかかることがあります。

ステップ 6 インストールが完了すると、システムはハードドライブから自動的に再起動されます。再起動後にコマンドプロンプト **nfvis login** が表示されたら、システムにログインします。

ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123＃** を使用します。

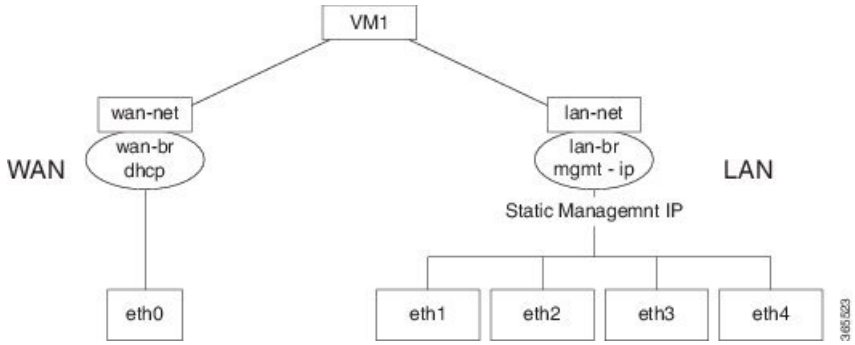
（注） 初めてログイン試行すると、デフォルトのパスワードを変更するように求められます。アプリケーションを続行するには、画面の指示に従って強力なパスワードを設定する必要があります。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。デフォルトのパスワードがリセットされていない場合、API コマンドは 401 未承認エラーを返します。

ステップ 7 システム API または CLI を使用するか、Cisco Enterprise NFV ポータルからシステム情報を表示して、インストールを確認します。

Cisco UCS C220 M4 サーバーおよび Cisco CSP 2100 のデフォルトのシステム設定

Cisco Enterprise NFVIS でネットワークを設定すると、インバウンドおよびアウトバウンドのトラフィックと VM をサービスチェーン化できます。次の図は、デフォルトのネットワーク設定を示しています。

図 *8 : Cisco UCS C220 M4* および *Cisco CSP 2100* でのデフォルトのネットワーク設定



次のネットワークとブリッジはデフォルトで作成され、削除できません。必要に応じてさらに設定できます。

- LAN ネットワーク（lan-net）と LAN ブリッジ（lan-br）：NFVIS ホストのデフォルトの静的管理 IP アドレス（192.168.1.1）は、LAN ブリッジで設定されます。インバウンドおよびアウトバウンドのトラフィック用のポートの 1 つは、LAN ブリッジに関連付けられます。任意の LAN ポートを使用して、デフォルトの静的 IP アドレスにアクセスできます。デフォルトでは、ホスト名は「nfvis」に設定されます。
- WAN ネットワーク（wan-net）と WAN ブリッジ（wan-br）：これは「eth0」ポートで作成され、DHCP 接続を有効にするように設定されます。

デフォルトでは、デバイスの最初のポートが WAN ブリッジに関連付けられます。デバイスの他のポートの 1 つは LAN ブリッジに関連付けられます。

初期セットアップの詳細については、『*Cisco UCS C220 M4* サーバーのインストールおよびサービスガイド』または『*Cisco Cloud Services Platform 2100* ハードウェアのインストールガイド』の「サーバーのインストール」の章を参照してください。

UCS-E シリーズ サーバーへの NFVIS のインストール

- UCS-E シングルワイドは、新規インストール用の単一の RAID ディスクグループのみをサポートしています。UCS-E ダブルワイド シリーズは、NFVIS 4.1 の新規インストール用のシングルまたはデュアル RAID ディスクグループ、または NFVIS 3.X の新規インストール用の 1 つの RAID ディスクグループをサポートしています。
  - シングルディスクグループ（4 ディスク）：RAID0/RAID1/RAID10/RAID5。FDE ディスクを使用する場合は、Secured RAID0/RAID1/RAID10/RAID5 を有効にすることもできます。
  - デュアルディスクグループ（各 2 ディスク）：RAID0/RAID1 または （FDE ディスクを使用する場合）Secured RAID0/RAID1。NFVIS のインストールは、JBOD ディスクを使用した構成をサポートしていません。

  詳細については、「UCS-E デバイスの RAID を使用したストレージの管理」を参照してください。
- Cisco ISR ルータでギガビット イーサネット インターフェイスを設定します。
- Cisco ISR ルータで UCS E インターフェイスを設定します。次の設定例は、DHCP が有効になっている Cisco ISR 4451 ルータで実行される基本設定を示しています。

```
Last configuration change at 02:36:37 UTC Thu Feb 18 2016
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname NFVIS-ISR4451
!
boot-start-marker
boot system bootflash:isr4300-universalk9.03.16.01a.S.155-3.S1a-ext.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
!
!
!
```

```
ip domain name cisco.com
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
!
license udi pid ISR4331/K9 sn FDO192207MN
!
!
ucse subslot 1/0
 imc access-port shared-lom console
 imc ip address 172.19.183.172 255.255.255.0 default-gateway 172.19.183.1
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
vlan internal allocation policy ascending
!
!
!
interface GigabitEthernet0/0/0
 ip address 172.19.183.171 255.255.255.0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface ucse1/0/0
 ip unnumbered GigabitEthernet0/0/0
 negotiation auto
 switchport mode trunk
 no mop enabled
 no mop sysid
!
interface ucse1/0/1
 no ip address
 no negotiation auto
 switchport mode trunk
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
```

```
interface Vlan1
 no ip address
 shutdown
!
ip default-gateway 172.19.183.1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 172.19.183.1
ip route 172.19.183.172 255.255.255.255 ucse1/0/0
ip ssh version 2
!
!
!

control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login local
 transport input all
 transport output all
!
!
end
```

（注） サポートされている次のファームウェアバージョン以上が使用可能であることを確認してください。

- UCS-E160D-M2/K9 および UCS-E180D-M2/K9 の BIOS UCSED.2.5.0.3 以降
- UCS-E140S-M2/K9 の BIOS UCSES.1.5.0.5 以降
- UCS-E160S-M3 の BIOS UCSEM3_2.5 以降
- UCS-E180D-M3 および UCS-E1120D-M3 の BIOS UCSEDM3_2.5 以降

ステップ 1 CIMC にログインします。

（注） USC-E シリーズ サーバーの推奨 CIMC バージョンは、3.2(7) 以降です。

ステップ 2 KVM コンソールを起動するには、CIMC ホームページから **[KVMの起動（Launch KVM）]** を選択します。

Java または HTML ベースの KVM を選択できます。HTML ベースの KVM の使用をお勧めします。KVM コンソールは別のウィンドウで開くため、ポップアップブロッカーが無効になっていることを確認します。

ステップ 3 KVM コンソールから仮想メディアをマッピングするには、次の手順を実行します。

a) ダウンロードしたファイルを安全にインストールできるかどうかを確認するには、ファイルのチェックサムを比較してから使用する必要があります。チェックサムを確認することで、ネットワーク送信中にファイルが破損したり、ダウンロード前にファイルが悪意のある第三者によって変更されたりしていないことを確認できます。詳細については、「仮想マシンのセキュリティ」を参照してください。

b) **[仮想メディア（Virtual Media）]** を選択し、**[仮想デバイスのアクティブ化（Activate Virtual Devices）]** を選択します。

c) **[仮想メディア（Virtual Media）]** を再度選択し、**[CD/DVDのマッピング（Map CD/DVD）]** を選択します。画面を参照し、Cisco Enterprise NFVIS ISO イメージを選択します。**[ドライブを開いてマッピングする（Open and Map Drive）]** をクリックしてイメージをマウントします。

d) **[仮想メディア（Virtual Media）]** を再度選択し、NFVIS ISO イメージが CD/DVD にマッピングされたことを確認します。

ステップ 4 起動順序を設定します。

a) **[CIMCコンピューティング（CIMC Compute）]** から、**[BIOS]** を選択します。

b) **[起動順序の設定（Configure Boot Order）]** を選択すると、**[起動順序の設定（Configure Boot Order）]** ダイアログボックスが表示されます。

c) **[CD/DVD]** ページで、**[Cisco vKVMにマッピングされたvDVD（Cisco vKVM-Mapped vDVD）]** を選択し、**[追加（Add）]** を選択します。

d) **[HDD]** から **[RAIDアダプタ（RAID Adapter）]** を選択し、**[追加（Add）]** を選択します。

e) [Up] および [Down] オプションを使用して、起動の順序を設定します。**Cisco vKVM にマッピングされた vDVD** の起動順序を最初に選択する必要があります。**[変更を保存（Save Changes）]** をクリックして、起動順序の設定を完了します。

（注） CIMC を介して UEFI の起動順序を設定する場合、サポートされる BIOS バージョンは 2.10 以降です。他の BIOS バージョンを使用する場合は、BIOS セットアップメニューで UEFI 起動順序を設定し、**[BootOrderRules]** を **[Loose]** に設定する必要があります。

UEFI の起動順序を設定するには、次の手順を実行します。

a) **[CIMCコンピューティング（CIMC Compute）]** から、**[BIOS]** を選択します。

b) **[起動順序の設定（Configure Boot Order）]** を選択すると、**[起動順序の設定（Configure Boot Order）]** ダイアログボックスが表示されます。

c) **>>**、**<<**、**[上（up）]**、および **[下（down）]** ボタンを使用して、**UEFI イメージマップ**をユーザーインターフェイスの右側の列の最初のオプションにします。

d) **>>**、**<<**、**[上（up）]**、および **[下（down）]** ボタンを再度使用して、**UEFI OS** をユーザーインターフェイスの右側の列の 2 番目のオプションにします。

e) [変更の保存（Save Changes）] をクリックします。

ステップ 5 サーバーの電源を再投入して、インストールを開始します。

CIMC ホームページから、**[ホスト電源（Host Power）]** を選択します。**[電源オフ（Power Off）]** オプションを選択して、サーバーを再起動します。サーバーの電源が切れたら、**[電源オン（Power On）]** オプションを選択します。

サーバーが再起動すると、KVM コンソールによって、仮想 CD/DVD ドライブから Cisco Enterprise NFVIS が自動的にインストールされます。インストールが完了するまで 30 分～ 1 時間ほどかかることがあります。

ステップ 6 ENCS 5000 シリーズ プラットフォームでは、ファームウェアが自動アップグレードされます。

NFVIS 3.8.x リリース以降、ファームウェアの自動アップグレードがサポートされています。NFVIS のインストールが完了すると、BIOS または CIMC は対応するバージョンに自動的にアップグレードされます。CIMC と NFVIS は複数回再起動されます。ファームウェアのアップグレードが完了するまで 30 分～ 1 時間ほどかかることがあります。ファームウェアのアップグレード中は、システムを使用しないでください。

ステップ 7 インストールが完了すると、システムはハードドライブから自動的に再起動されます。再起動後にコマンドプロンプト **nfvis login** が表示されたら、システムにログインします。

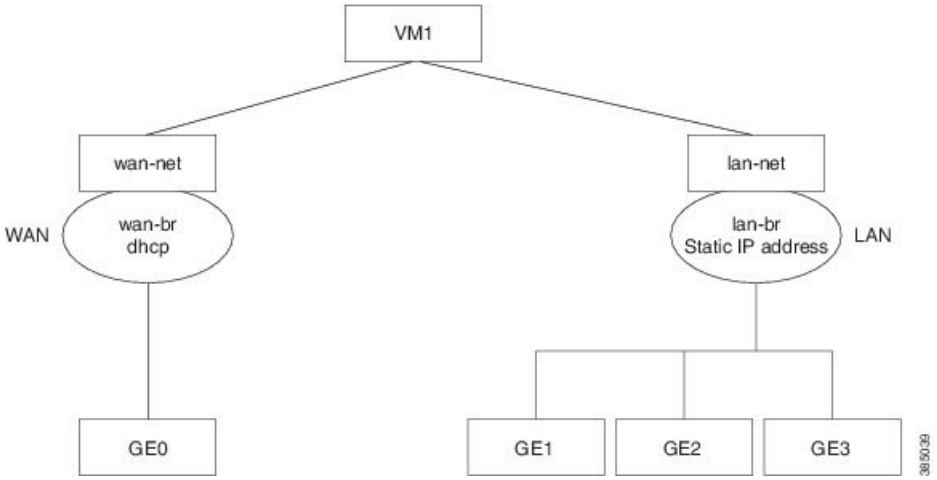
ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123＃** を使用します。

（注） 初めてログイン試行すると、デフォルトのパスワードを変更するように求められます。アプリケーションを続行するには、画面の指示に従って強力なパスワードを設定する必要があります。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。デフォルトのパスワードがリセットされていない場合、API は 401 未承認エラーを返します。

ステップ 8 システム API または CLI を使用するか、Cisco Enterprise NFV ポータルからシステム情報を表示して、インストールを確認します。

Cisco UCS E シリーズ サーバーのデフォルトのシステム設定

図 *9 : Cisco UCS E* シリーズ サーバーのデフォルトのネットワーク設定



次のネットワークとブリッジはデフォルトで作成され、削除できません。必要に応じてさらに設定できます。

- LAN ネットワーク（lan-net）と LAN ブリッジ（lan-br）：NFVIS ホストのデフォルトの静的管理 IP アドレス（192.168.1.1）は、LAN ブリッジで設定されます。インバウンドおよびアウトバウンドのトラフィック用のその他のすべてのポートは、LAN ブリッジに関連付けられます。デフォルトでは、ホスト名は「nfvis」に設定されます。

- WAN ネットワーク（wan-net）および WAN ブリッジ（wan-br）：物理 WAN ポートは Cisco ISR モジュール上にあります。これらは、Cisco UCS E サーバーで外部から使用することはできません。WAN トラフィックは ISR WAN ポートから送られ、バックプレーンを経由して Cisco UCS-E サーバーに到達します。バックプレーンには、Cisco UCS-E サーバーとの接続を確立するための内部 WAN インターフェイス（GE0）が 1 つあります。デフォルトでは、「GE0」インターフェイスが DHCP 接続に対して有効になっています。

初期セットアップの詳細については、『Cisco UCS E シリーズ サーバーおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップガイド』を参照してください。

USB を介した NFVIS のインストール

Cisco ENCS 5104 および Cisco Catalyst 8200 UCPE への Cisco Enterprise NFVIS のインストール

始める前に

Cisco Catalyst 8200 UCPE のインストールでは、NFVIS を 1 台のドライブにのみインストールし、インストール時にはそのドライブのみが存在するようにしてください。

Cisco Catalyst 8200 UCPE については、NFVIS にログインした後に BIOS パスワードを設定することをお勧めします。

BIOS パスワードを設定するには、**hostaction change-bios-password** コマンドを使用します。この手順を行わないと、NFVIS をインストールするデバイスを選択できません。

ステップ 1 NFVIS イメージを使用してブート可能な USB を作成します。

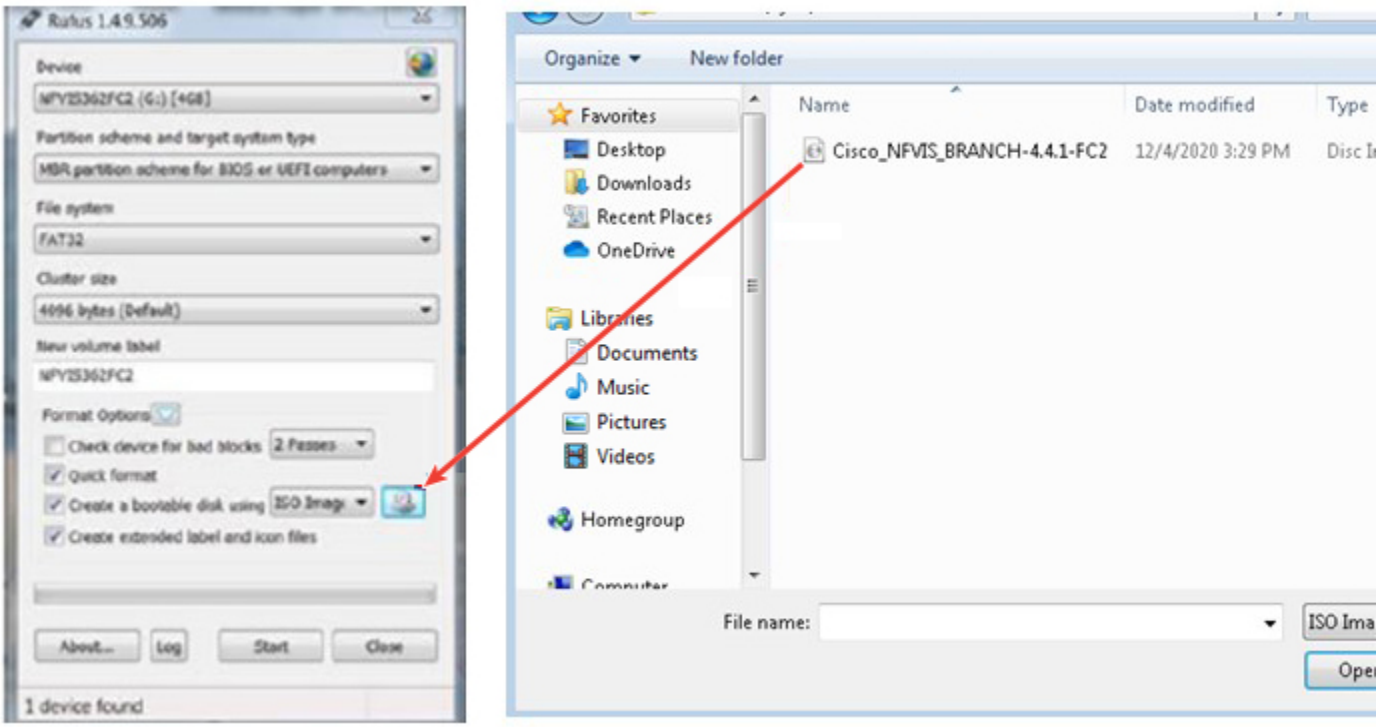
この例では、Windows 環境で Rufus ユーティリティを使用しました。Rufus ユーティリティは https://rufus.akeo.ie/ でダウンロードできます。この例では、次のパラメータを使用してブート可能な NFVIS USB デバイスを書き込みました。

- デバイス：USB スティック
- パーティションスキーム：MBR
- ファイルシステム：FAT32
- クラスタサイズ：デフォルトを使用
- ボリュームラベル：デフォルトを使用
- クイックフォーマット：オン
- ブート可能の作成：[ISOイメージ（ISO Image）] を選択し、隣のアイコンをクリックして、NFVIS イメージを選択します。

- 拡張ラベルの作成：オン

[開始（Start）] を押して、完了するまで待ちます。

USB サムドライブのイジェクト



ステップ 2 ENCS5104 の USB スロットのいずれかに USB デバイスを挿入します。

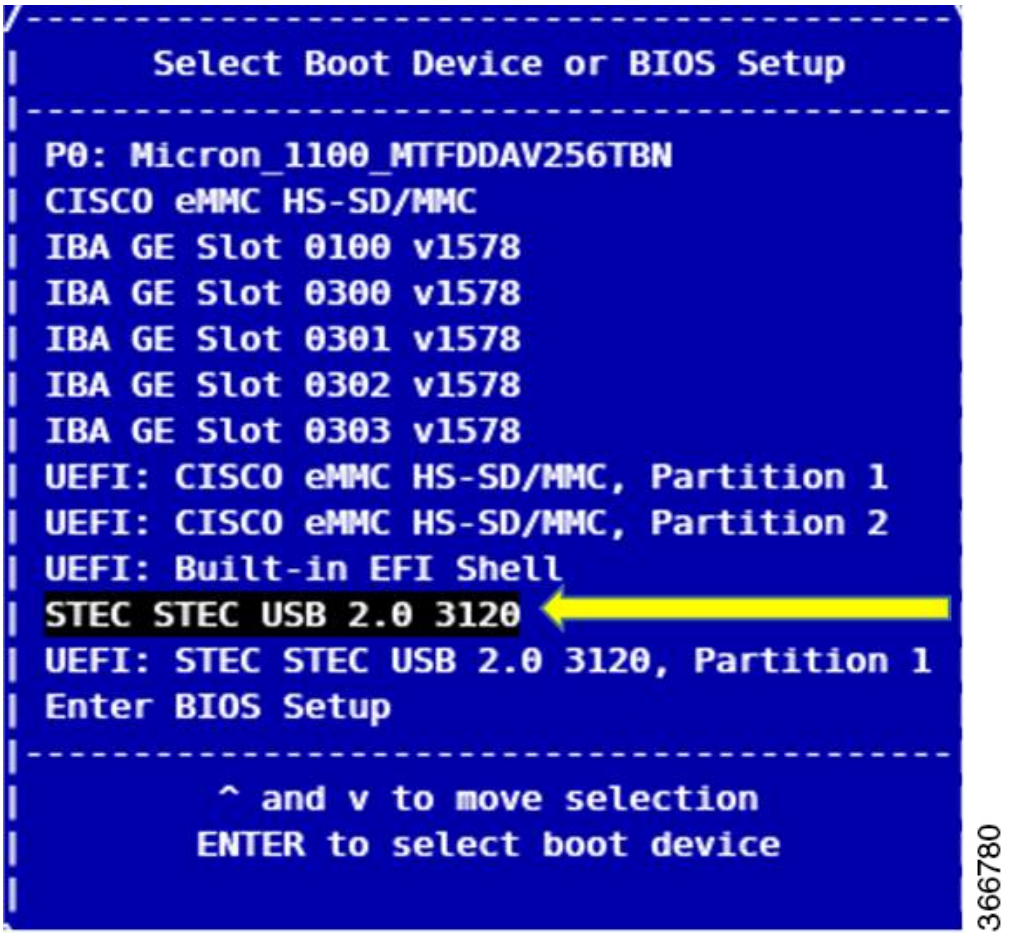
ステップ 3 システムの電源を入れます。

ステップ 4 システムの起動中に、F6 キーを押します。

```
Press <DEL> or <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot in 5 seconds or press any
key to continue.
```

ステップ 5 F6 を押すと次のスクリーンショットが表示され、起動元のデバイスを選択できます。USB デバイスを選択します。

次のスクリーンショットの例では、使用されている STEC USB があります。この表示は、USB デバイスのベンダーによって異なります。矢印キーを使ってデバイスを選択します。



ステップ 6 インストールが完了するまで待ちます。インストールが完了すると、システムが再起動されます。

ステップ 7 ユーザー名 **admin**、デフォルトパスワード **Admin123#** を使用してシステムにログインします。

ステップ 8 最初のログイン時にパスワードの変更を求めるプロンプトが表示されます。続行するには、画面の指示に従って強力なパスワードを設定する必要があります。

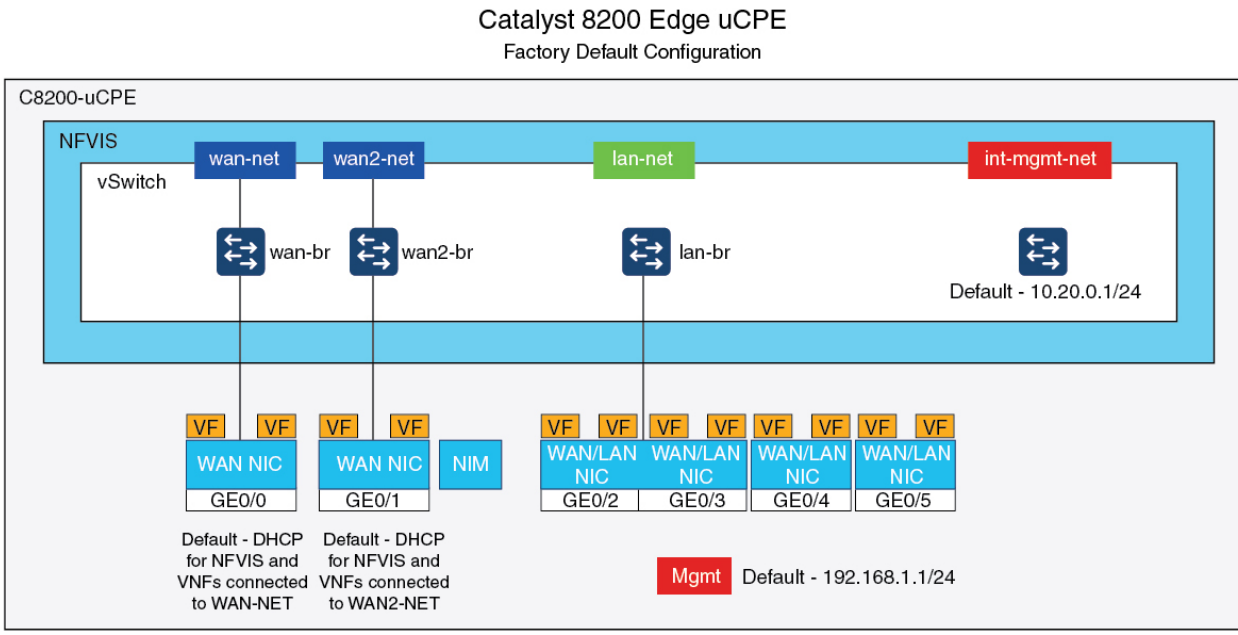
ステップ 9 NFVIS ユーザーガイドに従って、システム API またはコマンド ライン インターフェイスを使用してインストールステータスを確認できます。

次のタスク

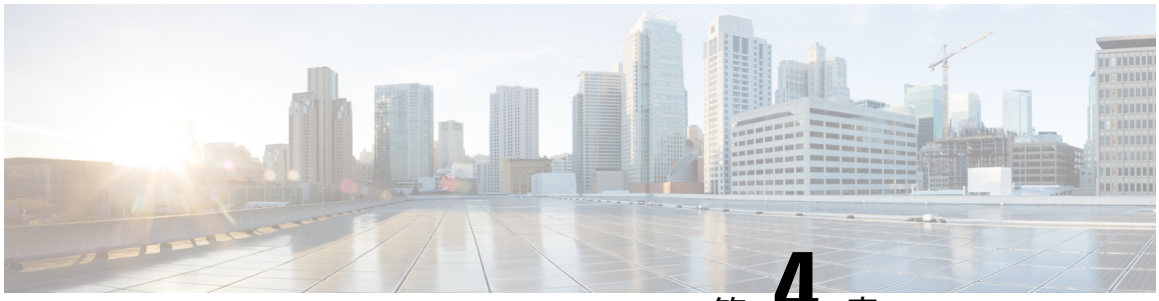
デフォルト設定を確認し、Cisco Enterprise NFV ポータルを起動するための初期 IP 設定をセットアップできます。

Cisco Catalyst 8200 UCPE のデフォルトのシステム設定

次の図は、Cisco ENCS を搭載した Cisco Enterprise NFVIS のデフォルトのネットワーク設定を示しています。



- デフォルトでは、NFVIS には WAN ポートまたは管理用の GE0/2 LAN ポートを介してアクセスできます。
- WAN ネットワーク（wannet および wan2net）と WAN ブリッジ（wanbr および wan2br）は、デフォルトでは DHCP を有効にするように設定されています。GE0 は、デフォルトでは WAN ブリッジと WAN2 ブリッジに関連付けられています。
- Cisco Catalyst 8200 UCPE の管理 IP アドレス 192.168.1.1 は、GE0/2 を介してアクセスできます。
- GE0/2 は LAN ブリッジに関連付けられています。
- 内部管理ネットワーク（int-mgmt-net）とブリッジ（int-mgmt-br）が作成され、内部でシステムモニタリングに使用されます。



第 4 章

Cisco NFVIS のアップグレード

Cisco NFVIS 対応ハードウェアには、Cisco NFVIS バージョンがプリインストールされています。次の手順に従って、リリースの最新バージョンにアップグレードしてください。

Cisco Enterprise NFVIS アップグレードイメージは、`.iso` および `.nfvispkg` ファイルとして使用できます。現在、ダウングレードはサポートされていません。Cisco Enterprise NFVIS アップグレードイメージのすべての RPM パッケージは、暗号の完全性と真正性を保証するために署名されます。さらに、Cisco Enterprise NFVIS のアップグレード中にすべての RPM パッケージが検証されます。

アップグレードプロセスを開始する前に、イメージを Cisco NFVIS サーバーにコピーしてください。イメージを登録するときは、常にイメージの正確なパスを指定します。**scp** コマンドを使用して、リモートサーバーから Cisco Enterprise NFVIS サーバーにアップグレードイメージをコピーします。**scp** コマンドを使用する場合は、イメージを Cisco Enterprise NFVIS サーバーの「`/data/intdatastore/uploads`」フォルダにコピーする必要があります。

（注）

- Cisco NFVIS リリース 4.2.1 以前のリリースでは、.nfvispkg ファイルを使用して、あるリリースからその次のリリースに Cisco NFVIS をアップグレードできます。たとえば、NFVIS を Cisco NFVIS リリース 3.5.2 から Cisco NFVIS リリース 3.6.1 にアップグレードできます。
- Cisco NFVIS リリース 4.4.1 以降では、.iso ファイルを使用して NFVIS をアップグレードできます。
- ダウンロードしたファイルを安全にインストールできるかどうかを確認するには、ファイルのチェックサムを比較してから使用する必要があります。チェックサムを確認することで、ネットワーク送信中にファイルが破損したり、ダウンロード前にファイルが悪意のある第三者によって変更されたりしていないことを確認できます。詳細については、「仮想マシンのセキュリティ」を参照してください。

Cisco NFVIS のアップグレードに関するアップグレードマトリックス

（注）
- 次の表を使用して、Cisco NFVIS ソフトウェアの現在のバージョンから、サポートされている最新のアップグレードバージョンのみにアップグレードします。サポートされていないバージョンにアップグレードすると、システムがクラッシュする可能性があります。
- サポートされているアップグレード イメージ タイプに .iso と .nfvispkg の両方がある場合は、.iso ファイルを使用してアップグレードすることをお勧めします。

表 *1 : Cisco NFVIS* リリース *4.6.1* 以降から *Cisco NFVIS* をアップグレードするためのアップグレードマトリックス

実行されているバージョン	サポート対象アップグレード バージョン	サポートされて
4.12.1	4.13.1	iso
4.11.1	4.12.1	iso
4.10.1	4.11.1	iso
4.9.4	4.11.1	
	4.10.1	
4.9.3	4.11.1	iso
	4.10.1	
	4.9.4	
4.9.2	4.11.1	iso
	4.10.1	
	4.9.4	
	4.9.3	

4.9.1	4.11.1	iso
	4.10.1	
	4.9.4	
	4.9.3	
	4.9.2	
4.8.1	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
4.7.1	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
	4.8.1	iso、nfvispk
4.6.3	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
	4.8.1	
	4.7.1	nfvispkg
46-2	4.9.1 または 4.9.2 または 4.9.3 または 4.9.4	iso
	4.8.1	
	4.7.1	
	4.6.3	
4.6.1	4.9.1 または 4.9.2 または 4.9.3 または 4.9.4	iso
	4.8.1	
	4.7.1	iso、nfvispk
	4.6.3	iso
	46-2	

表 *2 : Cisco NFVIS* リリース *4.5.1* 以前から *Cisco NFVIS* をアップグレードするためのアップグレードマトリックス

実行されているバージョン	サポート対象アップグレードバージョン	サポートされているアップグレード イメージ タイプ

4.5.1	4.7.1	iso
	4.6.3	iso、nfvispkg
	46-2	iso、nfvispkg
	4.6.1	iso、nfvispkg
4.4.2	4.6.3	iso
	46-2	iso
	4.6.1	iso
	4.5.1	iso、nfvispkg
4.4.1	4.6.3	iso
	46-2	iso
	4.6.1	iso
	4.5.1	iso、nfvispkg
	4.4.2	iso、nfvispkg
4.2.1	4.4.2	nfvispkg
	4.4.1	nfvispkg
4.1.2	4.2.1	nfvispkg
4.1.1	4.2.1	nfvispkg
	4.1.2	nfvispkg
3.12.3	4.1.1	nfvispkg
3.11.3	3.12.3	nfvispkg
3.10.3	3.11.3	nfvispkg
3.9.2	3.10.3	nfvispkg
3.8.1	3.9.2	nfvispkg

Cisco NFVIS ISO ファイルのアップグレードに関する制限事項

- Cisco NFVIS は、Cisco NFVIS リリース 4.6.x 以降（Cisco NFVIS リリース 4.7.x および 4.8.x は除く）、バージョン N からバージョン N+1、N+2、および N+3 への .iso アップグレードのみをサポートしています。NFVIS は、バージョン N からバージョン N+4 以降への .iso アップグレードをサポートしていません。
- .iso ファイルを使用したイメージのダウングレードはサポートされていません。

（注） バージョン N から N+1 または N+2 へのアップグレード中にエラーが発生した場合、Cisco NFVIS はイメージバージョン N にロールバックします。

ISO ファイルを使用した Cisco NFVIS 4.8.1 以降のアップグレード

次の例では、**scp** コマンドを使用してアップグレードイメージをコピーする方法を示します。

- アップグレードイメージをコピーするには、Cisco NFVIS CLI から **scp** コマンドを使用します。

```
nfvis# scp
admin@192.0.2.9:/NFS/2022-01-23/13/nfvis/iso/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
 intdatastore:Cisco_NFVIS-4.8.0-13-20220123_020232.iso
```

- アップグレードイメージをコピーするには、リモート Linux から **scp** コマンドを使用します。

```
config terminal
system settings ip-receive-acl 0.0.0.0/0
service scpd action accept
commit

scp -P22222 Cisco_NFVIS-4.8.0-13-20220123_020232.iso
admin@172.27.250.128:/data/intdatastore/uploads/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
```

または、Cisco Enterprise NFVIS ポータルの **[システムアップグレード（System Upgrade）]** オプションを使用して、Cisco Enterprise NFVIS サーバーにイメージをアップロードすることもできます。

（注） NFVIS のアップグレードが進行中の場合は、システムの電源がオフになっていないことを確認します。NFVIS のアップグレードプロセス中にシステムの電源がオフになると、システムが動作不能になり、システムの再インストールが必要になる場合があります。

アップグレードプロセスは、次の 2 つのタスクで構成されます。

1. **system upgrade image-name** コマンドを使用したイメージの登録。
2. **system upgrade apply-image** コマンドを使用したイメージのアップグレード。

イメージの登録

イメージを登録するには、次のコマンドを使用します。

```
config terminal
system upgrade image-name Cisco_NFVIS-4.8.0-13-20220123_020232.iso location
/data/intdatastore/uploads/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
commit
```

（注） **system upgrade apply-image** コマンドを使用してイメージをアップグレードする前に、イメージの登録ステータスを確認する必要があります。パッケージのステータスは、登録したイメージに対して有効である必要があります。

イメージ登録ステータスを確認するには、次のコマンドを使用します。

```
nfvis# show system upgrade

                    PACKAGE
NAME                                        LOCATION
                    VERSION   STATUS  UPLOAD DATE
-------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00


nfvis# show system upgrade reg-info

                    PACKAGE
NAME                                        LOCATION
                    VERSION   STATUS  UPLOAD DATE
-------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00
```

登録したイメージのアップグレード

登録したイメージをアップグレードするには、次のコマンドを使用します。

```
config terminal
system upgrade apply-image Cisco_NFVIS-4.8.0-13-20220123_020232.iso scheduled-time 5
commit
```

アップグレードステータスを確認するには、特権 EXEC モードで **show system upgrade apply-image** コマンドを使用します

```
nfvis# show system upgrade
                                                  UPGRADE  UPGRADE
NAME                                        STATUS     FROM     TO
-------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso  SCHEDULED  -        -
```

```
                    PACKAGE
NAME                                                LOCATION
                    VERSION    STATUS   UPLOAD DATE
-------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00
```

API およびコマンドのアップグレード

次の表に、API とコマンドのアップグレードをリストアップします。

アップグレード API	アップグレード コマンド
• /api/config/system/upgrade • /api/config/system/upgrade/image-name • /api/config/system/upgrade/reg-info • /api/config/system/upgrade/apply-image	• system upgrade image-name • system upgrade apply-image • show system upgrade reg-info • show system upgrade apply-image

.nvfispkg ファイルを使用した Cisco NFVIS 4.7.1 以前のアップグレード

次の例では、**scp** コマンドを使用してアップグレードイメージをコピーする方法を示します。

NFVIS CLI からの **scp** コマンド：

```
nfvis# scp admin@192.0.2.9:/NFS/Cisco_NFVIS_BRANCH_Upgrade-351.nfvispkg
intdatastore:Cisco_NFVIS_BRANCH_Upgrade-351.nfvispkg
```

リモート Linux からの **scp** コマンド：

```
config terminal
system settings ip-receive-acl 0.0.0.0/0
service scpd action accept
commit

scp -P 22222 nfvis-351.nfvispkg
admin@192.0.2.9:/data/intdatastore/uploads/nfvis-351.nfvispkg
```

または、Cisco Enterprise NFVIS ポータルの **[システムアップグレード（System Upgrade）]** オプションを使用して、Cisco Enterprise NFVIS サーバーにイメージをアップロードすることもできます。

（注） NFVIS のアップグレードが進行中の場合は、システムの電源がオフになっていないことを確認します。NFVIS のアップグレードプロセス中にシステムの電源がオフになると、システムが動作不能になり、システムの再インストールが必要になる場合があります。

アップグレードプロセスは、次の 2 つのタスクで構成されます。

- **system upgrade image-name** コマンドを使用したイメージの登録。
- **system upgrade apply-image** コマンドを使用したイメージのアップグレード。

イメージの登録

イメージを登録するには、次の手順を実行します。

```
config terminal
system upgrade image-name nfvis-351.nfvispkg location
/data/intdatastore/uploads/<filename.nfvispkg>
commit
```

（注） **system upgrade apply-image** コマンドを使用してイメージをアップグレードする前に、イメージの登録ステータスを確認する必要があります。パッケージのステータスは、登録したイメージに対して有効である必要があります。

イメージの登録の確認

イメージの登録を確認するには、特権 EXEC モードで **show system upgrade reg-info** コマンドを使用します。

```
nfvis# show system upgrade reg-info
PACKAGE
NAME             LOCATION                                    VERSION        STATUS UPLOAD
DATE
--------------------------------------------------------------------------------------------------
nfvis-351.nfvispkg /data/upgrade/register/nfvis-351.nfvispkg 3.6.1-722 Valid
2017-04-25T10:29:58.052347-00:00
```

登録したイメージのアップグレード

登録したイメージをアップグレードするには、次の手順を実行します。

```
config terminal
system upgrade apply-image nfvis-351.nfvispkg scheduled-time 5
commit
```

アップグレードステータスの確認

特権 EXEC モードで **show system upgrade apply-image** コマンドを使用します

```
nfvis# show system upgrade apply-image
UPGRADE
NAME    STATUS      FROM      UPGRADE TO
-----------------------------------------------------------------------------------------------
nfvis-351.nfvispkg SUCCESS 3.5.0 3.5.1
```

ENCS 5400 プラットフォームで BIOS セキュアブート（UEFI モード）が有効になっている場合にサポートされる唯一のアップグレードは次のとおりです。

NFVIS 3.8.1 + BIOS 2.5（レガシー）--> NFVIS 3.9.1 + BIOS 2.6（レガシー）

次のアップグレードでは、UEFI モードで NFVIS を再インストールする必要があります。

NFVIS 3.8.1 + BIOS 2.5（レガシー）--> NFVIS 3.9.1 + BIOS 2.6（UEFI）

NFVIS 3.9.1 + BIOS 2.6（レガシー）--> NFVIS 3.9.1 + BIOS 2.6（UEFI）

アップグレード API とアップグレードコマンド

次の表に、アップグレード API とアップグレードコマンドをリストアップします。

アップグレード API	アップグレード コマンド
• /api/config/system/upgrade • /api/config/system/upgrade/image-name • /api/config/system/upgrade/reg-info • /api/config/system/upgrade/apply-image	• system upgrade image-name • system upgrade apply-image • show system upgrade reg-info • show system upgrade apply-image

Firmware アップグレード

（注） ファームウェアのアップグレードは、ENCS 5400 シリーズのデバイスでのみサポートされます。

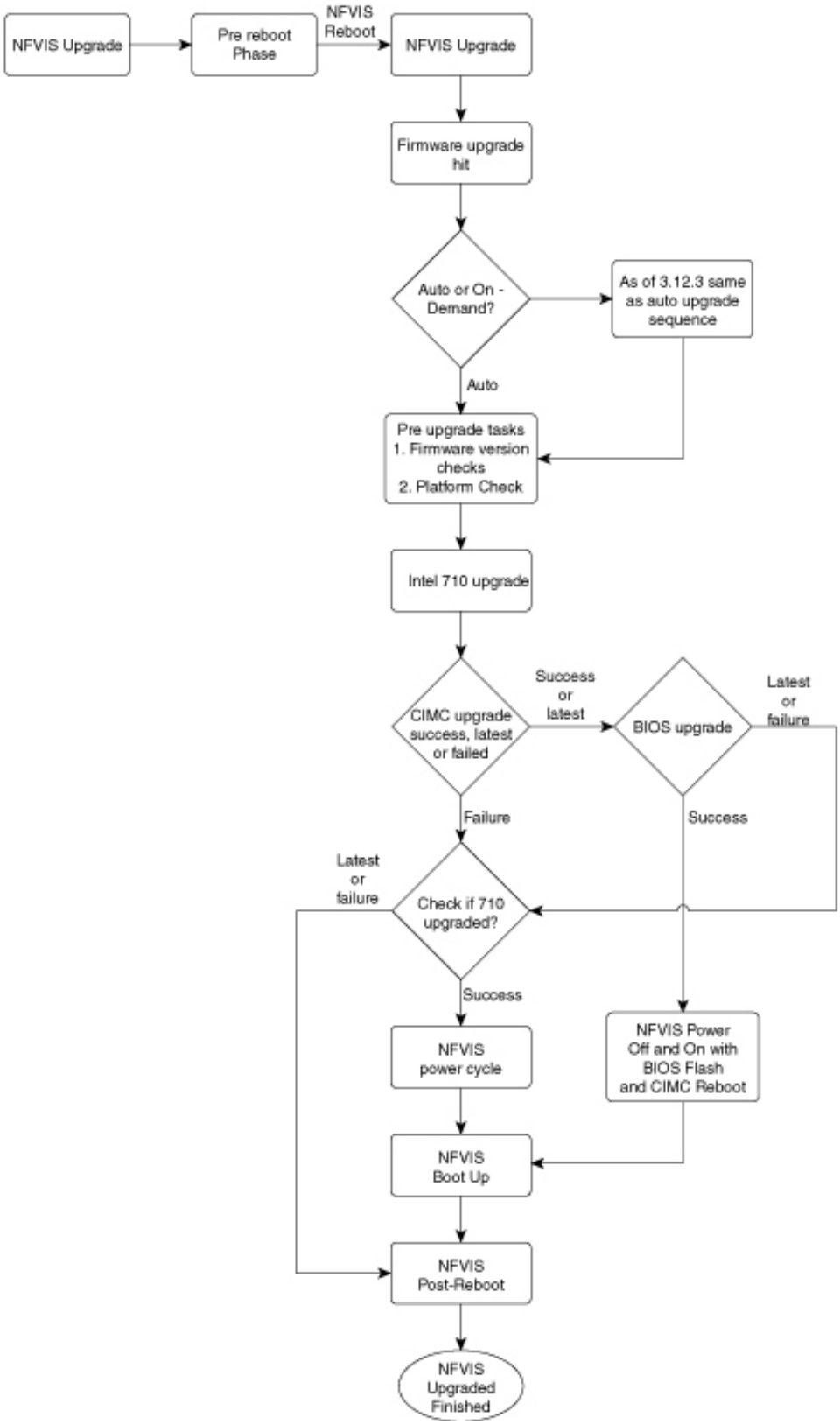
この機能は、NFVIS 自動アップグレードの一部として NFVIS 3.8.1 リリースで導入され、ENCS 5400 シリーズデバイスの選択されたファームウェアのアップグレードをサポートしています。ファームウェアのアップグレードは、再起動後のフェーズの一部として NFVIS のアップグレード中にトリガーされます。ファームウェアのアップグレードをトリガーするには、NFVIS アップグレード機能を参照してください。

NFVIS 3.9.1 リリース以降、オンデマンドアップグレードがサポートされており、NFVIS CLI を通じて登録および適用される個別のファームウェアパッケージ（.fwpkg 拡張）が提供されま

す。NFVIS の新規インストールによって最新のファームウェアにアップグレードすることもできます。

次のファームウェアをアップグレードできます。

- Cisco Integrated Management Controller（CIMC）
- BIOS
- Intel 710
- FPGA


NFVIS Upgrade
Pre reboot Phase
NFVIS Reboot
NFVIS Upgrade
Firmware upgrade hit
Auto or On - Demand?
As of 3.12.3 same as auto upgrade sequence
Auto
Pre upgrade tasks
1. Firmware version checks
2. Platform Check
Intel 710 upgrade
CIMC upgrade success, latest or failed
Success or latest
BIOS upgrade
Latest or failure
Failure
Success
Latest or failure
Check if 710 upgraded?
Success
NFVIS power cycle
NFVIS Power Off and On with BIOS Flash and CIMC Reboot
NFVIS Boot Up
NFVIS Post-Reboot
NFVIS Upgraded Finished

NFVIS 3.12.3 リリース以降、ファームウェア アップグレード スクリプトは実行ファイル形式からモジュール形式に変更されています。コードはモジュール化されており、各ファームウェアを個別にアップグレードできます。シェルコマンドは、os.system() コールではなくサブプロセスで呼び出されます。各ファームウェアアップグレードコールは、時間制限付きでモニターされます。コールがスタックしている場合、プロセスは強制終了され、実行制御は適切なメッセージとともにコードフローに戻ります。

次の表に、ファームウェア アップグレードの流れを示します。

NFVIS のアップグレード	新規インストール	オンデマンドアップグレード
Intel 710		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710 5. NFVIS 電源の再投入 6. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710 5. NFVIS 電源の再投入 6. ログイン	1. ファームウェアのアップグレード 710 2. NFVIS 電源の再投入 3. ログイン
Intel 710 および BIOS		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710 および BIOS 5. BIOS による NFVIS 電源のオフ/オン 6. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710 および BIOS 5. BIOS による NFVIS 電源のオフ/オン 6. ログイン	1. ファームウェアのアップグレード 710 および BIOS 2. BIOS による NFVIS 電源のオフ/オン 3. ログイン
Intel 710 および CIMC		

NFVIS のアップグレード	新規インストール	オンデマンドアップグレード
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード710およびCIMC 5. CIMC の再起動 6. 710 による NFVIS 電源の再投入 7. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード710およびCIMC 5. CIMC の再起動 6. 710 による NFVIS 電源の再投入 7. ログイン	1. ファームウェアのアップグレード 710 および CIMC 2. CIMC の再起動 3. 710 による NFVIS 電源の再投入 4. ログイン
CIMC		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード CIMC 5. CIMC の再起動 6. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード CIMC 5. CIMC の再起動 6. ログイン	1. ファームウェアのアップグレード CIMC 2. CIMC の再起動 3. ログイン
CIMC および BIOS		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード CIMC および BIOS 5. NFVIS 電源オフ 6. CIMC の再起動 7. BIOS フラッシュ 8. NFVIS 電源オン 9. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード CIMC および BIOS 5. NFVIS 電源オフ 6. CIMC の再起動 7. BIOS フラッシュ 8. NFVIS 電源オン 9. ログイン	1. ファームウェアのアップグレード CIMC および BIOS 2. NFVIS 電源オフ 3. CIMC の再起動 4. BIOS フラッシュ 5. NFVIS 電源オン 6. ログイン

NFVIS のアップグレード	新規インストール	オンデマンドアップグレード
BIOS		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード BIOS 5. NFVIS 電源オフ 6. BIOS フラッシュ 7. NFVIS 電源オン 8. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード BIOS 5. NFVIS 電源オフ 6. BIOS フラッシュ 7. NFVIS 電源オン 8. ログイン	1. ファームウェアのアップグレード BIOS 2. NFVIS 電源オフ 3. BIOS フラッシュ 4. NFVIS 電源オン 5. ログイン
Intel 710、CIMC、および BIOS		
1. NFVIS のアップグレード 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710、CIMC および BIOS 5. NFVIS 電源オフ 6. CIMC の再起動 7. BIOS フラッシュ 8. NFVIS 電源オン 9. ログイン	1. インストール 2. Reboot 3. ログイン 4. ファームウェアのアップグレード 710、CIMC および BIOS 5. NFVIS 電源オフ 6. CIMC の再起動 7. BIOS フラッシュ 8. NFVIS 電源オン 9. ログイン	1. ファームウェアのアップグレード 710、CIMC および BIOS 2. NFVIS 電源オフ 3. CIMC の再起動 4. BIOS フラッシュ 5. NFVIS 電源オン 6. ログイン

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。