# Cisco EPN Manager 7.1 のインストール

この章では、Cisco EPN Manager 7.1 のインストールを計画し、インストールに必要なすべての前提条件を満たしていることを確認するために必要な情報を示します。また、高可用性を持たない標準的な環境に Cisco EPN Manager 7.1 をインストールする手順についても説明します。高可用性については、Cisco EPN Manager 7.1 高可用性インストールを参照してください。



# インストールの概要

Cisco EPN Manager 7.1 は、仮想マシンに新規インストールとしてインストールできます。以前のバージョンの Cisco EPN Manager をすでに使用している場合は、Cisco EPN Manager 7.1 にアップグレードしてデータを保持できます。

以降のトピックでは、Cisco EPN Manager 7.1 のインストールおよびアップグレードのオプションの概要と、その他の役に立つインストール関連の情報を提供します。

- インストール オプション
- アップグレード オプション
- インストール時に作成されるユーザー

（注） リリースまたはメンテナンス パックをインストールした後に、cisco.com のソフトウェア ダウンロード サイトでポイント パッチを確認し、そのリリースまたはメンテナンス パックに利用可能な最新のポイント パッチをインストールすることをお勧めします。ポイント パッチとインストールの手順に関する情報は、cisco.com のソフトウェア ダウンロード サイトのパッチ ファイルに付属している readme ファイルで確認できます。

# インストール オプション

Cisco EPN Manager 7.1 は、仮想マシン（VM）にインストールできます。

- OVA/VMWare VM のインストール：VM インストールの場合は、「OVA/VM の要件」に記載されている要件に準拠した専用サーバーにオープン仮想アプライアンス（OVA）ファイルをインストールします。サーバー ハードウェアごとに Cisco EPN Manager の VM インスタンスを 1 つだけ実行することをお勧めします。

（注） レガシー BIOS モードではなく UEFI（EFI）モードでインストールされているサーバーに Cisco EPN Manager 7.1 をインストールする場合は、以下の必須手順に従ってください。

1. CEPNM 管理 CLI で、シェルに切り替えます。**`$ shell`**
2. ルートに切り替えます。**`$ sudo -i`**
3. 公式の RH rpm を含む zip ファイルを解凍します。**`$ mkdir rpms; cd rpms`**
4. grub2_packages.zip ファイルを解凍します。
5. 次のコマンドを使用してファイルをインストールします。**`$ rpm -Uvh *.rpm –force`**

（注） シスコ以外のハードウェアに Cisco EPN Manager をインストールするには、VMware を使用して OVA ファイルをインストールします。VMware を使用すると、ハードウェアのコンプライアンス違反の問題が最小限に抑えられますが、VM のプロビジョニングを可能にするために必要なリソースがハードウェアに含まれていることを確認する必要があります。

OVA のインストールには、次が含まれています。

- Red Hat Enterprise Linux 8.8 オペレーティングシステム
- Oracle Database 19c Enterprise Edition リリース 19.13.0.0.0
- EPN Manager

（注） Cisco EPN Manager は、ユーザーがインストールする個別の Linux/Oracle パッチをサポートしていません。必要なパッチは、Cisco EPN Manager のリリースまたはポイント パッチに含まれています。

### ファームウェア アップグレード

Cisco EPN Manager は、ファームウェアまたは製品のアップグレードをサポートしていません。アップグレードに関するサポートが必要な場合は、シスコ アドバンスト サービスの担当者にお問い合わせください。

# アップグレード オプション

既存の展開に関連する有効なアップグレードパスに従うことで、Cisco EPN Manager 7.1 にアップグレードできます。有効なアップグレード パス を参照してください。

Cisco EPN Manager 7.1 へのアップグレードには、次の方法を使用できます。

- バックアップ/復元アップグレード：一般に、このアップグレード オプションには新しいハードウェアが必要です（ただし、既存のハードウェアを使用することも可能ですが）。新しいバージョンを新しいハードウェアにインストールする間は、現在のバージョンの Cisco EPN Manager が動作し続けるため、このタイプのアップグレードを実行する際のダウンタイムは短くなります。ただし、インストール後は、バックアップからデータを復元する必要があります。復元プロセスを開始すると、すべてのデータがコピーされるまで、一部のデータが新しいサーバーで使用できなくなる期間があります。詳細については、「バックアップ/復元アップグレード」を参照してください。

（注） Cisco EPN Manager は、アップグレード後の以前のバージョンへの自動ロールバックをサポートしていませんが、手動で以前のバージョンに戻すことができます。詳細については、「以前のバージョンの Cisco EPN Manager への復帰」を参照してください。

# インストール時に作成されるユーザー

インストール プロセス時に次のタイプのユーザーが作成されます。

- **Cisco EPN Manager CLI 管理者ユーザー**：アプリケーションの停止と再起動やリモート バックアップ リポジトリの作成などの高度な管理操作に使用されます。システムへのセキュアで限定的なアクセスを提供するシスコ独自のシェルである CEPNM 管理 CLI へのアクセス権を提供します（Linux シェルと比較した場合）。

  CLI 管理者ユーザーのパスワードはインストール時にユーザーによって定義されますが、次のコマンドを入力して後の段階で変更できます。

```
admin# change-password
```

- **Linux CLI 管理者ユーザー**：Linux レベルの管理のために使用されます。Linux コマンドすべてを提供する Linux シェルである Linux CLI へのアクセスを提供します。Linux シェルは、シスコ テクニカル サポート担当者のみが使用できます。標準のシステム管理者は、Linux シェルを使用しないでください。Linux シェルは、Cisco EPN Manager 管理シェルと CLI を介してのみ到達できます。Linux CLI 管理者ユーザーは、主に製品関連の運用上の問題をデバッグするために、Linux ルートレベルの特権を取得できます。ユーザーは初期インストール時に admin とは異なる名前を付けることができます。
- **Cisco EPN Manager Web GUI ルート ユーザー**：Web GUI への最初のログインと、他のユーザーアカウントの作成に必要です。ルートユーザーパスワードは、インストール時にユーザーが定義します。
- **ftp-user**：FTP を使用して外部サーバーにアクセスするデバイスへのイメージ配信やその他の操作のような内部操作に使用されます。パスワードはランダムに生成され、定期的に変更されます。管理者権限を持つユーザーは ftp のユーザー パスワードを変更できますが、このユーザー定義のパスワードは数か月後に期限切れになります。ftp のユーザー パスワードを変更するには、次のコマンドを使用します。

```
admin# ncs password ftpuser username password password
```

- **scpuser**：デバイスへのイメージ配布や、SCP を使用して外部サーバーにアクセスするその他の操作などの内部操作に使用されます。パスワードはランダムに生成され、定期的に変更されます。
- **prime**：すべてのアプリケーション プロセスが実行されるシステム生成アカウント。変更できません。
- **oracle**：Oracle プロセスで使用されるシステム生成アカウント。変更できません。

（注） 最初の 4 つのユーザーアカウントは、実際のネットワーク ユーザーに関連付けられています。Cisco EPN Manager は、**scpuser**、**prime**、および **oracle** ユーザー アカウントを使用して内部操作を実行し、どのような方法でも変更できません。

ユーザー タイプとユーザーの管理の詳細については、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』参照してください。

# システム要件

以降の項で、Cisco EPN Manager 7.0 をインストールする前に満たす必要がある要件を示します。

# ハードウェアおよびソフトウェアの要件

## OVA/VM の要件

次の表は、OVA/VM システムの要件の概要を示します。

- [拡張（Extended）]：実稼働環境での大規模なネットワーク設定に推奨されます。
- [プロフェッショナル（Professional）]：実稼働環境での非スケールネットワーク設定に推奨されます。

[非常に大規模（Very-Large）] プロファイルを使用することはお勧めしません。これは、Cisco TAC から要求された場合にのみ使用され、標準インストールでは使用されません。

（注） OVA/VM のインストールでは、外部ストレージがサポートされています。

| サーバー タイプ | 項目 | 拡張 | プロフェッショナル |
|---|---|---|---|
| 仮想マシン | VMware ESXi のバージョン<br>（注） OVA イメージを使用したインストールは、独自のハードウェア上の VMWare ESXi でサポートされます。どのような場合も、サーバーはこの表に記載されている要件を満たしているか、超えている必要があります。 | 6.7、7.0.1、8 | 6.7、7.0.1、8 |
| | アプライアンス イメージの形式 | OVA | OVA |

| サーバー タイプ | 項目 | 拡張 | プロフェッショナル |
|---|---|---|---|
| ハードウェア | 仮想 CPU（vCPU） | 24 | 16 |
| | メモリ（DRAM） | 128 GB | 64 GB |
| | ディスク容量<br>（注） 報告されたディスクサイズでは、RAID 構成が考慮されていません。 | 4 TB | 2.8 TB |
| | ディスク I/O 速度 | 最小：900 Mbps 以上 フルスケール：1150 Mbps 以上 | 最小：700 Mbps 以上 フルスケール：900 Mbps 以上 |

# Web クライアントの要件

次に、Cisco EPN Manager Web GUI のクライアントとブラウザの要件を示します。

- ハードウェア：以下のテスト済みサポート対象ブラウザのいずれかに対応している Mac または Windows のラップトップかデスクトップ。
- ブラウザ：

（注） 1 つのブラウザセッションで Cisco EPN Manager のタブを同時に 3 つまで開くことができます。

  - Google Chrome バージョン 70 以降
  - Mozilla Firefox ESR バージョン 78
  - Mozilla Firefox バージョン 70 以降

- 推奨される表示解像度：1600 X 900 ピクセル以上（最小：1366 X 768）

ロード時間を短縮し、ネットワーク帯域幅の使用量を削減するために、Cisco EPN Manager は同じバージョンの Cisco EPN Manager（Firefox ブラウザ）のブラウザに静的ファイル（js、css）をキャッシュします。

（注） Google Chrome では、自己署名証明書に関する既知の制限により、すべてのキャッシングディレクティブが無視され、ページコンテンツがリロードされます。

# Cisco EPN Manager で使用するポート

（注） インストール プロセスでは、サーバーの eth0 および eth1 イーサネット ポートを使用します。別のポートを使用すると、システムが正常に動作しない場合があります。

次の表に、Cisco EPN Manager がデバイスからの接続要求をリッスンするために使用するポートを示します。また、セキュリティ強化のため、この表にはポートを無効にしても製品に悪影響が及ばず安全かどうかも示します。

一般的なポリシーとして、不要なポートや非セキュアなポートをすべて削除する必要があります。まず、どのポートが有効になっているかを確認した後、Cisco EPN Manager の通常の機能を妨げることなく安全に無効化できるポートを判別する必要があります。これを行うには、開いているポートを一覧表示して、安全に無効化できるポートの一覧と比較します。Cisco EPN Managerの組み込みファイアウォールでは、一部のリスニング ポートは公開されません。展開で使用されるポートのリストを表示するには、Cisco EPN Manager CLI 管理者ユーザーとしてログインし、**show security-status** コマンドを実行します。

組み込みのファイアウォールに加えて、追加のネットワーク ファイアウォールを展開し、他の未使用のポートとそのトラフィックをブロックすることもできます。

**表 *1* : 組み込みのファイアウォールを介した開いているポートのリスニング**

| ポート | プロトコル | 使用方法 | 無効にしても安全か? | 注記 |
|---|---|---|---|---|
| 21 | TCP | FTP を使用してデバイスとの間でファイルを転送する。 | はい | Web GUI の [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] から [全般（General）] > [サーバー（Server）] を選択して FTP を無効にします。FTP を無効にした後に CLI 管理者ユーザーとしてサーバーを停止し、再起動します。 |

| ポート | プロトコル | 使用方法 | 無効にしても安全か? | 注記 |
|---|---|---|---|---|
| 22 | TCP | Cisco EPN Manager サーバーとの SSH 接続を開始し、SCP または SFTP を使用してファイルを Cisco EPN Manager サーバーにコピーする。 | 場合による | SCP、SFTP、HTTPS などの代替プロトコルがイメージ配布に使用され、管理対象デバイスでサポートされている場合にのみ。 |
| 69 | UDP | TFTP を使用してデバイスにイメージを配布する。 | 場合による | これは、TFTP のみをサポートし、SFTP または SCP をサポートしていない古い管理対象デバイスでも必要になる場合があります。 |
| 162 | UDP | ネットワーク デバイスから SNMP トラップを受信する。 | × | — |
| 443 | TCP | HTTPS 経由で Cisco EPN Manager サーバーにアクセスするブラウザの場合。 | × | — |
| 514 | UDP | ネットワーク デバイスから syslog メッセージを受信する。 | × | — |
| 1522 | TCP | アクティブとスタンバイの Cisco EPN Manager サーバー間の高可用性（HA）通信の場合。<br>Oracle データベース同期用の Oracle JDBC トラフィックを許可するために使用されます。 | はい | HA 用に少なくとも 1 つの Cisco EPN Manager サーバーが設定されていない場合、このポートは自動的に無効になります。 |
| 2021 | TCP | FTP を使用してデバイスにイメージを配布する。 | × | — |
| 8082 | TCP | HA ヘルス モニターの Web インターフェイスの場合（HTTP 経由）。<br>プライマリ サーバーとセカンダリ サーバーが HTTP を介してヘルス ステータスを監視するために使用します。 | いいえ（HA が設定されている場合） | — |

| ポート | プロトコル | 使用方法 | 無効にしても安全か? | 注記 |
|---|---|---|---|---|
| 8085 | TCP | ユーザーがハイアベイラビリティで準備テストを実行する場合、プライマリサーバーとセカンダリサーバー間のネットワーク帯域幅速度を確認するためにヘルスモニタープロセスで使用されます | いいえ（HA が設定されている場合） | — |
| 8087 | TCP | HA セカンダリ バックアップ サーバー上のソフトウェアを更新する（トランスポートとして HTTPS を使用）。 | × | — |
| 9991 | UDP | Netflow データ パケットを受信する。 | はい | Cisco EPN Manager はネットフローをサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。 |
| 9992 | TCP | HTTP または HTTPS を使用して M-Lync を管理する。 | はい | Cisco EPN Manager は M-Lync をサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。 |
| 11011 ～ 11014 | TCP | 独自の Cisco Networking Services（CNS）プロトコル トラフィックの PnP 操作の場合。 | はい | Cisco EPN Manager は PnP をサポートしていません。次のコマンドをこの順番で入力し（Cisco EPN Manager CLI 管理者ユーザーとして）、ネットワーク ファイアウォール内でこのトラフィックを無効にします。<br>**ncs pnp-gateway disable**<br>**ncs stop**<br>**ncs start** |

次の表に、ファイアウォールで保護される可能性のある外部デバイス上の宛先ポートを示します。これらのポートは、Cisco EPN Manager がネットワーク デバイスへの接続に使用します。

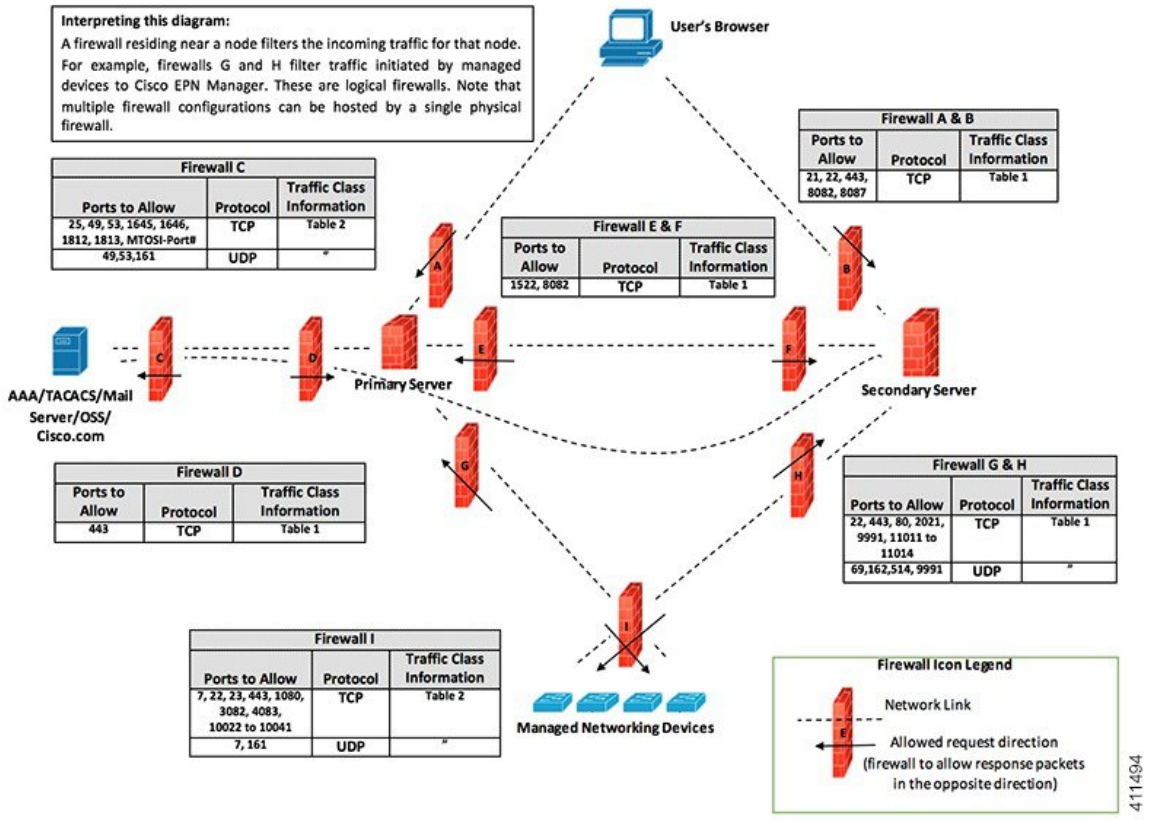
Cisco EPN Manager がこれらのデバイスに接続できるようにするには、必要なポートを開く必要があります。

表 *2 : Cisco EPN Manager* で使用する宛先ポート

| ポート | プロトコル | 使用する場合 |
|---|---|---|
| 7 | TCP/UDP | ICMP を使用したエンドポイントの検出。 |
| 22 | TCP | 管理対象デバイスとの SSH 接続の開始。 |
| 23 | TCP | Telnet を使用した管理対象デバイスとの通信。 |
| 25 | TCP | SMTP サーバーを使用した電子メールの送信。 |
| 49 | TCP/UDP | TACACS を使用した Cisco EPN Manager のユーザーの認証。 |
| 53 | TCP/UDP | DNS サービスへの接続。 |
| 161 | UDP | SNMP を使用したポーリング。 |
| 443 | TCP | HTTPS を使用した Cisco NCS 2000 デバイスのイメージのアップロードおよびダウンロードと設定バックアップ/復元の実行。 |
| 1522 | TCP | プライマリとセカンダリの HA サーバー間での通信（プライマリとセカンダリのサーバー間での Oracle データベースの同期に Oracle JDBC トラフィックを許可する）。 |
| 1080 | TCP | Socket Secure（SOCKS）プロトコルを使用した Cisco オプティカル ネットワーキング システム（ONS）および Cisco NCS 2000 シリーズのデバイスとの通信。 |
| 1645、1646、および 1812、1813 | UDP | RADIUS を使用した Cisco EPN Manager のユーザーの認証。 |
| 3082 | TCP | TL1 プロトコルを使用した Cisco ONS および Cisco NCS 2000 のデバイスとの通信。 |
| 4083 | TCP | セキュア TL1 プロトコルを使用した、Cisco ONS および Cisco NCS 2000 シリーズのデバイスとの通信。 |
| 8082 | TCP | HTTPS を使用したプライマリとセカンダリの HA サーバー間の通信による相互の正常性の監視。 |
| 10022 ～ 10041 | TCP | パッシブ FTP ファイル転送（デバイスの設定やレポートの取得など）。 |

| ポート | プロトコル | 使用する場合 |
|---|---|---|
| *RESTCONF TCP* ポート番号 | [TCP] | Cisco EPN Manager サーバーに接続された NBI クライアントでリッスンする（このポートが NBI クライアントシステムによって設定された後、ポート番号を含む登録通知メッセージが Cisco EPN Manager サーバーに送信される）。詳細については、RESTCONF API のガイドを参照してください。 |

次の図に、前の表に示したポート情報を示します。この図を使用して、ネットワークインフラストラクチャに対する適切なファイアウォール設定（適切な着信トラフィックの許可）を決定します。トラフィックのクラスを識別するには、「組み込みファイアウォールを介して開いているリスニングポート」という表の「使用方法」の列を参照してください。Cisco EPN Manager でサポートされていないサービスで使用されるポートを無効にすることをお勧めします。



# インストールの前提条件

## ライセンシング

Cisco EPN Manager には、初回インストールで自動的にアクティブ化される 90 日間の試用ライセンスが含まれています。試用期間を超えてアプリケーションを使用するには、次に示すように、実稼働環境と実稼働以外の環境の両方に必要な Cisco EPN Manager ライセンスを取得してインストールする必要があります。

実稼働環境の場合：

- 基本ライセンス（必須）
- スタンバイ ライセンス（オプション）：冗長性構成で構成された 2 台の Cisco EPN Manager サーバーを使用して高可用性展開を行う場合は、このライセンスを取得します。
- Cisco EPN Manager が管理するデバイスのタイプと対応する数の管理用ライセンス。

実稼働以外の環境（ラボ検証環境や開発環境など）については、Cisco EPN Manager のラボ インストールごとに Cisco EPN Manager ラボ ライセンスを取得してインストールしてください。ラボ ライセンスは、冗長性（HA）、無制限の管理範囲を含むすべての Cisco EPN Manager のオプションを対象としています。

Cisco EPN Manager ライセンスを購入するには、最寄りの営業担当者にお問い合わせください。

Cisco EPN Manager で使用できるライセンスのタイプの詳細については、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のライセンスの表示と管理に関する情報を参照してください。

## OVA/VM のインストールの前提条件

Cisco EPN Manager をインストールする前に、次を確認してください。

- 展開が「システム要件」に記載されている一般的なハードウェアとソフトウェアの要件、特に「OVA/VM の要件」を満たしている。
- 最適なパフォーマンスを確保するために、ハードウェア リソースが Cisco EPN Manager サーバー用に予約されている。CPU の最小クロックは、CPU あたり 2.2 Ghz です。
- Cisco EPN Manager サーバーとして使用する予定のマシン上に VMware ESXi がインストールされ、設定されている。VMware ホストのセットアップと設定については、VMware のマニュアルを参照してください。
- インストールされた VMware ESXi ホストが到達可能です。
- Cisco EPN Manager OVA は、vSphere Web インターフェイスが起動するのと同じマシンに保存される。

- ダウンロードした OVA パッケージが、「OVA パッケージの確認」の説明のとおりに検証されている。

# OVA パッケージの確認

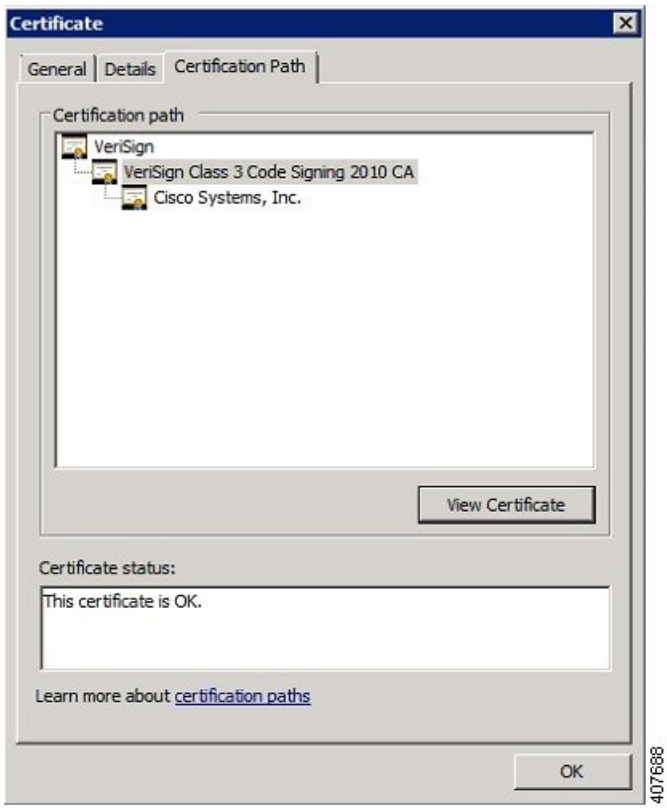
Cisco EPN Manager をインストールする前に、OVA パッケージを確認する必要があります。OVA パッケージ内にバンドルされている個々の UBF ファイルを確認する必要はありません。

VMware vSphere クライアントを使用してパブリッシャと証明書チェーンを確認します。

1. Cisco Systems が発行者であることを確認します。
   1. VMware vSphere クライアントで、[ファイル（File）] > [OVF テンプレートの展開（Deploy OVF Template）] を選択します。
   2. OVA インストール ファイル（*.ova）を参照して選択し、[次へ（Next）] をクリックします。
   3. [OVF テンプレートの詳細（OVF Template Details）] ウィンドウの [パブリッシャ（Publisher）] フィールドに、緑色のチェック マーク付きで [Cisco Systems, Inc.] が表示されていることを確認します。[パブリッシャ（Publisher）] フィールドに「**No certificate present**」と表示されている場合は、先に進まないでください。これは、イメージが署名されていないか、あるいはファイルが Cisco Systems 製ではない、またはファイルが改ざんされていることを示しています。Cisco の担当者にお問い合わせください。

      （注） [ベンダー（Vendor）] フィールドの情報を使用してイメージを検証しないでください。このフィールドは Cisco Systems を発行者として認証しません。

2. 証明書チェーンを確認します。
3. [OVF テンプレートの詳細（OVF Template Details）] ウィンドウの [パブリッシャ（Publisher）] フィールドで、[Cisco Systems, Inc.] ハイパーリンクをクリックします。
4. [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブをクリックします。
5. 次の図に示すように、[認証パス（Certification Path）] タブ（証明書チェーンのリストが表示されている）で、[認証パス（Certification Path）] 領域に [Cisco Systems, Inc.] が、[認証ステータス（Certification Status）] に [この証明書は正常です（The certificate is OK）] が表示されていることを確認します。




# Cisco EPN Manager 7.0 のインストール（非HA）

## OVA/VM を使用した Cisco EPN Manager のインストール

1. 展開が「システム要件」に記載されている要件を満たしていることを確認します。
2. 展開が「OVA/VM のインストールの前提条件」に記載されている前提条件を満たしていることを確認します。これには、OVA パッケージの確認が含まれます。
3. VMware vSphere クライアントからの OVA の展開。
4. 展開した OVA のシステム時刻を設定します。
5. Cisco EPN Manager 設定プロセスの開始。

### VMware vSphere クライアントからの OVA の展開

**ステップ 1** VMware vSphere クライアントを起動します。

**ステップ 2** [ファイル（File）] > [OVF テンプレートの導入（Deploy OVF Template）] の順に選択します。

**ステップ 3** [OVF テンプレートの展開（Deploy OVF Template）] ウィンドウで、[参照（Browse）] をクリックします。

**ステップ 4** OVA ファイルに移動して選択し、[次へ（Next）] をクリックします。

**ステップ 5** [エンド ユーザー ライセンス契約（End User License Agreement）] に同意し、[OVF テンプレートの詳細（OVF Template Details）] ウィンドウで製品名、バージョン、サイズなどの OVA ファイルの詳細を確認した後、[同意（Accept）] をクリックします。

**ステップ 6** [名前と場所（Name and Location）] ウィンドウで、次の手順を実行します。

1. 導入するテンプレートの名前と場所を指定します。名前はインベントリ フォルダ内で固有である必要があり、最大 80 文字で構成できます。
2. ネットワーク サイズに基づいて、設定タイプに[プロフェッショナル（Professional）]、[拡張（Extended）]、または [非常に大規模（Very-Large）] を選択します（「システム要件」を参照）。
3. [次へ（Next）] をクリックします。

**ステップ 7** OVA をインストールするクラスタまたはホストを選択し、[次へ（Next）] をクリックします。

**ステップ 8** 展開する OVA の宛先ストレージを選択し、[次へ（Next）] をクリックします。

**ステップ 9** ディスク形式として [シックプロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] を選択し、[次へ（Next）] をクリックします。

**ステップ 10** 設定された IP アドレスに基づいてネットワーク マッピングを選択し、[次へ（Next）] をクリックします。

**ステップ 11** [終了準備の完了（Ready to Complete）] ウィンドウで、次の手順を実行します。

1. 選択内容を確認します。
2. （オプション）OVA の展開が完了した後に仮想マシンを自動的に起動する場合は、[展開後に電源を投入する（Power on after deployment）] チェックボックスをオンにします。
3. [終了（Finish）] をクリックします。

このプロセスが完了するまでに数分かかる場合があります。[仮想アプリケーションの展開（Deploying Virtual Application）] ウィンドウの経過表示バーをチェックして、タスクのステータスをモニターします。展開タスクが正常に完了すると、確認ウィンドウが表示されます。

**ステップ 12** [閉じる（Close）] をクリックします。展開した仮想アプライアンスが、VMware vSphere クライアントの左側のペインのホストの下に表示されます。

## 展開した OVA のシステム時刻を設定します。

**ステップ 1** VMware vSphere クライアントで、左側のペインの VM を選択します。

**ステップ 2** [起動設定（Boot Settings）] オプションにアクセスします（[設定の編集（Edit Settings）] > [VM オプション（VM Options）] > [起動設定（Boot Settings）]）。

**ステップ 3** [強制 BIOS のセットアップ（Force BIOS Setup）] 領域のチェックボックスをオンにして、次回の VM 起動時に BIOS 設定画面が表示されるようにします。

**ステップ 4** [保存（Save）] をクリックします。

**ステップ 5** VM を起動します。

**ステップ 6** [BIOS 設定（BIOS setup）] 画面で、システムの時刻と日付を現在の UTC 時刻に設定します。

**ステップ 7** F10 を押して変更内容を保存し、画面を終了します。

# Cisco EPN Manager 設定プロセスの開始

**ステップ 1** VMware vSphere クライアントの [コンソール（Console）] タブをクリックし、ローカルホストのログインプロンプトで **setup** と入力します。

**ステップ 2** 表示されるプロンプトに対して、次のパラメータを入力します。

| パラメータ | 説明 |
|---|---|
| ホスト名（Hostname） | 仮想マシンのホスト名。 |
| IP アドレス（IP Address） | 仮想マシンの IP アドレス。 |
| IP デフォルト ネットマスク（IP default netmask） | 仮想マシンの IP アドレスのデフォルトのサブネット マスク。 |
| IP デフォルト ゲートウェイ（IP default gateway） | デフォルト ゲートウェイの IP アドレス。 |
| デフォルト DNS ドメイン（Default DNS domain） | デフォルト DNS ドメイン名 |
| プライマリ ネーム サーバー（Primary nameserver） | プライマリ DNS サーバーの IP アドレス。<br>セカンダリ ネームサーバーの追加を求めるメッセージがコンソールに表示されます。以下を入力します。<br>• セカンダリ ネームサーバーを入力する場合は **Y**。<br>• インストールの次のステップに進む場合は **N**。 |
| 別のネームサーバー（Another nameserver） | プライマリサーバーに到達できない場合に使用する別の DNS サーバーの IP アドレス。 |

| パラメータ | 説明 |
|---|---|
| プライマリ NTP サーバー（Primary NTP server） | 使用するプライマリ ネットワーク タイム プロトコル サーバーの IP アドレスまたはホスト名（デフォルトは **time.nist.gov**）。<br>セカンダリ NTP サーバーの追加を求めるメッセージがコンソールに表示されます。以下を入力します。<br>• NTP サーバーを入力する場合は **Y**。<br>• インストールの次のステップに進む場合は **N**。 |
| 別の NTP サーバー（Another NTP servers） | プライマリ NTP サーバーに到達できない場合に使用する別の NTP サーバーの IP アドレス。 |
| システム時間帯（System Time Zone） | 使用するタイム ゾーン。 |
| クロック タイム（Clock time） | クロック タイム（選択したシステム タイム ゾーンに基づく）。これはマシンに表示される時刻です。タイム ゾーンに基づいて時刻が正しいことを確認し、必要に応じて変更します。<br>コンソールからシステム クロック タイムの変更を求めるメッセージが表示されます。以下を入力します。<br>• クロック タイムを変更する場合は **Y**。<br>• インストールの次のステップに進む場合は **N**。 |
| ユーザー名（Username） | 最初の管理ユーザーの名前（デフォルトでは **admin**）。これは、SSH を使用して Cisco EPN Manager にログインする Cisco EPN Manager **CLI 管理ユーザー**です。 |
| パスワード（Password） | 最初の管理者ユーザーのパスワード。パスワードは 8 文字以上で、1 つ以上の数字と 1 つ以上の大文字を使用する必要があります。 |

（注） インストール時に、UI アクセスに使用する予定の IP サブネットを使用する必要があります。この IP は、管理 CLI で GigabitEthernet0 とも呼ばれる eth0 インターフェイス上で設定されます。

**ステップ 3** 新たにインストールされたサーバーを HA 実装環境でセカンダリ サーバーとして機能させるかどうかを選択するよう求めるメッセージが表示されます。

- HA を使用していて、このサーバーをセカンダリ サーバーにする場合は、**yes** と入力します。次のステップには進まず、高可用性展開での Cisco EPN Manager 7.1 のインストールに進みます。
- 次の場合は、**no** と入力します。
  - HA を使用していない。
  - HA を使用していても、このサーバーをプライマリ サーバーにする。

**ステップ 4** Cisco EPN Manager **Web GUI ルート ユーザー**のパスワードを入力します（2 回入力する必要があります）。このパスワードを使用して、初めて Web GUI にログインし、他のユーザー アカウントを作成します（同じレベルの権限を持つ新しいユーザー アカウントを作成した後、このアカウントを無効にする必要があります）。

**ステップ 5** 設定を表示して、次の手順を実行します。

- 設定が正しければ、[Y] を選択します。
- 設定が誤っている場合は、[N] を選択し、それらを編集してから適用します。

# 複数の NIC のインストール

次のトピックでは、複数の NIC をインストールする方法について説明します。



（注） 複数のネットワークアダプタベースのシステムの場合は、インストール時に 1 つのアダプタ（UI に使用されるアダプタ）のみが有効になっていることを確認します。EPNM をインストールしたらシステムの電源をオフにし、追加のネットワークアダプタを有効にして電源をオンにします。

また、メインインターフェイス（UI に使用されるインターフェイス）のみを有線（接続）のままにし、EPNM をインストールしたら、システムを再起動せずにアダプタの再接続を開始できます。

## 前提条件

HA 環境では、次の手順を実行します。

- 高可用性の削除
- 追加の NIC に必要な設定の追加
- プライマリ サーバーとセカンダリ サーバー間の高可用性の登録の実行

# プライマリサーバーとセカンダリサーバーでの追加の NIC の設定

管理 CLI に次のコマンドを入力します。

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# interface GigabitEthernet 1
storm-ha-194/admin(config-GigabitEthernet)# ip address 172.23.222.32 255.255.255.0
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
storm-ha-194/admin(config-GigabitEthernet)# end
```

（注） この設定は、両方のサーバー（プライマリとセカンダリ）に適用する必要があります。

# プライマリサーバーとセカンダリサーバーでのデバイスサブネットの静的ルートの追加

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# ip route 172.0.0.0 255.0.0.0 gateway 172.23.222.32
storm-ha-194/admin(config)# end
storm-ha-194/admin# write memory
```

# マルチ NIC サーバーの動作

静的ルートは、バックアップの復元プロセスの一部として移行されません。復元後に手動で設定する必要があります。ただし、この設定は、アップグレードされた[バックアップ/リストア/アップグレード（Backup and Restore Upgrade）] サーバーに保持できます。

HA 環境では、次の手順を実行します。

- 最初のインターフェイス（ハートビートに使用（最初のインターフェイス））障害によって、HA フェールオーバーが発生します。
- 設定によっては、追加のNICに障害が発生するとフェールオーバーがトリガーされます。詳細については、「複数の NIC のモニタリングの有効化」を参照してください。

# IP 設定の削除

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# interface gigabitEthernet 1
storm-ha-194/admin(config-GigabitEthernet)# no ip 172.23.222.32 255.255.255.0
```

# 複数の NIC のモニタリングの有効化

Cisco EPN Manager では、モニター可能な複数のインターフェイスを追加できます。登録すると、モニター対象の NIC の設定がセカンダリサーバーにコピーされ、この時点からシステムがインターフェイスをモニターします。プライマリサーバーのモニター対象のインターフェイスがダウンした場合、システムはセカンダリサーバーへのフェールオーバーを実行します（モニター対象のすべてのインターフェイスがセカンダリサーバーで稼働している場合のみ）。新しいプライマリサーバーにフォールバックする場合、監視対象の NIC は新しいプライマリサーバーにコピーされます。プライマリサーバーとセカンダリサーバーの有効な NIC の数が異なっている場合、登録と新しいプライマリ操作へのフォールバックは禁止されます（システムは適切なメッセージで通知します）。

複数の NIC（モニタリング）のサポートを有効にするには、次の手順を実行します。

- Cisco EPN Manager の CLI 管理者ユーザーとしてサーバーにログインします。
- 次のコマンドを入力してインターフェイスを追加します。

```
ncs ha monitor interface add <interface-name>
```

（注） インターフェイスを削除するには、次のコマンドを入力します。

```
ncs ha monitor interface del <interface-name>
```

- （オプション）次のコマンドを実行して設定を確認します。

```
show run
```

# Cisco EPN Manager のアンインストール

## Cisco EPN Manager のアンインストール（OVA/VM）

### はじめる前に

バックアップを実行します。次の方法を使用した Cisco EPN Manager のアンインストールでは、サーバー設定およびローカルバックアップなどのサーバー上のすべてのデータが完全に削除されます。リモート バックアップがない場合、データを復元できません。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のバックアップのトピックを参照してください。

**ステップ 1** VMware vSphere クライアントで、Cisco EPN Manager 仮想マシンを右クリックします。

**ステップ 2** 仮想マシンの電源をオフにします。

**ステップ 3** [ディスクから削除（Delete from Disk）] をクリックして、Cisco EPN Manager 仮想アプライアンスを削除します。

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