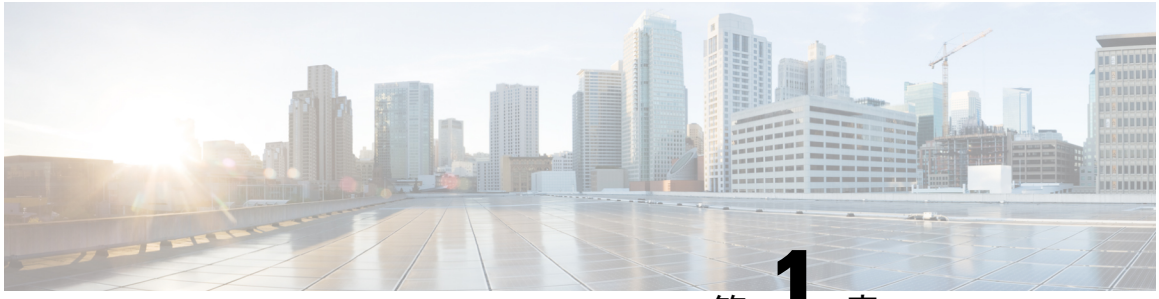
Cisco Evolved Programmable Network Manager 7.1 インストールガイド

初版：2023 年 8 月 31 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。



第 1 章

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 （23 ページ）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 （33 ページ） 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（非 HA）」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 （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 （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。 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）。 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。 **ncs pnp-gateway disable** **ncs stop** **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。

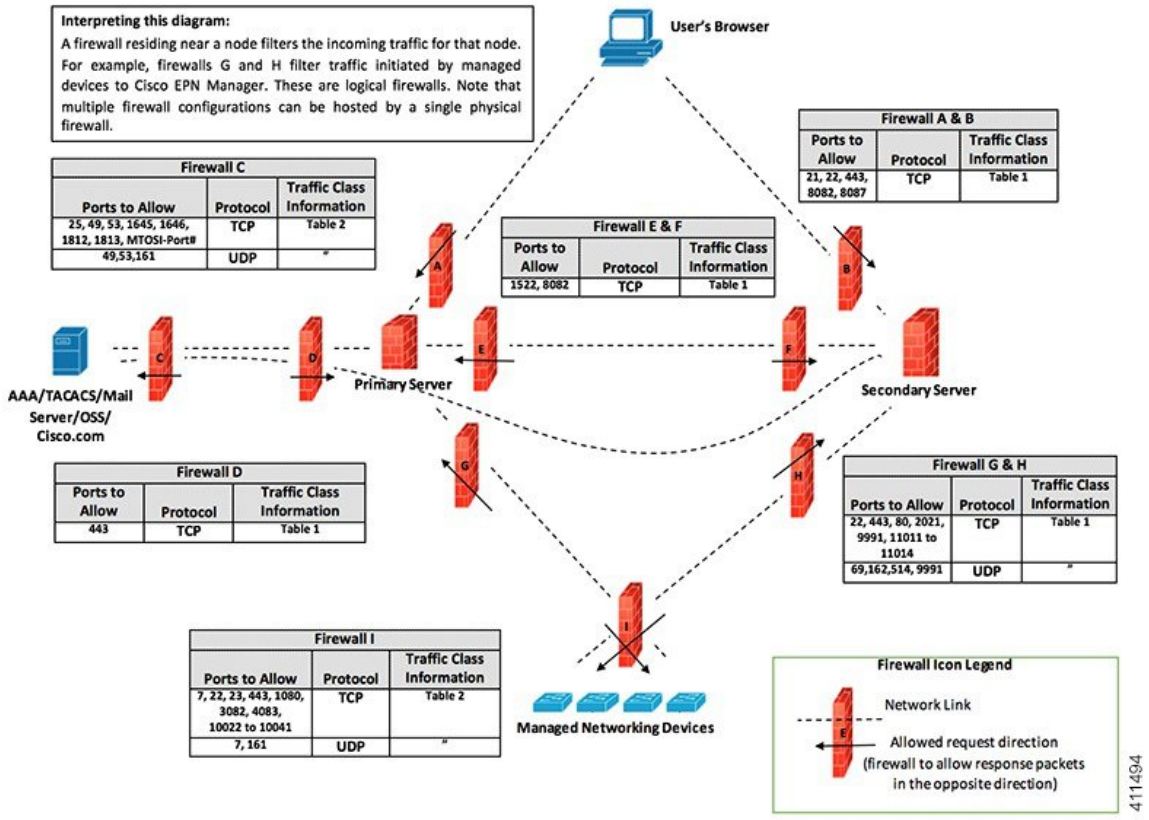
Cisco EPN Manager がこれらのデバイスに接続できるようにするには、必要なポートを開く必要があります。

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

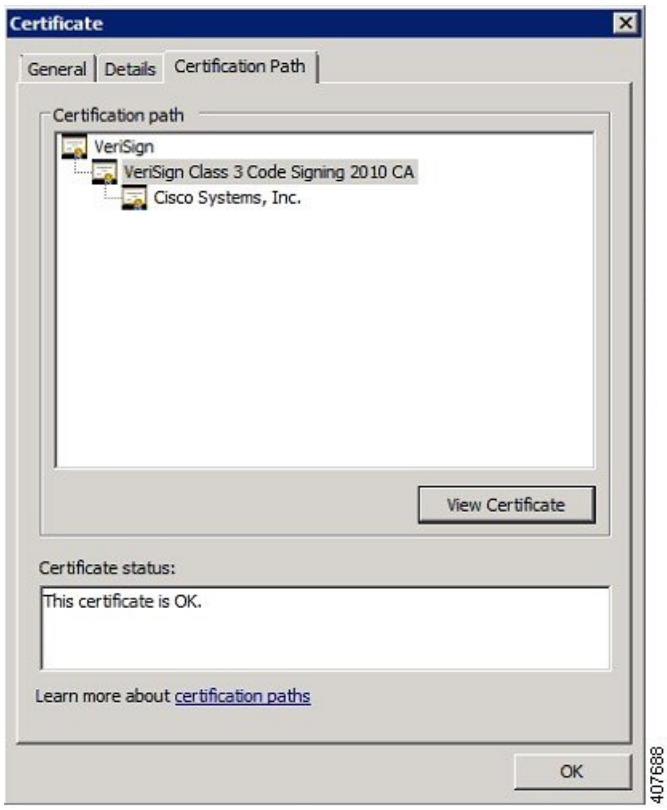
Cisco EPN Manager をインストールする前に、OVA パッケージを確認する必要があります。OVA パッケージ内にバンドルされている個々の UBF ファイルを確認する必要はありません。

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。 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。 • セカンダリ ネームサーバーを入力する場合は **Y**。 • 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**）。 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。 • NTP サーバーを入力する場合は **Y**。 • 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。 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。 • クロック タイムを変更する場合は **Y**。 • 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 （28 ページ）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）

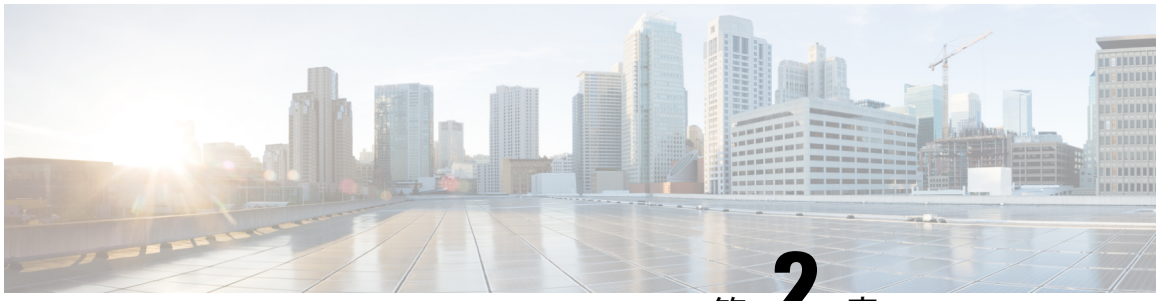
はじめる前に

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。



第 2 章

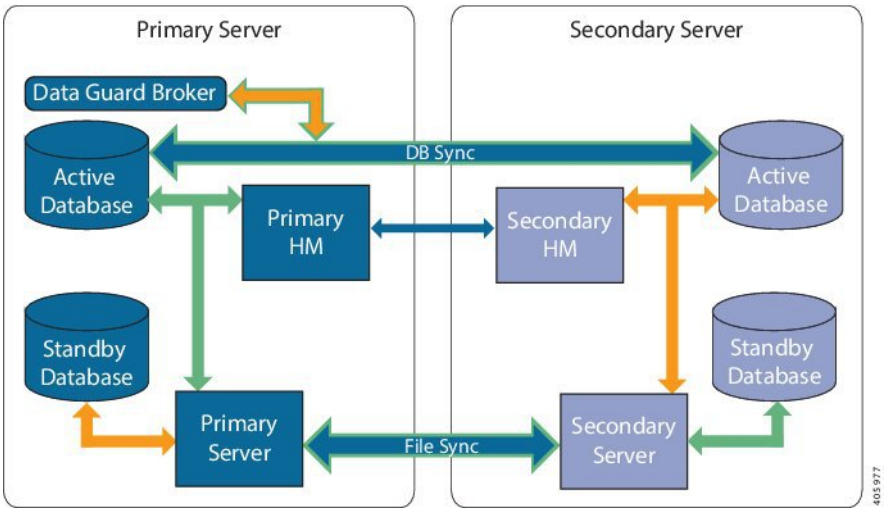
Cisco EPN Manager 7.1 高可用性インストール

この章では、高可用性環境における Cisco EPN Manager に関する情報を示します。

高可用性の概要

Cisco EPN Manager 高可用性（HA）システムは、障害発生時に継続的なシステム動作を確保します。HA では、リンクされて同期された Cisco EPN Manager サーバーのペアを使用して、いずれかのサーバーで発生する可能性のあるアプリケーション障害またはハードウェア障害による影響を最小限に抑えるか、あるいは完全に排除します。

次の図に、高可用性展開の主なコンポーネントとプロセス フローを示します。



高可用性展開は、プライマリ サーバーとセカンダリ サーバーで構成され、両方のサーバー上にヘルス モニター（HM）インスタンス（アプリケーション プロセスとして実行）が存在します。プライマリ サーバーに障害が発生すると（問題が発生したためか、または手動で停止させたため）、プライマリ サーバーへのアクセスを復元する間はセカンダリ サーバーがネットワークの管理を引き継ぎます。自動フェールオーバーするように展開を設定すると、プライマリ サーバーの障害発生後 2 ～ 3 分以内にセカンダリ サーバーがアクティブなロールを引き継ぎます。

プライマリ サーバーに関する問題が解決し、サーバーが実行状態になっても、スタンバイ モードのままとなり、アクティブなセカンダリ サーバーとのデータの同期が開始されます。フェールバックがトリガーされると、プライマリ サーバーがアクティブなロールを再度引き継ぎます。プライマリ サーバーとセカンダリ サーバーの間でのこのロールの切り替えは、障害後、プライマリ サーバーが再インストールされていない限り、通常、約 2 ～ 3 分かかります。プライマリ サーバーが再インストールされている場合は、（セットアップのサイズに基づき）それよりも長く時間がかかります。

HA 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 HA に関する項を参照してください。

高可用性展開の考慮事項

高可用性展開のモデル

Cisco EPN Manager は、次の高可用性（HA）展開モデルをサポートしています。

HA 展開モデル	プライマリ サーバーとセカンダリ サーバーの場所	例：
ローカル（Local）	同じサブネット上（レイヤ 2 プロキシミティ）	同じデータ センターにあるサーバー
キャンパス（Campus）	LAN 経由で接続されているさまざまなサブネット	同じキャンパス、市区町村、県などにあるサーバー
リモート（Remote）	WAN 経由で接続されているさまざまなサブネット	サーバーが地理的に分散している

ローカル、キャンパス、またはリモートの HA 展開モデルを使用するかどうかの決定時には、次の要因を考慮してください。

- 災害へのリスク：展開モデルの分散が多いほど、自然災害によるビジネスへのリスクが軽減されます。リモートからの HA 展開は自然災害による影響を最も受けにくく、複雑さとコストが軽減されたビジネス継続性モデルを実現できます。ローカルでの HA 展開は、サーバー コロケーションにより災害に対して最も脆弱になります。
- 仮想 IP アドレスを使用できるかどうか：ローカルでの HA 展開のみが仮想 IP アドレスを使用できます。仮想 IP アドレスは、フェールオーバーやフェールバックの後でも、常にアクティブなサーバーを指す単一の IP アドレスです。また、プライマリ サーバーとセカンダリ サーバーの両方で共通の管理 IP アドレスを共有することもできます。
- 帯域幅/遅延：プライマリ サーバーとセカンダリ サーバーは、帯域幅が高く、遅延が小さい短いネットワーク リンクによって接続されているため、ローカル HA 展開において帯域幅は最も高くなり、遅延は最も小さくなります。キャンパス HA 展開では、ローカルでの HA 展開よりも帯域幅が低くなり、遅延が大きくなる場合があります。リモートからの HA 展開では、帯域幅は最も低く、遅延は最も大きくなります。
- 管理：HA 管理は、ローカルでの HA 展開で最も簡単ですが、キャンパスおよびリモートの HA 展開の場合はより複雑になります。リモートでの HA 展開には、管理上の修復が必要になります。
- デバイス イベントの転送の設定：イベント転送の設定は、ローカルでの HA 展開が最も簡単です。これは、仮想 IP アドレスを使用し、その単一の仮想 IP アドレスにイベントを転送するようにデバイスを設定できるためです。仮想 IP アドレスを使用しない場合は、プライマリ サーバーとセカンダリ サーバーの両方にイベントを転送するようにデバイスを設定する必要があります。

HA 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』を参照してください。

高可用性の制限について

Cisco EPN Manager の HA システムには、次の制限要因が適用されます（これは、すべての高可用性展開モデルに適用されます）。

- HA システムでは、HA 動作に対応するために、少なくとも 500 Mbps（メガビット/秒）以上のネットワーク帯域幅が必要です。これらの操作には、HA 登録、データベース同期、ファイル同期、フェールバックのトリガーが含まれます（ただし、これらに限定されません）。Cisco EPN Manager は、すべてのネットワーク ニーズに単一の物理ポートを使用するため、帯域幅が不十分になり、HA パフォーマンスに影響を与える可能性があります。
- HA システムでは、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リンク上は低遅延（最大 100 ms、70 ms 未満を推奨）が必要です。この 2 台のサーバーの物理的な近接性に関わらず、サーバー間のリンクで発生する遅延が大きい場合、Cisco EPN Manager によるプライマリ サーバーとセカンダリ サーバー間のセッション維持状態に影響が及ぶ可能性があります。これは、大規模なデータベースには、より低い遅延とより高い帯域幅を必要とする同期トランザクションが多く必要になるためです。Cisco EPN Manager を使用して比較的小規模なネットワークを管理している場合、データベースは小さいため、HA はネットワーク遅延が長くなり、帯域幅が低くなる可能性があります。

- HAパフォーマンスは、プライマリ サーバーとセカンダリ サーバーに接続するネットワークが提供するネットワーク スループットに大きく影響されます。この制約は、すべての展開モデルに（ある程度まで）適用されます。たとえば、地理的に分散した展開では、低帯域幅と高遅延により、リモート HA 展開に問題が発生する可能性が高くなります。ただし、ローカルおよびキャンパスでの HA 展開が正しく設定されていない場合、使用率の高いネットワークでの帯域幅の制限により、遅延による問題の影響を非常に受けやすくなります。

さまざまなHAのどれにネットワークが適しているかを判断するには、シスコの担当者に問い合わせ、支援を受けてください。

仮想アドレスを使用できるかどうかの検討

ローカル HAは 展開のセットアップに仮想 IP アドレスを使用すると、ユーザーは実際にアクティブなサーバーを知らなくても、単一の IP アドレスまたは Web URL を使用してアクティブなサーバーに接続できます。仮想 IP アドレスを使用すると、両方のサーバーが共通の管理 IP アドレスを共有することもできます。通常の操作中、仮想 IP アドレスはプライマリ サーバーをポイントします。フェールオーバーが発生すると、仮想 IP アドレスはセカンダリ サーバーを自動的にポイントします。フェールバックが発生すると、仮想 IP アドレスは自動的にプライマリ サーバーに切り替わります。

仮想 IP アドレスを使用するには、次の IP アドレスが同じサブネット上にある必要があります。

- 仮想 IP アドレス
- プライマリ サーバーおよびセカンダリ サーバーの IP アドレス
- プライマリ サーバーとセカンダリ サーバーに設定されているゲートウェイの IP アドレス

次に、仮想、プライマリ、およびセカンダリのIPアドレスを相互に割り当てる例を示します。プライマリ サーバーとセカンダリ サーバーに、特定のサブネット内の次の IP アドレスが割り当てられている場合は、両方のサーバーの仮想 IP アドレスは次のように割り当てることができます。

- サブネット マスク：255.255.255.224（/32）
- プライマリ サーバーの IP アドレス：10.10.101.1
- セカンダリ サーバーの IP アドレス：10.10.101.2
- 仮想 IP アドレス：10.10.101.[3-30] 例：10.10.101.3。仮想 IP アドレスは、特定のサブネット マスクで有効なアドレス範囲内の任意のアドレスになることに注意してください。

仮想 IP アドレスを使用しない場合は、プライマリ サーバーとセカンダリ サーバーの両方にイベントを転送するように（特定のサブネット、またはプライマリ サーバーとセカンダリ サーバーの両方を含む IP アドレスの範囲にイベントを転送するなどによって）デバイスを設定する必要があります。データを損失する可能性を低減する（または排除する）には、フェールオーバーが発生する前にデバイス イベントの転送を設定する必要があります。インストール中にセカンダリ サーバーに変更を加える必要はありません。プライマリ サーバーとセカンダリ サーバーを個別の IP アドレスでプロビジョニングするだけです。

HA 展開で単一の IP アドレスを使用するかどうかにかかわらず、ユーザーはアクティブなサーバー IP アドレス/URL を使用して Cisco EPN Manager Web GUI に常に接続する必要があります。

高可用性インストールの前提条件

次に、高可用性展開で Cisco EPN Manager をインストールする前に満たす必要がある前提条件を示します。

- ハードウェアとソフトウェアが、関連するトピックに示されている前提条件を満たしていることを確認します。
  - OVA/VM の要件
- セカンダリ サーバーが次のように設定されていることを確認します。
  - セカンダリ サーバーのハードウェアとソフトウェアの仕様は、プライマリ サーバーの仕様と同じである必要があります。たとえば、プライマリ サーバーに Cisco EPN Manager をインストールし、プロフェッショナル システム サイズを指定した場合、セカンダリ サーバーも プロフェッショナル システム サイズを使用してインストールする必要があり、また、「システム要件」に プロフェッショナル サイズ サーバーの要件すべてを満たす必要があります。
  - セカンダリ サーバーは、プライマリ サーバーと同じソフトウェア レベル（パッチ レベルを含む）を実行している必要があります。
  - ローカル HA 展開に仮想 IP アドレスを使用する場合は、仮想 IP アドレス、プライマリ サーバーおよびセカンダリ サーバーが同じサブネット上にある必要があります。プライマリ サーバーとセカンダリ サーバー上のゲートウェイも同じサブネット上に存在する必要があります。
- プライマリ サーバーとセカンダリ サーバーの間にファイアウォールがある場合は、HA で使用されるポートに対するファイアウォールからのアクセス許可が必要です。ポートは、「Cisco EPN Manager で使用するポート」に記載されています。
- インストール中に入力する必要がある次の情報を準備します。
  - セカンダリ サーバーの IPv4 IP アドレスまたはホスト名（仮想 IP アドレスを使用していない場合）。プライマリ サーバーで HA を設定する際に必要になります。
  - 両方のサーバーに使用する仮想 IPv4 と IPv6（使用している場合）の IP アドレス（仮想 IP アドレスを使用する予定の場合）。
  - HA 認証キーに使用するパスワード。このパスワードは、セカンダリ サーバーのインストール時にユーザーが指定したものです。プライマリ サーバーとセカンダリ サーバー間の通信の認証に使用されます。HA を設定する際、つまり、プライマリ サーバーにセカンダリ サーバーを登録する（サーバーのペアリングともいう）ときに入力

する必要があります。最後に、セカンダリ サーバーの [ヘルス モニター（Health Monitor）] ページへのログインに必要になります。

- プライマリ サーバーの管理権限を持つ Cisco EPN Manager Web GUI のユーザー ID。また、ユーザーのパスワードも必要です。
- HA 通知を送信できる有効な電子メール アドレス。

高可用性展開での Cisco EPN Manager 7.1 のインストール

この項の手順は、高可用性環境で製品を新規にインストールするための手順です。以前のバージョンから Cisco EPN Manager 7.1 にアップグレードする場合は、「Cisco EPN Manager 7.1 へのアップグレード（高可用性）」を参照してください。

はじめる前に

サーバーが「高可用性インストールの前提条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。

ステップ 1 「Cisco EPN Manager 7.0 のインストール（非HA）」に記載されているように、Cisco EPN Manager をプライマリサーバーにインストールします。

ステップ 2 「Cisco EPN Manager 7.0 のインストール（非HA）」に記載されているように、Cisco EPN Manager をセカンダリサーバーにインストールします。

ステップ 3 新たにインストールしたサーバーを HA 実装環境でセカンダリ フォールバック 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たら、**yes** と入力します。

ステップ 4 プライマリ サーバーとセカンダリ サーバー間の通信に*HA* 認証キーとして使用するパスワードを入力します。HA を設定するには、このキーが必要になります。（通常の操作中に、セカンダリ サーバーの [ヘルス モニター（Health Monitor）] ページにログインするには、HA 認証キーを入力する必要があります）。

ステップ 5 確認のため、パスワードを再入力します。

ステップ 6 このサーバーをセカンダリ サーバーとしてインストールすることを確認するには、**Y** と入力します。インストールが完了すると、VM（OVA/VM）がリブートします。

ステップ 7 インストール時に指定した Cisco EPN Manager CLI 管理者ユーザー名とパスワードを使用してログインします。

ステップ 8 イベント（syslog、trap、および TL1 メッセージ）を両方のサーバー（または仮想 IP アドレスを使用している場合は仮想IPアドレス）に転送するように、すべてのデバイスが設定されていることを確認します。

（注） プライマリ サーバーにセカンダリ サーバーを登録する前にこの手順を実行せず、フェールオーバーが発生した場合、一部のデータを損失する場合があります。

ステップ 9 プライマリ サーバーにセカンダリ サーバーを登録して HA を設定します。登録プロセスはプライマリ サーバーから実行する必要があります。詳細については、『Cisco Evolved Programmable Network Manager User

and Administrator Guide』のプライマリサーバーへのセカンダリサーバーの登録に関するセクションを参照してください。

HA 設定の準備状況の確認

HA 設定時に、HA に関連する他の環境パラメータ（システム仕様、ネットワーク構成、サーバー間の帯域幅など）によって HA 設定が完了したかが判別されます。

15 のチェックがシステムで実行され、エラーや障害なく HA 設定が完了したことが確認されます。準備状況の確認機能を実行すると、チェックリストの名前および対応するステータスが、該当する場合は推奨事項とともに表示されます。

（注） **準備状況の確認**によって HA 設定がブロックされることはありません。すべてのチェックに合格しなくても、HA を設定できます。

プライマリとセカンダリの認証キーが異なる場合、準備状況チェックは続行されません。HA 登録を続行できます。

HA 設定の準備状況を確認するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Cisco EPN Manager によって HA ステータス ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択します。

ステップ 4 [セカンダリサーバー（Secondary Server）] フィールドにセカンダリサーバーの IP アドレスを入力し、[認証キー（Authentication Key）] フィールドにセカンダリの認証キーを入力します。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックします。

ポップアップウィンドウが開き、システム仕様およびその他のパラメータが表示されます。画面には、チェックリスト項目の名前、ステータス、影響、推奨事項の詳細が示されます。

その下に、準備状況の確認に使用されたチェックリストのテスト名と説明のリストが表示されます。

表 *3*：チェックリストの名前と説明

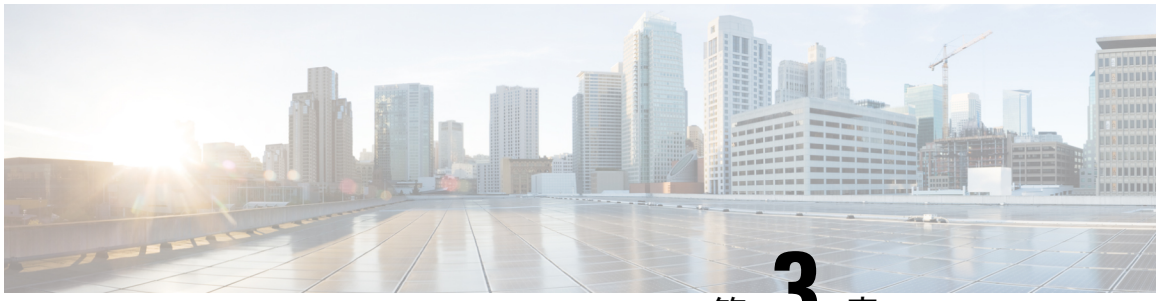
チェックリストのテスト名	テストの説明
システム - CPU数の確認（SYSTEM - CHECK CPU COUNT）	プライマリサーバーとセカンダリサーバーの CPU 数を確認します。 両方のサーバーの CPU 数が要件を満たしている必要があります。

システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリサーバーとセカンダリサーバーのディスク速度を確認します。 必要な最小ディスク速度は 200 Mbps です。
システム - RAM サイズの確認（SYSTEM - CHECK RAM SIZE）	プライマリサーバーとセカンダリサーバーの RAM サイズを確認します。 両方のサーバーの RAM サイズが要件を満たしている必要があります。
システム - ディスクサイズの確認（SYSTEM - CHECK DISK SIZE）	プライマリサーバーとセカンダリサーバーのディスクサイズを確認します。 両方のサーバーのディスクサイズが要件を満たしている必要があります。
システム - サーバーへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリサーバーが ping を介してセカンダリサーバーに到達できることを確認します。
システム - OS互換性の確認（SYSTEM - CHECK OS COMPATABILITY）	プライマリ サーバーとセカンダリ サーバーの OS バージョンが同じであることを確認します。
システム - ヘルス モニターのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルスモニタープロセスがプライマリサーバーとセカンダリサーバーで実行されているかどうかを確認します。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	インターフェイス eth0 の速度がプライマリサーバーとセカンダリサーバーで推奨されている 100 Mbps に一致しているかどうかを確認します。 このテストでは、プライマリサーバーとセカンダリサーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - データベース ポートの開閉についてファイアウォールの確認（NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY）	データベース ポート 1522 がシステム ファイアウォールで開いているかどうかを確認します。 このポートが無効になっていると、テストは IP テーブルリストで 1522 の権限を付与します。
データベース - オンラインステータスの確認（DATABASE - CHECK ONLINE STATUS）	データベースファイルのステータスがオンラインになっており、プライマリサーバーとセカンダリサーバーでアクセス可能であるかどうかを確認します。
データベース - メモリターゲットの確認（DATABASE - CHECK MEMORY TARGET）	HA セットアップの「/dev/shm」データベース メモリ ターゲット サイズを確認します。

データベース - リスナーのステータス（DATABASE - LISTENER STATUS）	プライマリサーバーとセカンダリサーバーでデータベースリスナーが稼働中であるかどうかを確認します。 障害が発生した場合、テストによってリスナーの起動とステータスの報告が試行されます。
データベース - リスナー設定ファイルの破損確認（DATABASE - CHECK LISTENER CONFIG CORRUPTION）	すべてのデータベースインスタンスがデータベースリスナー設定ファイル「listener.ora」に存在するかどうかを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	すべての「WCS」インスタンスがデータベース TNS リスナー設定ファイル「tnsnames.ora」に存在するかどうかを確認します。
データベース - TNS 到達可能性のステータス（DATABASE - TNS REACHABILITY STATUS）	プライマリサーバーとセカンダリサーバーで TNSPING が成功しているかどうかを確認します。

ステップ 6 すべてのパラメータのチェックが完了したら、パラメータのステータスを確認し、[クリア（Clear）] をクリックしてウィンドウを閉じます。

（注） **準備状況の確認**中のフェールバック イベントとフェールオーバー イベントは、[アラームおよびイベント（Alarms and Events）] ページに転送されます。設定障害イベントは [アラームおよびイベント（Alarms and Events）] リストに表示されません。



第 3 章

Cisco EPN Manager 7.1 へのアップグレード

以下の有効なアップグレード パス （33 ページ）のいずれかに従って、Cisco EPN Manager 7.1 にアップグレードできます。

この章では、バックアップ/復元アップグレードを使用して Cisco EPN Manager 7.1 へアップグレードする手順を説明します。

バックアップ/復元アップグレードには、現在インストールされているバージョンの Cisco EPN Manager からのすべてのデータのバックアップ、次に、新しいサーバーへの Cisco EPN Manager 7.1 のインストール、さらに、新しい Cisco EPN Manager 7.1 サーバーへのバックアップされたデータの復元が含まれます。

有効なアップグレード パス

次の表に、以前のバージョンから Cisco EPN Manager 7.1 へのインストール/アップグレードに有効なパスを示します。

現在の Cisco EPN Manager バージョン	Cisco EPN Manager 7.1.0 へのインストールパス
Cisco EPN Manager 7.0.1	**Cisco EPN Manager 7.0.1 > 7.1.0**
Cisco EPN Manager 6.1.1	**Cisco EPN Manager 6.1.1 > 7.1.0**
Cisco EPN Manager 6.0.1.1	**Cisco EPN Manager 6.0.1.1 > 7.1.0**

Cisco EPN Manager バージョンのインストールの前提条件と手順については、関連するインストール ガイドを参照してください。

ポイントパッチのインストール手順については、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の readme ファイルを参照してください。

Cisco EPN Manager 7.1 へのアップグレードの前提条件

アップグレードを開始する前に、次の手順を実行します。

1. 現在のバージョンの Cisco EPN Manager に基づいて、関連するアップグレード パスに従っていることを確認します。有効なアップグレードパス（33ページ）を参照してください。
2. 展開が関連する前提条件トピックの要件を満たしていることを確認します。
   - OVA/VM のインストールの前提条件。OVA/VM 展開の場合、アップグレードは VMware vSphere クライアントから実行されます。
3. 認定されていないソフトウェア バージョンを Cisco EPN Managerから実行しているデバイスを削除します。この手順は必須ではありませんが、強くお勧めします。
4. データをバックアップする。「データのコピーの作成」を参照してください。
5. バックアップが実行されていないことを確認します。
6. SCP がクライアント マシン上で有効になっており、必要なポートが開いていることを確認します（「Cisco EPN Manager で使用するポート」を参照）。SCP を使用して、クライアント マシンから Cisco EPN Manager サーバーにファイルをコピーする必要があります。
7. /localdisk/defaultRepo にある gpg ファイルを外部リポジトリにコピーし、このフォルダからそれらのファイルを削除します。

（注） EPNM で NCS1001 の OTDR 機能を使用しているお客様は、次の手順を実行する必要があります。

```
Take a backup of /opt/CSCOlumos/conf/ncs1k-otdr-ports.xml. The below feature entry has
to be updated in /opt/CSCOlumos/conf/Migration.xml to retain the OTDR mapping configuration
 done for NCS1001 devices.
<feature name="Otdr-ports-Properties">
<files>
<file optional="true">/opt/CSCOlumos/conf/ncs1k-otdr-ports.xml</file>
</files>
</feature>
```

データのコピーの作成

現在のデータのコピーを作成するには、データをリモートリポジトリにバックアップします。『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。必要に応じて、データを復元することによって以前のバー

ジョンに戻すことができます。「データ復元を使用して以前のバージョンに戻す」を参照してください。

Cisco EPN Manager 7.1 へのアップグレード（非 HA）

次のトピックで、標準展開（高可用性なし）で以前のバージョンの Cisco EPN Manager から Cisco EPN Manager 7.1 にアップグレードする方法について説明します。

- バックアップ/復元アップグレード（非 HA）
- アップグレード後のタスク

高可用性展開でアップグレードを実行する場合は、Cisco EPN Manager 7.1 へのアップグレード（高可用性） （36 ページ）を参照してください。

バックアップ/復元アップグレード（非 HA）

バックアップ/復元アップグレードには、現在インストールされているバージョンの Cisco EPN Manager からのすべてのデータのバックアップ、次に、新しいサーバーへの Cisco EPN Manager 7.1 のインストール、さらに、新しい Cisco EPN Manager 7.1 サーバーへのバックアップされたデータの復元が含まれます。これは推奨されるアップグレード方法です。

はじめる前に

- 新しいサーバーがバックアップ元のサーバーと同じハードウェア仕様であることを確認します。
- 以前のサーバーが使用するリモートバックアップリポジトリの場所に注意してください。新しいサーバーと同じバックアップ場所を設定する必要があります。

ステップ 1 『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のリモート バックアップ リポジトリに関するトピックに記載されているように、以前のサーバーと同じリモートバックアップ リポジトリを使用するように新しいサーバーを設定します。

ステップ 2 『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のリモート バックアップ リポジトリに関するトピックに記載されているように、リモート リポジトリのバックアップを新しいサーバーに復元します。

アップグレード後のタスク

- Cisco Smart Licensing を使用している場合、cisco.com の Cisco Smart Software Manager（CSSM）に、Cisco EPN Manager を再登録します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のライセンスの管理を説明するトピックを参照してください。

- すべてのデバイスのインベントリを次のようにデータベースと同期します。
  1. Cisco EPN Manager GUI で、[モニター（Monitor）]>[ネットワーク デバイス（Network Devices）] を選択します。
  2. すべてのデバイスを選択し、[同期（Sync）] をクリックします。
- アップグレードされた Cisco EPN Manager サーバーへの接続を試行する前に、Cisco EPN Manager の以前のバージョンにアクセスしたすべてのクライアント マシンのブラウザ キャッシュをクリアするようにユーザーに指示します。
- アップグレード前に外部 AAA を使用していた場合は、外部認証をもう一度設定します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のユーザー管理に関するトピックを参照してください。
- アップグレード中に、Cisco EPN Manager ホーム ページがデフォルトのホーム ページ（[はじめに（Getting Started）] ページ）にリセットされます。ユーザーは、[はじめに（Getting Started）] ページまたはページの右上にある [設定（Settings）] メニューから、独自のデフォルト ホーム ページを選択できます。

既存のタブの新しいダッシュレットは、アップグレード後に自動的に追加されることはありません。ダッシュレットはダッシュボードメニューの [設定（Settings）]>[ダッシュレットの追加（Add Dashlet(s)）] から手動で追加できます。

手動で作成されたコマンドセット（例：ip access-list、チームインターフェイスまたはインターフェイス GigabitEthernet 1、追加の NTP サーバーおよび IP ルート）は、アップグレード後は使用できなくなります。ユーザーが手動で追加する必要があります。『**Cisco Evolved Programmable Network Manager コマンドリファレンスガイド**』を参照してください。

新しいダッシュボード タブが自動的に追加されます。

Cisco EPN Manager 7.1 へのアップグレード（高可用性）

以降のトピックで、高可用性展開で Cisco EPN Manager 7.1 にアップグレードするための手順を示します。

バックアップ/復元アップグレード（高可用性）

（注） アップグレードが完了するまで、高可用性は機能しません。

バックアップ/復元アップグレード（高可用性）

HA 環境でのバックアップ/復元のアップグレードには、次の手順で詳しく説明する次の基本的な手順が含まれます。

1. HA を削除します。

2. データをリモート リポジトリにバックアップします。
3. プライマリ サーバーとセカンダリ サーバーの両方で Cisco EPN Manager の新規インストールを実行します。
4. プライマリ サーバーでバックアップ データを復元します。
5. HA を再設定します。

はじめる前に

- 展開が一般的な HA 要件を満たしていることを確認します。
- 展開がアップグレード固有の要件を満たしていることを確認します。
- 新しいサーバーが少なくともバックアップ元のサーバーと同じハードウェア仕様であることを確認します。
- 以前のサーバーが使用するリモート バックアップ リポジトリの場所に注意してください（該当する場合）。新しいサーバーと同じバックアップ場所を設定する必要があります。
- HA を有効にしたときに作成したパスワード（認証キー）があることを確認します。このパスワードは、セカンダリサーバーで Cisco EPN Manager のインストールを実行するために必要になります。

ステップ 1 プライマリ サーバーで、高可用性設定を削除します。

1. 管理者権限を持つユーザーとして Cisco EPN Manager にログインします。
2. [管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] を選択します。
3. HA 設定を書き留めます。アップグレード後に HA を再設定するには、この情報が必要です。
4. 左側のナビゲーション領域で [HA 設定（HA Configuration）] を選択し、[削除（Remove）] をクリックします。
5. 削除操作が完了するまで待ちます。
6. 左側のナビゲーション領域で、[HA 設定（HA Configuration）] をクリックし、[設定モード（Configuration Mode）] フィールドに [HA 設定なし（HA Not Configured）] が表示されていることを確認します。

ステップ 2 データをリモート リポジトリにバックアップします。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のバックアップに関するトピックを参照してください。

（注） リモート リポジトリがない場合は、リポジトリを設定します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のリモート バックアップ リポジトリに関するトピックを参照してください。

ステップ 3 新しいプライマリサーバーを設定して、以前のプライマリサーバーと同じリモートバックアップ リポジトリ（ステップ *2*で使用したリポジトリ）を使用します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のリモート バックアップ リポジトリに関するトピックを参照してください。

ステップ 4 プライマリ サーバー（のみ）で、リモート リポジトリからバックアップを復元します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のデータ復元に関するトピックを参照してください。

（注） プライマリ サーバーでの復元操作の実行のみが必要です。HA が再び有効になると、セカンダリ サーバーはプライマリ サーバーと同期されます。

ステップ 5 プライマリ サーバー：

1. サーバーが再起動していることを確認します。
2. **ncs status** コマンドを実行して、ヘルス モニター プロセスとその他のプロセスが再起動したことを確認します。最低でもヘルス モニター、データベース、NMS、SAM デーモン、DA デーモン、コンプライアンス エンジンの各サービスが稼働していることを確認します。最適な Cisco EPN Manager 機能を使用するには、すべてのサービスが稼働している必要があることに注意してください。

ステップ 6 復元が完了したら、プライマリ サーバーでアップグレード後のタスクを実行します。「アップグレード後のタスク」を参照します。

ステップ 7 プライマリ サーバーにセカンダリ サーバーを登録して HA を再設定します。ステップ 1 で保存した情報を使用します。登録プロセスはプライマリ サーバーから実行する必要があります。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』のプライマリ サーバーへのセカンダリ サーバーの登録に関する項を参照してください。

アップグレード後のタスク

- Cisco Smart Licensing を使用している場合、cisco.com の Cisco Smart Software Manager（CSSM）に、Cisco EPN Manager を再登録します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のライセンスの管理を説明するトピックを参照してください。
- すべてのデバイスのインベントリを次のようにデータベースと同期します。
  1. Cisco EPN Manager GUI で、[モニター（Monitor）]>[ネットワーク デバイス（Network Devices）] を選択します。
  2. すべてのデバイスを選択し、[同期（Sync）] をクリックします。
- アップグレードされた Cisco EPN Manager サーバーへの接続を試行する前に、Cisco EPN Manager の以前のバージョンにアクセスしたすべてのクライアント マシンのブラウザ キャッシュをクリアするようにユーザーに指示します。
- アップグレード前に外部 AAA を使用していた場合は、外部認証をもう一度設定します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のユーザー管理に関するトピックを参照してください。
- アップグレード中に、Cisco EPN Manager ホーム ページがデフォルトのホーム ページ（[はじめに（Getting Started）] ページ）にリセットされます。ユーザーは、[はじめに（Getting

Started）] ページまたはページの右上にある [設定（Settings）] メニューから、独自のデフォルト ホーム ページを選択できます。

既存のタブの新しいダッシュレットは、アップグレード後に自動的に追加されることはありません。ダッシュレットはダッシュボードメニューの [設定（Settings）] > [ダッシュレットの追加（Add Dashlet(s)）] から手動で追加できます。

手動で作成されたコマンドセット（例：ip access-list、チームインターフェイスまたはインターフェイス GigabitEthernet 1、追加の NTP サーバーおよび IP ルート）は、アップグレード後は使用できなくなります。ユーザーが手動で追加する必要があります。『**Cisco Evolved Programmable Network Manager コマンドリファレンスガイド**』を参照してください。

新しいダッシュボード タブが自動的に追加されます。

以前のバージョンの Cisco EPN Manager への復帰

この項では、高可用性環境と標準環境の両方で、Cisco EPN Manager をインストールした後に Cisco EPN Manager の以前のバージョンに戻す方法について説明します。これは手動プロセスであり、自動ロールバックはサポートされていません。

（注） 「データのコピーの作成」で説明したように、Cisco EPN Manager インストールする前にデータのコピーを作成していた場合にのみ、以前のバージョンに戻すことができます。

以前のバージョンの Cisco EPN Manager に戻す手順は、データのコピーの作成に使用した方法によって異なります。

- バックアップ機能を使用した場合は、「データ復元を使用して以前のバージョンに戻す」を参照してください。
- VM スナップショットを取得した場合は、「VM のスナップショットを使用して以前のバージョンに戻す」を参照してください。

データ復元を使用して以前のバージョンに戻す

バックアップ機能を使用してデータのコピーを作成した場合は、次の手順のいずれかを使用して Cisco EPN Manager の以前のバージョン（非 HA または HA）に戻します。

非 HA 環境の場合は、次の手順を実行します。

1. Cisco EPN Manager の以前のリリース（バックアップ元のリリース）を再インストールします。
2. バックアップからデータを復元します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のデータ復元に関するトピックを参照してください。

HA 環境の場合は、次の手順を実行します。

1. プライマリ サーバーとセカンダリ サーバーで Cisco EPN Manager の以前のリリース（バックアップを行ったリリース）を再インストールします。
2. プライマリ サーバーで、バックアップからデータを復元します。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のデータ復元に関するトピックを参照してください。
3. HA を設定し、プライマリ サーバーにセカンダリ サーバーを登録します。登録プロセスはプライマリ サーバーから実行する必要があります。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』のプライマリ サーバーへのセカンダリ サーバーの登録に関する項を参照してください。

VM のスナップショットを使用して以前のバージョンに戻す

インストールに VM を使用しており、インストール前に VM のスナップショットを取得した場合は、次のいずれかの手順に従って、Cisco EPN Manager の以前のバージョンに戻します（非 HA または HA）。

非 HA 環境の場合は、次の手順を実行します。

1. VM をシャットダウンします。
2. VM のスナップショットを復元します。
3. VM を起動します。
4. Cisco EPN Manager を起動します。

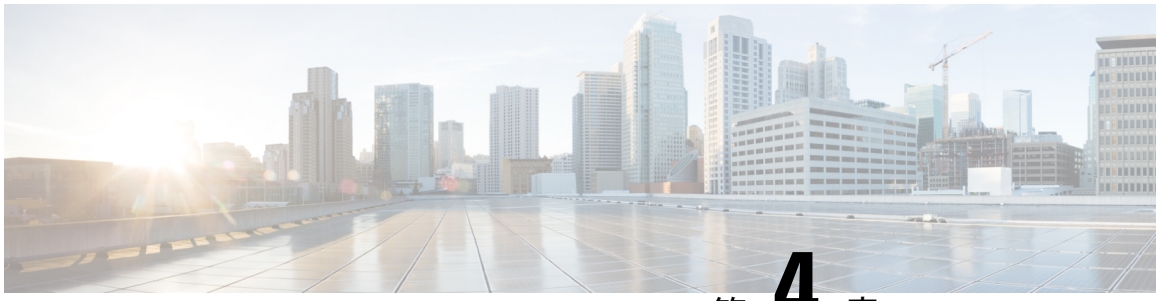
```
ncs start
```

HA 環境の場合は、次の手順を実行します。

1. プライマリとセカンダリの VM サーバーをシャットダウンします。
2. 両方のサーバーで VM のスナップショットを復元します。
3. プライマリとセカンダリの VM サーバーを起動します。
4. プライマリ サーバーとセカンダリ サーバーで Cisco EPN Manager を起動します。

```
ncs start
```

5. HA を設定し、プライマリ サーバーにセカンダリ サーバーを登録します。登録プロセスはプライマリ サーバーから実行する必要があります。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』のプライマリ サーバーへのセカンダリ サーバーの登録に関する項を参照してください。



第 4 章

オフラインで使用する Geo マップ リソース ファイルのインストール

ネットワークは、トポロジ マップまたは地理的マップ（Geo マップ）で視覚化できます。Geo マップを使用すると、ネットワーク デバイスを世界地図上に配置し、それらの地理的コンテキスト内でモニターすることができます。

Geoマップを GUI に表示するために、クライアントからの直接インターネット接続またはプロキシとして機能する EPN Manager サーバー経由で、マップ タイルを特定の Mapbox URL から取得するようにシステムがデフォルトで設定されています。インターネットに接続していない場合は、マップ リソースをローカルにインストールし、ローカル マップ リソースを使用するように指定する必要があります（オフライン使用など）。

次のトピックでは、HA 環境と非 HA 環境の両方で、オフラインで使用する Geo マップをダウンロードしてインストールする方法について説明します。

（注） Geoマップの圧縮ファイルは非常に大きいファイルです。ファイルをリモート リポジトリに保存することを推奨します。

Geo マップ リソース ファイルのインストール（標準展開）

標準環境（高可用性なし）でオフラインで使用する Geoマップ リソース ファイルをインストールするには、次の手順が必要です。

1. Cisco EPN Manager サーバーへの Geo マップ リソース ファイルの配置。

2. Cisco EPN Manager サーバーへの Geo マップ リソース ファイルのインストール 。
3. インストールしたマップ リソースを使用する Cisco EPN Manager サーバーの設定 。
4. Geo マップファイルが正常にインストールされたことを確認する。

Cisco EPN Manager サーバーへの Geo マップ リソース ファイルの配置

はじめる前に

- （Geo マップ ファイルが非常に大きいため）リモート リポジトリを使用する場合は、リモート リポジトリが設定されていることを確認してください。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』のリモート FTP バックアップ リポジトリの使用に関するトピックを参照してください。
- SCP がクライアントマシンで有効であり、必要なポートが開いていることを確認します。

この手順では、Cisco EPN Manager サーバー上のデフォルトのローカル リポジトリに Geo マップ リソースをダウンロードしてコピーする方法を示します。

ステップ 1 Geo マップの圧縮ファイルをクライアント マシンにダウンロードします。

1. cisco.com のソフトウェア ダウンロード サイトに移動します。
2. [すべてのリリース（All Releases）] > [7.1] を選択して、ファイルに移動します。
3. ダウンロードするマップを特定し、[ダウンロード（Download）] をクリックします。
4. クライアント マシンにファイルを保存する手順に従います。

ステップ 2 ローカルマシンから Cisco EPN Manager サーバーのデフォルト ローカル リポジトリ（/localdisk/defaultRepo）に Geo マップの圧縮ファイルをコピーします。

次の例では、ロシアの Geo マップ ファイルは、クライアント マシンの /temp ディレクトリにダウンロードされました。ユーザーは、Linux CLI 管理者ユーザーとして Cisco EPN Manager サーバーにログインし、クライアント マシンからファイルを取得し、サーバー上の /localdisk/defaultRepo にファイルをコピーしています。

```
scp joesmith@123.456.789.101:/temp/Russia_GeoMap_CEPNM_7_1_0-bundle.tar.gz/localdisk/defaultRepo
```

Cisco EPN Manager サーバーへの Geo マップ リソース ファイルのインストール

はじめる前に

インストール プロセスでは、Geo マップ ファイルが抽出され、/opt/CSCOlumos/resources/offline_geo にインストールされます。ストレージの制約を解消するには、Linux CLI 管理者ユーザーとしてログインした後で、/etc/fstab ファイルを編集して、追加のストレージをディレクトリにマウントすることを検討してください。高可用性があり、

追加のストレージをマウントする必要がある場合は、必ずプライマリ サーバーとセカンダリ サーバーの両方で /etc/fstab ファイルを編集してください。

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。

ステップ 2 /localdisk/defaultRepo にある Geo マップ リソース ファイルをインストールします。

例：

```
application install filename defaultRepo
```

filename は、/localdisk/defaultRepo にある Geo マップ リソース ファイルです（これは「Cisco EPN Manager サーバーへの Geo マップ リソース ファイルの配置」でコピーしたファイルです）。次に例を示します。

例：

```
application install Russia_GeoMap_CEPNM_7_1_0-bundle.tar.gz defaultRepo
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

マップ リソースのサイズに応じて、インストールには数分かかります。

インストールしたマップ リソースを使用する Cisco EPN Manager サーバーの設定

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択して、**[マップ（Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [Geo マップの有効化（Enable Geo Maps）] をオンにします。

ステップ 3 [マップ プロバイダー（Map Provider）] ドロップダウンリストから [インストール済みマップ リソース（Installed Map Resources）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

変更を適用するために Cisco EPN Manager サーバーを再起動する必要はありません。通知メッセージによって、システムがインストールされたマップ リソースを使用して動作するようになったことが通知されます。

Geo マップファイルが正常にインストールされたことを確認する

Geo マップファイルをインストールし、それらの Geo マップファイルを使用するようにシステムを設定した後、それらが正常にインストールされ、GUI に表示されていることを確認します。

マップが GUI に表示されていることを確認します。

1. Cisco EPN Manager Web GUI に管理者権限を持つユーザーとしてログインします。
2. 左側のサイドバーのメニューから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。
3. Geo マップを表示するトポロジ ウィンドウの右上にある [地理的マップ（Geographical Map）] アイコンをクリックします。
4. 目的のマップが表示されることを確認します。

Geo マップ リソース ファイルのインストール（高可用性展開）

高可用性環境では、プライマリ サーバーとセカンダリ サーバーの両方にオフライン マップ リソースをインストールする必要があります。

（注） プライマリ サーバーで Cisco EPN Manager の再インストールが必要となる障害がプライマリ サーバーで発生した場合は、プライマリ サーバーに Geo マップ リソースを再インストールしてサーバーを再起動する必要があります。

高可用性展開に Geo マップ ファイルをインストールするには、次のワークフローに従います。

ステップ 1 「Cisco EPN Manager サーバーへの Geo マップ リソース ファイルの配置」に説明されているように、プライマリ サーバーとセカンダリ サーバーに Geo マップ ファイルを配置します。

ステップ 2 「Cisco EPN Manager サーバーへの Geo マップ リソース ファイルのインストール」に記載されているように、Geo マップ ファイルをプライマリ サーバーにインストールします。

ステップ 3 「Cisco EPN Manager サーバーへの Geo マップ リソース ファイルのインストール」に記載されているように、Geo マップ ファイルをセカンダリ サーバーにインストールします。

ステップ 4 「インストールしたマップ リソースを使用する Cisco EPN Manager サーバーの設定」に記載されているように、インストールされたマップ ファイルを使用できるようにします。

ステップ 5 「Geo マップファイルが正常にインストールされたことを確認する」に記載されているように、プライマリ サーバーで Geo マップが表示されていることを確認します。

Cisco EPN Manager へのアップグレード後の Geo マップ リソース ファイルの更新

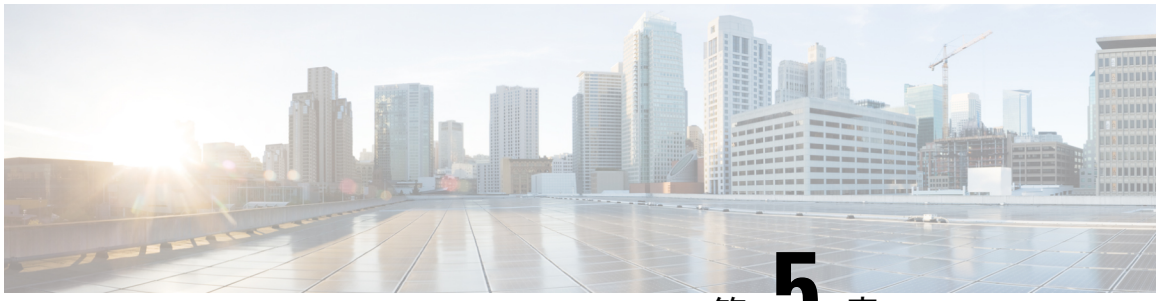
ジオ マップ ファイルは、アップグレード後に再インストールする必要があります。

ステップ 1 必要な Cisco EPN Manager Geo マップ ファイルをダウンロードし、再インストールします。

ステップ 2 サーバーを停止し、再起動します。

ステップ 3 キャッシュをクリアします。

ステップ 4 Geo マップ ファイルがインストールされていることを確認します。「Geo マップファイルが正常にインストールされたことを確認する」を参照してください。



第 5 章

インストール関連の補足情報と手順

Cisco EPN Manager Web GUI へのログイン

次の手順に従って、Cisco EPN Manager Web GUI にログインします。

ステップ 1 クライアントマシンで、サポートされているブラウザのいずれかを起動します。

ステップ 2 ブラウザのアドレス行に **https://*serverIP*** と入力します。ここで、*serverIP* はインストールした Cisco EPN Manager 上のサーバーの IP アドレスです。ログインウィンドウが表示されます。

クライアントが Cisco EPN Manager Web GUI に初めてアクセスした場合は、サイトが信頼されていないという警告がブラウザに表示されることがあります。この場合は、指示に従ってセキュリティ例外を追加し、Cisco EPN Manager サーバーから自己署名証明書をダウンロードします。この手順の完了後に、ブラウザは将来のすべてのログイン試行で Cisco EPN Manager を信頼できるサイトとして受け入れます。

ステップ 3 インストール中に指定した Web GUI ルートのユーザー名とパスワードを入力します。

ライセンスの問題が発生した場合は、アラート ボックスにメッセージが表示されます。評価ライセンスがある場合は、ライセンスの有効期限までの日数が表示されます。ライセンスの期限が切れているというアラートが表示されます（この問題に対処するには、**[管理（Administration）]** > **[ライセンスとソフトウェアの更新（Licenses and Software Updates）]** > **[ライセンス（Licenses）]** ページに直接移動するオプションもあります）。ライセンスの詳細については、『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。

ステップ 4 [ログイン（Login）] をクリックし、Cisco EPN Manager Web GUI にログインします。ホーム ページが表示され、Web GUI を使用できるようになりました。ダッシュボードとダッシュレットについては、『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。

ステップ 5 セキュリティを強化するため、次の手順を実行します。

1. **[管理（Administration）]** > **[ユーザー（Users）]** > **[ロールと AAA（Roles & AAA）]** > **[パスワードの変更（Change Password）]** を選択し、Web GUI ルート ユーザーのパスワードを変更します。

2. 管理者権限またはスーパーユーザー権限を持つ Cisco EPN Manager Web GUI ユーザーを少なくとも 1 人作成し、Web GUI ルート ユーザーを無効にします。このユーザーの無効化については、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のユーザー管理に関するトピックを参照してください。
3. まだ実行していない場合は、Linux CLI ユーザーを無効にします。『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』を参照してください。

次のタスク

サーバー、ユーザー、障害、および Web GUI 管理のセットアップ タスクを実行します。タスクの詳細なリストについては、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』の管理に関する頁の冒頭を参照してください。

Cisco EPN Manager ユーザー インターフェイスとユーザー タイプについては、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』を参照してください。

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。