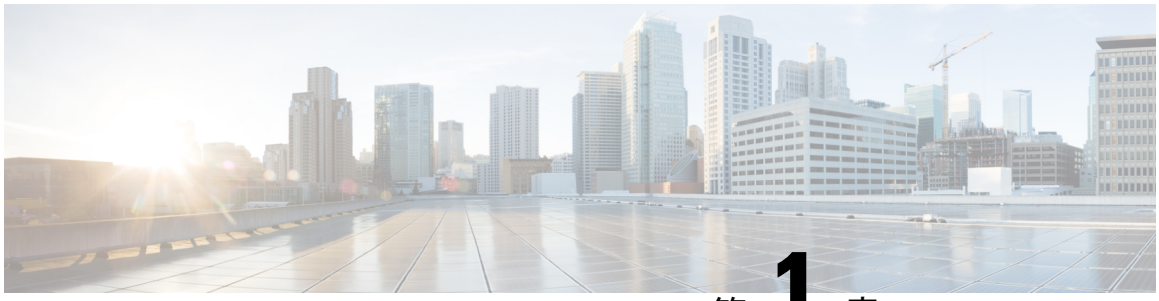
Cisco Evolved Programmable Network Manager 5.1 インストールガイド

初版：2021 年 4 月 29 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 EPN Manager 5.1 のインストール

この章では、Cisco EPN Manager 5.1 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 5.1 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 5.1 高可用性インストール （15 ページ）を参照してください。

インストールの概要

Cisco EPN Manager 5.1 は、次の手順に従って新規インストールとしてインストールできます。

1. Cisco EPN Manager 5.0 は、仮想マシンまたはベアメタルサーバーのいずれかにインストールします。

   『Cisco Evolved Programmable Network Manager 5.0 インストール ガイド』を参照できます。

2. このガイドの手順の説明に従って、Cisco EPN Manager 5.1 UBF をインストールします。

次のトピックでは、標準展開および高可用性展開で Cisco EPN Manager 5.1 UBF をインストールするための情報と手順について説明します。

Note ベアメタルサーバーでのインストール手順を開始する前に、『Installation Guide for Cisco Evolved Programmable Network Manager 5.0』の「Installation Options」セクションに記載されている手順を実行していることを確認してください。

Note インストール手順を開始する前に、インストールに関する重要な情報や問題についてリリースノートを確認してください。

Cisco EPN Manager 5.1 の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 5.1 への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 5.1.0 へのインストールパス
Cisco EPN Manager 3.1.3	**Cisco EPN Manager 3.1.3 > 5.1.0**
Cisco EPN Manager 4.1.1	**Cisco EPN Manager 4.1.1 > 5.0.0 > 5.0.1 > 5.1.0**
Cisco EPN Manager 5.0.0 Cisco EPN Manager 5.0.1	**Cisco EPN Manager 5.0.0 > 5.0.1 > 5.1.0**
Cisco EPN Manager 5.0.2	**Cisco EPN Manager 5.0.2 > 5.1.0**

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 5.1 のインストールの前提条件

Note Cisco EPN Manager 5.1 のインストールは、Cisco EPN Manager 5.0 OVA/ISO のインストールと、それに続く Cisco EPN Manager 5.1 UBF のインストールで構成されます。

Cisco EPN Manager 5.1 をインストールする前に、次のタスクを実行する必要があります。

- Cisco EPN Manager 5.0 が仮想マシンまたはベアメタルサーバーのいずれかにインストールされていることを確認します。

『Cisco Evolved Programmable Network Manager 5.0 インストール ガイド』を参照できます。

• ライセンシング, on page 3
• 自動クライアント ログアウトの無効化

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。

ライセンスのコピーは作成しないでください。

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。

自動クライアント ログアウトの無効化

一定期間クライアントがアクティブでない場合、自動的にログアウトされることがあります。インストール中にログアウトしないようにするには、次のように、システム設定でアイドル ユーザーの自動ログアウトを無効にすることを推奨します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定 (System Settings)] > [サーバー（Server）]** の順に移動します。

ステップ 2 [グローバルアイドルタイムアウト（Global Idle Timeout）] セクションで、[アイドル状態のユーザーをすべてログアウト（Logout all idle users）] チェックボックスをオフにします。

ステップ 3 システム設定への変更を保存するように促すメッセージが表示されたら、[OK] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 Web GUI ウィンドウの右上にある歯車のアイコンをクリックし、[マイ設定（My Preferences）] をクリックします。[ユーザー アイドル タイムアウト（User Idle Timeout）] で、[アイドル ユーザーをログアウトする（Logout idle user）] チェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 Cisco EPN Manager からログアウトして、ログインし直します。

標準環境（非 HA）での Cisco EPN Manager 5.1 のインストール

標準環境（非高可用性）で Cisco EPN Manager 5.1 をインストールするには、次の手順に従います。

1. 「Cisco EPN Manager 5.1 のインストールの前提条件」のタスクを実行していることを確認します。
2. サーバーへの Cisco EPN Manager 5.1 インストールファイルの配置。
3. Cisco EPN Manager 5.1 のインストール（非 HA）。
4. すべてのデバイスのインベントリ収集を実行して、データベースと同期させます。「すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）」を参照してください。

外部の認証および承認を使用している場合は、インストール後に、最新のアップデートを取得するために、ユーザー タスク情報を AAA サーバーにエクスポート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』を参照してください。

サーバーへの Cisco EPN Manager 5.1 インストールファイルの配置

この手順では、ubf インストールファイルをローカルマシンにダウンロードし、ローカルマシンから Cisco EPN Manager サーバーにアップロードする方法を説明します。

Note インストールファイルをダウンロードするには、Cisco.com のアカウントが必要です。

ステップ 1 「Cisco EPN Manager 5.1 のインストールの前提条件」のタスクを実行していることを確認します。

ステップ 2 必要な ubf ファイルをローカル マシンにダウンロードします。

a. Cisco.com のソフトウェア ダウンロード サイトに移動します。

b. Cisco EPN Manager マイナーリリースファイル（cepn5.1-buildXXX.ubf 形式）を見つけます。

c. ローカル マシンにファイルをダウンロードします。

ステップ 3 ファイルがローカルサーバーにダウンロードされたら、チェックサム（MD5）と Cisco.com で入手可能なチェックサムを比較します。

ステップ 4 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。

ステップ 5 ローカルマシンから Cisco EPN Manager サーバーに ubf ファイルをアップロードします。

a. 左側のサイドバーメニューから、[管理（Administration）] > [ソフトウェア アップデート（Software Updates）] を選択します。

b. ページ上部の青色の [アップロード（Upload）] リンクをクリックします。

。

c. [アップデートのアップロード（Upload Update）] ダイアログボックスで、[参照（Browse）] をクリックして、ダウンロードしたファイルに移動します。

d. [OK] をクリックしてファイルをサーバーにアップロードします。

Cisco EPN Manager 5.1 が正常にアップロードされると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

Cisco EPN Manager 5.1 のインストール（非 HA）

標準環境（非高可用性）に Cisco EPN Manager 5.1 をインストールするには、次の手順に従います。

ステップ 1 左側のサイドバーから、**[管理（Administration）]** > **[ソフトウェアアップデート（Software Update）]** を選択します。

ステップ 2 [ソフトウェアアップデート（Software Update）] ページの EPN Manager 5.1 に関連付けられている [インストール（Install）] ボタンをクリックします。

ステップ 3 インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい（Yes）] をクリックします。

Note インストールが完了すると、サーバーが再起動します。

ステップ 4 既存のファイルを上書きするかどうかを確認するメッセージが表示された場合は、[はい（Yes）] をクリックします。

インストールが成功すると、ステータスが [インストール済み（Installed）] に変わります。Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります。

ステップ 5 Cisco EPN Manager サービスのステータスを確認します。

a. 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。

b. ncs status コマンドを実行して、少なくともヘルスモニター、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 Cisco EPN Manager の Web GUI にアクセスできる場合は、ログインして、[ソフトウェア アップデート（Software Updates）] ページで Cisco EPN Manager マイナーリリースのステータスが [インストール済み（Installed）] になっていることを確認します。

a. 左側のサイドバーから、**[管理（Administration）] > [ソフトウェアアップデート（Software Update）]** を選択します。

b. [Cisco EPN Managerマイナーリリース（Cisco EPN Manager Minor Release）] が [アップデート（Updates）] タブの下に [インストール済み（Installed）] として表示されていることを確認します。また、ubf ファイル（cepnm5.1-buildXXX.ubf の形式）が [ファイル（Files）] タブに表示されていて、[使用中（In Use）] ステータスが [はい（Yes）] になっていることを確認します。

What to do next

Note Cisco EPN Manager マイナーリリースをインストールすると Cisco EPN Manager が再起動されるため、同期クロック操作でのサービスの再起動は無視できます。

すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）

以前のバージョンの Cisco EPN Manager をすでに使用している場合（つまり、新規インストールではない場合）、デバイスで同期操作を実行する必要があります。同期操作では、デバイスの物理インベントリと論理インベントリを収集し、その情報をデータベースに保存するように Cisco EPN Manager に指示します。

ステップ 1 **[モニター（Monitor）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 すべてのデバイスを選択し、[同期（Sync）] をクリックします。

高可用性展開での Cisco EPN Manager 5.1 のインストール

HA 環境で Cisco EPN Manager 5.1 をインストールするには、次の手順に従います。

1. 一般インストールおよび HA インストールの前提条件タスクの実行。
2. HA 設定の削除。

3. サーバーへの Cisco EPN Manager 5.1 インストールファイルの配置（HA 展開）。
4. プライマリサーバーとセカンダリサーバーへの Cisco EPN Manager 5.1 のインストール（HA 展開）。
5. すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）。

Note 外部の認証および承認を使用している場合は、インストール後に、最新のアップデートを取得するために、ユーザー タスク情報を AAA サーバーにエクスポートする必要があります。

一般インストールおよび HA インストールの前提条件タスクの実行

HA のインストールを開始する前に、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の両方で「Cisco EPN Manager 5.1 のインストールの前提条件」のタスクを実行します。

HA 設定の削除

Note このプロセスは、サーバーが HA 設定に関連付けられている場合にのみ必要です。

ステップ 1 「Cisco EPN Manager 5.1 のインストールの前提条件」のタスクを実行していることを確認します。

ステップ 2 プライマリサーバーの 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。

ステップ 3 左側のサイドバーから、**[管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）]**の順に選択します。

ステップ 4 左側の [HA 設定（HA Configuration）] をクリックします。

ステップ 5 [削除（Remove）] をクリックします。

ステップ 6 削除操作が完了したら、[設定モード（Configuration Mode）] フィールドに [HA が設定されていません（HA Not Configured）] と表示されていることを確認します。

サーバーへの Cisco EPN Manager 5.1 インストールファイルの配置（HA 展開）

はじめる前に

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。セカンダリ サーバーにパッチをインストールするときに必要です。

ステップ 1 「HA 設定の削除」の説明に従い、HA 設定を削除していることを確認します。

ステップ 2 プライマリサーバーで、Cisco EPN Manager 5.1 ubf ファイルをアップロードします。「サーバーへの Cisco EPN Manager 5.1 インストールファイルの配置」の手順に従います。

ステップ 3 Cisco EPN Manager 5.1 ubf ファイルをセカンダリサーバーにアップロードします。（プライマリ サーバーにアップロードされてインストールされたものと同じファイルを使用します。）

a. ブラウザに次の URL を入力することにより、セカンダリ サーバーの HM Web ページにログインします。

`https://`*`serverIP`***`:8082`**

ここで、*serverIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

a. 認証キーを入力して、[ログイン（Login）] をクリックします。
b. [ヘルス モニター（Health Monitor）] ウィンドウの右上にある [ソフトウェア アップデート（Software Update）] をクリックして、[セカンダリ サーバーのソフトウェア アップデート（Secondary Server Software Update）] ウィンドウを開きます。
c. 認証キーを入力して、[ログイン（Login）] をクリックします。
d. ウィンドウ タイトルの下にある [アップロード（Upload）] リンクをクリックし、ubf ファイルを参照して、[OK] をクリックします。

ubf ファイルのアップロードが成功すると、[ファイル（Files）] タブの下にファイルが表示されます。

What to do next

プライマリサーバーとセカンダリサーバーへの Cisco EPN Manager 5.1 のインストール（HA 展開）。

プライマリサーバーとセカンダリサーバーへの Cisco EPN Manager 5.1 のインストール（HA 展開）

はじめる前に

- 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 マイナーリリースファイルをインストールするために必要になります。
- 進行中のバックアップがないことを確認します。

これにより、フェールオーバー後にコンプライアンス サーバーがセカンダリ サーバー上で起動して稼働するようになります。

ステップ 1 「Cisco EPN Manager 5.1 のインストール（非 HA）」の説明に従い、Cisco EPN Manager 5.1 をプライマリサーバーにインストールし、インストールの内容を確認します。インストール後に、プライマリ サーバーが自動的に再起動し、Web GUI にしばらくアクセスできません。

ステップ 2 プライマリサーバーとセカンダリサーバーの両方でハードウェアクロックと NTP クロックを同期し、各サーバーのクロックが相互に同期されていることを確認します。

Note Cisco EPN Manager マイナーリリースをインストールすると Cisco EPN Manager が再起動されるため、同期クロック操作でのサービスの再起動は無視できます。

ステップ 3 セカンダリサーバーに Cisco EPN Manager 5.1 をインストールします。

a. ブラウザに URL（https://serverIP:8082）を入力して、セカンダリサーバーの HM Web ページにログインします。

ここで、*serverIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

b. 認証キーを入力して、[ログイン（Login）] をクリックします。

c. [ヘルス モニター（Health Monitor）] ウィンドウの右上にある [ソフトウェア アップデート（Software Update）] をクリックして、[セカンダリ サーバーのソフトウェア アップデート（Secondary Server Software Update）] ウィンドウを開きます。

d. 認証キーを入力して、[ログイン（Login）] をクリックします。

e. [ソフトウェア アップデート（Software Updates）] ページの Cisco EPN Manager マイナーリリースに関連付けられている [インストール（Install）] ボタンをクリックします。

f. インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい（Yes）] をクリックします。正常にインストールされると、ステータスが [インストール済み（Installed）] に変わり、セカンダリ サーバーが自動的に再起動します。

ステップ 4 セカンダリ サーバーが再起動した後、セカンダリ サーバーでインストールを確認します。

a. セカンダリサーバーで SSH セッションを開始して、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。

b. ncs status コマンドを実行して、少なくともヘルスモニター、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。

c. Web GUI にアクセスできたら、セカンダリ サーバーの [HM Web] ページでインストールとバージョンを確認します。ブラウザに次の URL を入力します。https://serverIP:8082

ここで、**`serverIP`** はセカンダリ サーバーの IP アドレスまたはホスト名です。

d. 認証キーを入力して、[ログイン（Login）] をクリックします。

e. [ヘルス モニター（Health Monitor）] ウィンドウの右上にある [ソフトウェア アップデート（Software Update）] をクリックして、[セカンダリ サーバーのソフトウェア アップデート（Secondary Server Software Update）] ウィンドウを開きます。

f. 認証キーを入力して、[ログイン（Login）] をクリックします。

g. [ファイル（Files）] タブで、Cisco EPN Manager マイナーリリースファイル（cepnm5.1-buildXXX.ubf 形式）が表示されていて、[使用中（In Use）] ステータスが [はい（Yes）] になっていることを確認します。

ステップ 5 次のコマンドを実行して、すべてのサービスが起動していて実行されていることを確認します。

```
ncs status
```

ステップ 6 プライマリ サーバーで、高可用性を有効にし、プライマリ サーバーの HA のステータスが [プライマリ アクティブ（Primary Active）] であることを確認します。

a. 高可用性を有効にします。

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. 左側のサイドバーメニューから、[管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] の順に選択します。
3. 左側の [HA 設定（HA Configuration）] をクリックして、セカンダリサーバーの IP アドレス、セカンダリサーバーの認証キー、および Cisco EPN Manager が HA のステータス変更通知を送信する電子メールアドレスを入力します。
4. HA セットアップで仮想 IP アドレッシングを使用している場合（プライマリ サーバーとセカンダリ サーバーが同じサブネットにある場合）は、[仮想 IP の有効化（Enable Virtual IP）] チェックボックスをオンにして、仮想 IP アドレスを入力します。
5. 「HA 設定の準備状況の確認」で説明されているプロセスに従って、HA の準備状況を確認します。
6. [保存（Save）] をクリックして、サーバーが同期されるまで待ちます。
7. 設定モードが [HA 対応（HA Enabled）] になっていることを確認します。

b. プライマリ サーバーの HA ステータスを確認します。

1. 左側の [HA ステータス（HA Status）] をクリックします。
2. [現在のステータス モード（Current State Mode）] に [プライマリ アクティブ（Primary Active）] と表示されていることを確認します。

ステップ 7 セカンダリ サーバーの HA ステータスが [セカンダリ同期中（Secondary Syncing）] になっていることを確認します。

a. ブラウザに URL（https://serverIP:8082）を入力して、セカンダリサーバーの HM Web ページにログインします。

ここで、**serverIP** はセカンダリ サーバーの IP アドレスまたはホスト名です。

b. 認証キーを入力して、[ログイン（Login）] をクリックします。

c. [現在のステータス モード（Current State Mode）] が [セカンダリ同期中（Secondary Syncing）]（緑色のチェックマーク付き）になっていることを確認します。

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 設定が決定されます。

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。

プライマリ認証キーとセカンダリ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）] フィールドの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。

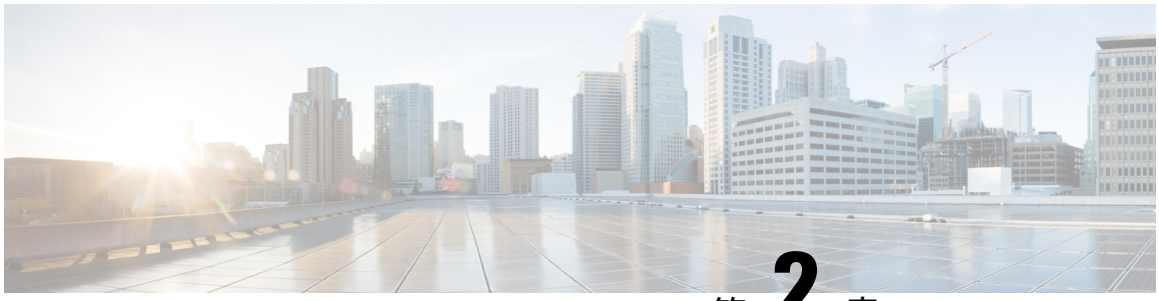
表 *1* : チェックリストの名前と説明

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 サーバーの両方の 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 サーバーの両方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 サーバーの両方の 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 サーバーの両方のディスク 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 サーバーの両方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 サーバーの両方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 サーバーの両方でデータベース 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 サーバーの両方で 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 2 章

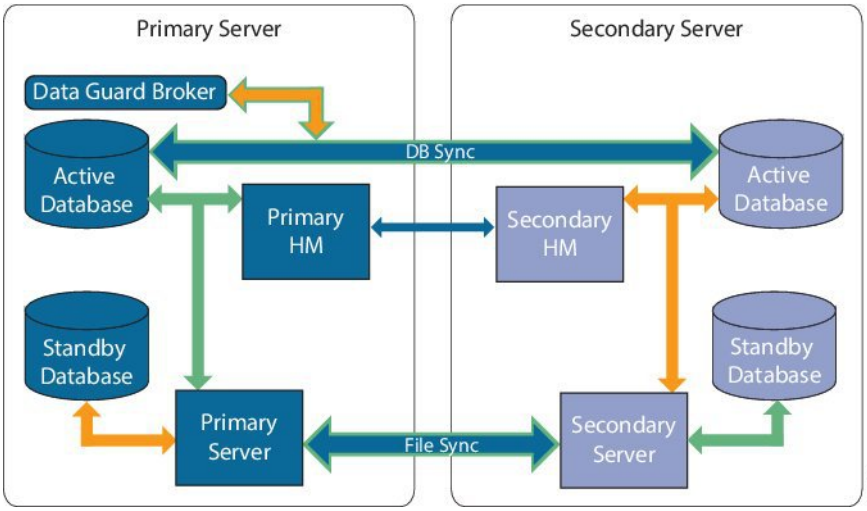
Cisco EPN Manager 5.1 高可用性インストール

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。

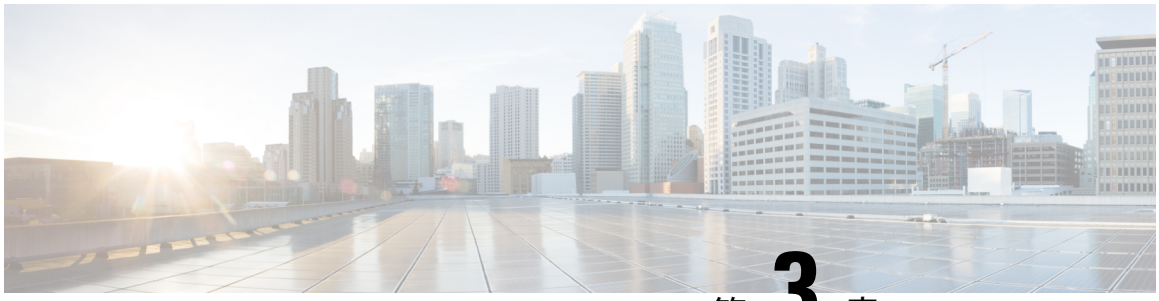
- 仮想 IP アドレス
- プライマリ サーバーおよびセカンダリ サーバーの IP アドレス
- プライマリ サーバーとセカンダリ サーバーに設定されているゲートウェイの IP アドレス

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。



第 3 章

Cisco EPN Manager 5.1 へのアップグレード

以下の有効なアップグレード パス （19 ページ）のいずれかに従って、Cisco EPN Manager 5.1 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 5.1 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 5.1 のインストール、さらに、新しい Cisco EPN Manager 5.1 サーバーへバックアップされたデータの復元が含まれます。

（注） Cisco EPN Manager 5.1 のインストールは、Cisco EPN Manager 5.0 OVA/ISO のインストールと、それに続く Cisco EPN Manager 5.1 UBF のインストールで構成されます。

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 6.0 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 6.0 へのインストールパス
Cisco EPN Manager 5.1.3	**Cisco EPN Manager 5.1.3 > 6.0**

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 6.0 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 6.0 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 6.0 へのアップグレード（高可用性）, on page 20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 6.0 のインストール、さらに、新しい Cisco EPN Manager 6.0 サーバーへ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。

Cisco EPN Manager 6.0 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 6.0 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）

Note 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 4.1 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。

a. 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。

b. [管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] を選択します。

c. 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。

d. 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。

e. 削除操作が完了するまで待ちます。

f. 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。

Note 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。

Note 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：

a. サーバーが再起動していることを確認します。

b. **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 プライマリ サーバーの **ncs status** 出力に **Compliance engine is stopped** が表示される場合は、次の操作を行います。

a. Cisco EPN Manager を停止します。

```
ncs stop
```

b. Linux CLI ルート ユーザーとしてログインします。

c. ソフト リンクを使用してタイム ゾーンを更新します（次のコマンドは 1 行です）。

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " "  -f
3) /etc/localtime
```

ステップ 7 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。

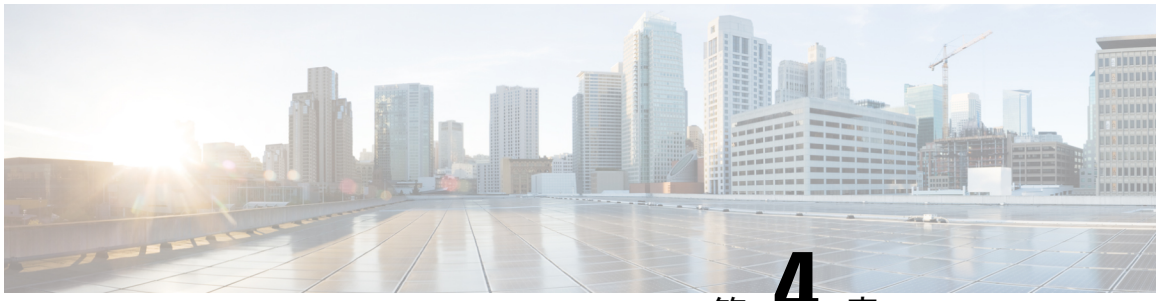
ステップ 8 プライマリ サーバーにセカンダリ サーバーを登録して HA を再設定します。ステップ 1 で保存した情報を使用します。登録プロセスはプライマリ サーバーから実行する必要があります。詳細については、『Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド』のプライマリ サーバーへのセカンダリ サーバーの登録に関する項を参照してください。

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。

新しいダッシュボード タブが自動的に追加されます。



第 4 章

インストール関連の補足情報と手順

復旧モードでの起動

ステップ 1 Cisco EPN Manager 5.0 から起動します。

ステップ 2 インストールメニューで、[Cisco EPNM System復旧モード（Cisco EPNM System Rescue Mode）] を選択します。

ステップ 3 復旧対象のターゲットシステムのディスクのマウントについてのプロンプトが表示されたら、20 秒待ち、オプション 1 [続行（Continue）] を選択します。これにより、/mnt/sysimage の下にシステムがマウントされます。シェルを取得するように促されたら、**Enter** キーを押します。このシェルは、/mnt/sysimage の下にターゲットシステムがマウントされた状態で、インストール/回復環境内に存在します。このシェルには、すべての共通ファイルシステム、ディスク、LVM、ネットワークツールなど、システムの復旧に使用できる多数のツールがあります。ターゲットシステムのさまざまな bin ディレクトリが、デフォルトの実行可能検索パス（${PATH}）に追加されます。

ステップ 4 chroot /mnt/sysimage の実行による /mnt/sysimage ディレクトリへの chroot

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。

手順

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。

a. **[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。

b. 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。

c. 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。

What to do next

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。

サポートされるタイム ゾーン

この表に、システムのタイム ゾーンで利用可能な値を示します。

Africa/Abidjan	America/St_Johns	Europe/Amsterdam
Africa/Accra	America/St_Kitts	Europe/Belgrade

Africa/Addis_Ababa	America/St_Lucia	America/Los_Angeles
Africa/Algiers	America/St_Thomas	Europe/Bratislava
Africa/Asmara	America/St_Vincent	Europe/Brussels
Africa/Bamako	America/Swift_Current	Europe/Bucharest
America/Tegucigalpa	America/Thunder_Bay	Europe/Budapest
Africa/Bangui	America/Tijuana	Europe/Chisinau
Africa/Banjul	America/Toronto	Europe/Copenhagen
Africa/Bissau	America/Vancouver	Europe/Dublin
Africa/Blantyre	America/Whitehorse	Europe/Gibraltar
America/Tortola	America/Winnipeg	Europe/Helsinki
Africa/Bujumbura	America/Yakutat	Europe/Isle_of_Man
Africa/Cairo	America/Yellowknife	Europe/Istanbul
Africa/Casablanca	Antarctica/Casey	Europe/Jersey
Africa/Ceuta	Antarctica/Davis	Europe/Kaliningrad
Africa/Conakry	Antarctica/DumontDUrville	Indian/Chagos
Africa/Dakar	Antarctica/Mawson	Indian/Christmas
Africa/Dar_es_Salaam	Antarctica/McMurdo	Indian/Comoro
Africa/Djibouti	Antarctica/Palmer	Asia/Jakarta
Africa/Douala	Antarctica/Rothera	Indian/Kerguelen
Africa/El_Aaiun	Antarctica/Syowa	Indian/Mahe
Africa/Freetown	Antarctica/Vostok	Indian/Maldives
Africa/Gaborone	rctic/Longyearbyen	Indian/Mauritius
Africa/Harare	Asia/Aden	Indian/Mayotte
Africa/Johannesburg	Asia/Almaty	Indian/Reunion
Africa/Kampala	Asia/Amman	New_Salem
Africa/Khartoum	Asia/Anadyr	Pacific/Apia
Africa/Kigali	Asia/Aqtau	Pacific/Auckland
Africa/Kinshasa	Asia/Aqtobe	Pacific/Chatham
Africa/Lagos	Asia/Ashgabat	Pacific/Easter

Africa/Libreville	Asia/Baghdad	Pacific/Efate
Africa/Lome	Asia/Bahrain	Pacific/Enderbury
Africa/Luanda	Asia/Baku	Pacific/Fakaofo
Africa/Lubumbashi	Asia/Bangkok	Pacific/Fiji
Africa/Lusaka	Asia/Beirut	Pacific/Funafuti
Africa/Malabo	Asia/Bishkek	Pacific/Galapagos
Africa/Maputo	Asia/Brunei	Pacific/Gambier
Africa/Maseru	Asia/Calcutta	Pacific/Guadalcanal
Africa/Mbabane	Asia/Choibalsan	Pacific/Guam
Africa/Mogadishu	Asia/Colombo	Pacific/Honolulu
Africa/Monrovia	Asia/Damascus	Pacific/Kiritimati
Africa/Nairobi	Asia/Dhaka	Pacific/Kosrae
Africa/Ndjamena	Asia/Dili	Pacific/Kwajalein
Africa/Niamey	Asia/Dubai	Pacific/Majuro
Africa/Nouakchott	Asia/Dushanbe	Pacific/Marquesas
Africa/Ouagadougou	Asia/Gaza	Pacific/Midway
Africa/Porto-Novo	Asia/Colombo	Pacific/Nauru
Africa/Sao_Tome	Asia/Ho_Chi_Minh	Pacific/Niue
Africa/Tripoli	Asia/Hong_Kong	Pacific/Norfolk
Africa/Tunis	Asia/Hovd	Pacific/Noumea
Africa/Windhoek	Asia/Irkutsk	Pacific/Pago_Pago
America/Adak	Asia/Jakarta	Pacific/Palau
America/Anchorage	Asia/Jayapura	Pacific/Pitcairn
America/Anguilla	Asia/Jerusalem	Pacific/Port_Moresby
America/Antigua	Asia/Kabul	Pacific/Rarotong
America/Araguaina	Asia/Kamchatka	Pacific/Saipan
America/Argentina/	Asia/Karachi	Pacific/Tarawa
America/Argentina/	Asia/Kathmandu	Pacific/Tongatapu
America/Argentina/Catamarca	Asia/Kolkata	Pacific/Wake

America/Argentina/Cordoba	Asia/Krasnoyarsk	Pacific/Wallis
America/Argentina/Jujuy	Asia/Kuala_Lumpur	UTC
America/Argentina/La_Rioja	Europe/Vaduz	New_Salem
America/Argentina/Mendoza	Asia/Kuwait	Mideast/Riyadh87
America/Argentina/Rio_Gallegos	Asia/Macau	Mideast/Riyadh88
America/Argentina/Salta	Asia/Magadan	Mideast/Riyadh89
America/Argentina/San_Juan	Asia/Makassar	America/Moncton
America/Argentina/San_Luis	Asia/Manila	America/Monterrey
America/Argentina/Tucuman	Asia/Muscat	America/Montevideo
America/Argentina/Ushuaia	Asia/Nicosia	Pacific/Tahiti
America/Aruba	Factory	America/Montserrat
America/Asuncion	Asia/Omsk	America/Nassau
America/Atikokan	Asia/Oral	America/New_York
Asia/Kuching	Asia/Phnom_Penh	America/Nipigon
America/Bahia	Asia/Pontianak	America/Nome
America/Barbados	Asia/Macau	America/Noronha
America/Belem	Asia/Magadan	America/North_Dakota/
America/Belize	Asia/Makassar	America/North_Dakota/Center
America/Blanc-Sablon	Asia/Manila	America/Panama
America/Boa_Vista	Asia/Qatar	America/Pangnirtung
America/Bogota	Asia/Qyzylorda	America/Paramaribo
America/Boise	Asia/Riyadh	America/Phoenix
Asia/Novosibirsk	Indian/Antananarivo	America/Port_of_Spain
America/Cambridge_Bay	Asia/Riyadh89	America/Port-au-Prince
America/Campo_Grande	Indian/Cocos	America/Porto_Velho
America/Cancun	Asia/Samarkand	America/Puerto_Rico
America/Caracas	Asia/Seoul	America/Rainy_River
Asia/Pyongyang	Asia/Shanghai	
America/Cayenne	Asia/Singapore	America/Moncton

America/Cayman	Asia/Taipei	Asia/Kabul
America/Chicago	Asia/Tashkent	Buenos_Aires
America/Chihuahua	Asia/Tbilisi	Canada/East-Saskatchewan
Asia/Riyadh87	Asia/Tehran	ComodRivadavia
Asia/Riyadh88	Asia/Samarkand	
America/Costa_Rica	Asia/Thimphu	America/Regina
America/Cuiaba	Asia/Tokyo	America/Resolute
Asia/Sakhalin	Asia/Ulaanbaatar	America/Rio_Branco
America/Danmarkshavn	Asia/Urumqi	America/Santarem
America/Dawson	Asia/Vientiane	America/Santiago
America/Dawson_Creek	Asia/Vladivostok	America/Santo_Domingo
America/Denver	Asia/Yakutsk	America/Sao_Paulo
America/Detroit	Asia/Yekaterinburg	America/Scoresbysund
America/Dominica	Asia/Yerevan	America/St_Barthelemy
America/Edmonton	Atlantic/Azores	Asia/Kabul
America/Eirunepe	Atlantic/Bermuda	Buenos_Aires
America/El_Salvador	Atlantic/Canary	Canada/East-Saskatchewan
America/Maceio	Atlantic/Cape_Verde	ComodRivadavia
America/Managua	Asia/Urumqi	America/Recife
America/Fortaleza	Asia/Vientiane	America/Regina
America/Glace_Bay	Asia/Vladivostok	America/Resolute
Asia/Jerusalem	Atlantic/Faroe	America/Rio_Branco
America/Goose_Bay	Atlantic/Madeira	America/Santarem
America/Grand_Turk	Atlantic/Reykjavik	America/Santiago
America/Grenada	Atlantic/South_Georgia	America/Santo_Domingo
America/Guadeloupe	Atlantic/St_Helena	America/Sao_Paulo
America/Guatemala	Atlantic/Stanley	America/Scoresbysund
America/Guayaquil	Atlantic/Madeira	America/St_Barthelemy
America/Guyana	Atlantic/Reykjavik	America/Kentucky/Louisville

America/Halifax	Atlantic/South_Georgia	America/Kentucky/Monticello
America/Havana	Australia/Adelaide	America/La_Paz
America/Hermosillo	Australia/Brisbane	America/Lima
America/Indiana/Indianapolis	Australia/Broken_Hill	America/Los_Angeles
America/Indiana/Knox	Australia/Currie	America/Maceio
America/Indiana/Marengo	Australia/Darwin	America/Managua
America/Indiana/Petersburg	Australia/Eucla	America/Manaus
America/Indiana/Tell_City	Australia/Hobart	America/Marigot
America/Indiana/Vevay	Australia/Currie	America/Martinique
America/Indiana/Vincennes	Australia/Lindeman	America/Mazatlan
America/Indiana/Winamac	Australia/Lord_Howe	America/Menominee
America/Manaus	Australia/Melbourne	America/Merida
America/Inuvik	Australia/Perth	America/Mexico_City
America/Iqaluit	Australia/Sydney	America/Miquelon
America/Jamaica	Asia/Jakarta	America/Kentucky/Louisville
America/Marigot	Asia/Jerusalem	America/Kentucky/Monticello
America/Juneau	Asia/Kabul	America/La_Paz
America/Lima	Asia/Kamchatka	Asia/Karachi