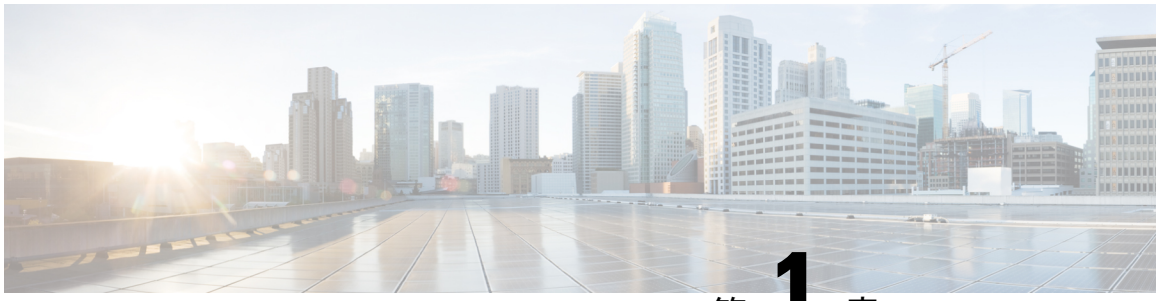
Cisco Evolved Programmable Network Manager 4.1 インストールガイド

初版：2020 年 7 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。

目 次



第 1 章

Cisco EPN Manager 4.1 のインストール

この章では、Cisco EPN Manager 4.1 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 4.1 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 4.1 の高可用性 （13 ページ）を参照してください。

設置の概要

Cisco EPN Manager 4.1 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 4.0 は、仮想マシンまたはベアメタルサーバのいずれかにインストールします。

   Cisco EPN Manager 4.0 インストールガイド [英語] を参照してください。

2. このガイドの手順の説明に従って、Cisco EPN Manager 4.1 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 4.1 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。

（注） 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 4.1 のインストールパス

次の表に、以前のバージョンから Cisco EPN Manager 3.1 へのインストール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 4.1 へのインストールパス
Cisco EPN Manager 4.0	**Cisco EPN Manager 4.0 > 4.1**
Cisco EPN Manager 4.0.1	**Cisco EPN Manager 4.0.1 > 4.1**
Cisco EPN Manager 4.0.2	**Cisco EPN Manager 4.0.2 > 4.1**

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 4.1 のインストールの前提条件

（注） Cisco EPN Manager 4.1 のインストールは、Cisco EPN Manager 4.0 OVA/ISO のインストールと、それに続く Cisco EPN Manager 4.1 UBF のインストールで構成されます。

Cisco EPN Manager 4.1 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 4.0 を仮想マシンまたはベアメタルサーバのいずれかにインストールしていることを確認します。

  Cisco EPN Manager 4.0 インストールガイド [英語] を参照してください。

- ライセンス （3 ページ）
- 自動クライアント ログアウトの無効化

ライセンス

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 User and Administrator Guide』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 **[Administration]** > **[Settings]** > **[System Settings]** > **[Server]** の順に移動します。

ステップ 2 [Global Idle Timeout] セクションで、[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 [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、[My Preferences] をクリックします。[ユーザ アイドル タイムアウト（User Idle Timeout）] で、[アイドル ユーザをログアウトする（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 4.1 のインストール

標準環境（非高可用性）で Cisco EPN Manager 4.1 をインストールするには、次の手順に従います。

1. 「Cisco EPN Manager 4.1 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. サーバへの Cisco EPN Manager 4.1 インストールファイルの配置。
3. Cisco EPN Manager 4.1 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 タスク情報を AAA サーバ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 ユーザおよび管理者ガイド [英語] 参照してください。

サーバへの Cisco EPN Manager 4.1 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 サーバにアップロードする方法を説明します。

（注） 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 4.1 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。

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. Cisco EPN Manager マイナーリリースファイル（cepn4.1-buildXXX.ubf 形式）を見つけます。
3. 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 サーバに ubf ファイルをアップロードします。

1. 左側のサイドバーメニューから、[Administration] > [Software Update] を選択します。
2. ページ上部の青色の [Upload] リンクをクリックします。

   。
3. [Upload Update] ダイアログボックスで、[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。
4. [OK] をクリックしてファイルをサーバにアップロードします。

Cisco EPN Manager 4.1 が正常にアップロードされると、[Files] タブの下にソフトウェアが表示されます。

Cisco EPN Manager 4.1 のインストール（非 HA）

標準環境（非高可用性）に Cisco EPN Manager 4.1 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、**[Administration]** > **[Software Update]** を選択します。

ステップ 2 [Software Update] ページの EPN Manager 4.1 に関連付けられている [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。

（注） インストールが完了すると、サーバが再起動します。

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、[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。

1. Cisco EPN Manager サーバとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザとしてログインします。
2. ncs status コマンドを実行して、少なくともヘルスモニタ、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、[Software Update] ページで Cisco EPN Manager マイナーリリースのステータスが [Installed] になっていることを確認します。

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。

2. [Cisco EPN Manager Minor Release] が Updates] タブの下に [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（cepnm4.1-buildXXX.ubf の形式）が [Files] タブに表示されていて、[In Use] ステータスが [Yes] になっていることを確認します。

次のタスク

（注） 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 **[Monitor]** > **[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 4.1 のインストール

HA 環境で Cisco EPN Manager 4.1 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. サーバへの Cisco EPN Manager 4.1 インストールファイルの配置（HA 展開）。
4. プライマリサーバとセカンダリサーバへの Cisco EPN Manager 4.1 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）。

（注） 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 タスク情報を AAA サーバ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. プライマリサーバとセカンダリサーバの両方で「Cisco EPN Manager 4.1 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

（注） このプロセスは、サーバが 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 4.1 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 プライマリサーバの Cisco EPN Manager Web GUI に管理者権限を持つユーザ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）]** > **[ハイ アベイラビリティ（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。

サーバへの Cisco EPN Manager 4.1 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 プライマリサーバで、Cisco EPN Manager 4.1 ubf ファイルをアップロードします。「サーバへの Cisco EPN Manager 4.1 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 4.1 ubf ファイルをセカンダリサーバにアップロードします。（プライマリ サーバ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。）

1. 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 サーバの IP アドレスまたはホスト名です。

1. 認証キーを入力して、[ログイン（Login）] をクリックします。
2. [ヘルス モニタ（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。
3. 認証キーを入力して、[ログイン（Login）] をクリックします。
4. 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、[Files] タブの下にファイルが表示されます。

次のタスク

プライマリサーバとセカンダリサーバへの Cisco EPN Manager 4.1 のインストール（HA 展開）。

プライマリサーバとセカンダリサーバへの Cisco EPN Manager 4.1 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 サーバがセカンダリ サーバ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 4.1 のインストール（非 HA）」の説明に従い、Cisco EPN Manager 4.1 をプライマリサーバにインストールし、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 プライマリサーバとセカンダリサーバの両方でハードウェアクロックと NTP クロックを同期し、各サーバのクロックが相互に同期されていることを確認します。

（注） 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 セカンダリサーバに Cisco EPN Manager 4.1 をインストールします。

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

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

2. 認証キーを入力して、[ログイン（Login）] をクリックします。

3. [ヘルス モニタ（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。
4. 認証キーを入力して、[ログイン（Login）] をクリックします。
5. [Software Update] 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 [Install] ボタンをクリックします。
6. 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 サーバが自動的に再起動します。

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

1. セカンダリサーバで SSH セッションを開始して、Cisco EPN Manager CLI 管理者ユーザとしてログインします。
2. ncs status コマンドを実行して、少なくともヘルスモニタ、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。
3. Web GUI にアクセスできたら、セカンダリ サーバの [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 サーバの IP アドレスまたはホスト名です。

4. 認証キーを入力して、[Login] をクリックします。
5. [ヘルス モニタ（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。
6. 認証キーを入力して、[ログイン（Login）] をクリックします。
7. [Files] タブで、Cisco EPN Manager マイナーリリースファイル（cepnm4.1-buildXXX.ubf 形式）が表示されていて、[In Use] ステータスが [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 サーバで、高可用性を有効にし、プライマリ サーバの 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。

1. 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、[Administration] > [Settings] > [High Availability] の順に選択します。
   3. 左側の [HA Configuration] をクリックして、セカンダリサーバの IP アドレス、セカンダリサーバの認証キー、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 サーバとセカンダリ サーバ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。

2. プライマリ サーバの 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。

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

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

2. 認証キーを入力して、[ログイン（Login）] をクリックします。
3. [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） **確認準備機能**は HA 設定をブロックしません。一部のチェックに合格しない場合でも、HA を設定できます。

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 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（Secondary Server）] フィールドにセカンダリ サーバの 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。

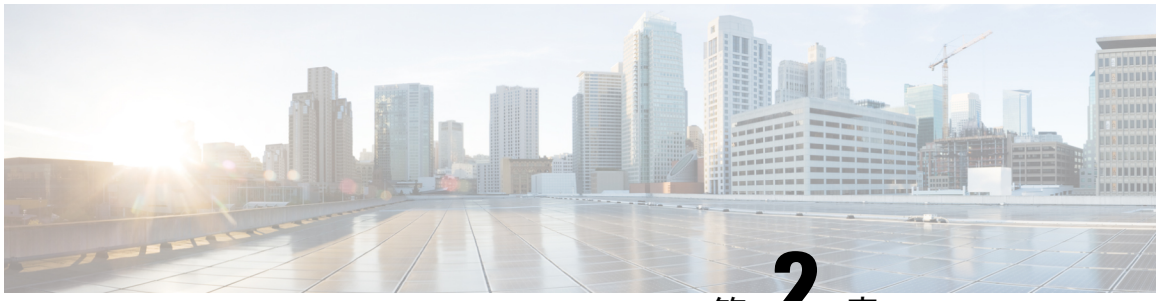
表 *1*：チェックリストの名前と説明

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 サーバとセカンダリ サーバの両方の CPU 数を確認します。 両方のサーバの CPU 数は要件を満たす必要があります。
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバとセカンダリ サーバ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 サーバとセカンダリ サーバの両方の RAM サイズを確認します。 両方のサーバの 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 - システム ディスク サイズ（SYSTEM - CHECK DISK SIZE）	プライマリ サーバとセカンダリ サーバの両方のディスク サイズを確認します。 両方のサーバのディスク サイズが要件を満たしている必要があります。
システム - サーバへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリ サーバが ping を介してセカンダリ サーバ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 サーバとセカンダリ サーバの 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 モニタのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルス モニタ プロセスがプライマリ サーバとセカンダリ サーバ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 サーバとセカンダリ サーバの両方で推奨されている 100 Mbps に一致していることを確認します。 このテストでは、プライマリ サーバとセカンダリ サーバ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ことを確認します。 このポートが無効になっていると、テストは iptables 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 サーバとセカンダリ サーバの両方でアクセス可能であることを確認します。
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）	データベースのリスナーがプライマリ サーバとセカンダリ サーバの両方で稼働中であることを確認します。 障害が発生した場合、テストはリスナーを起動し、ステータスを報告しようとします。
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」の下にあることを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	データベース TNS リスナーの設定ファイル「tnsnames.ora」の下にすべての「WCS」インスタンスが存在していることを確認します。
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 サーバとセカンダリ サーバの両方で TNSPING が成功していることを確認します。

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、[アラームとイベント（Alarms and Events）] ページに転送されます。設定障害イベントは [アラームとイベント（Alarms and Events）] ページにはありません。



第 2 章

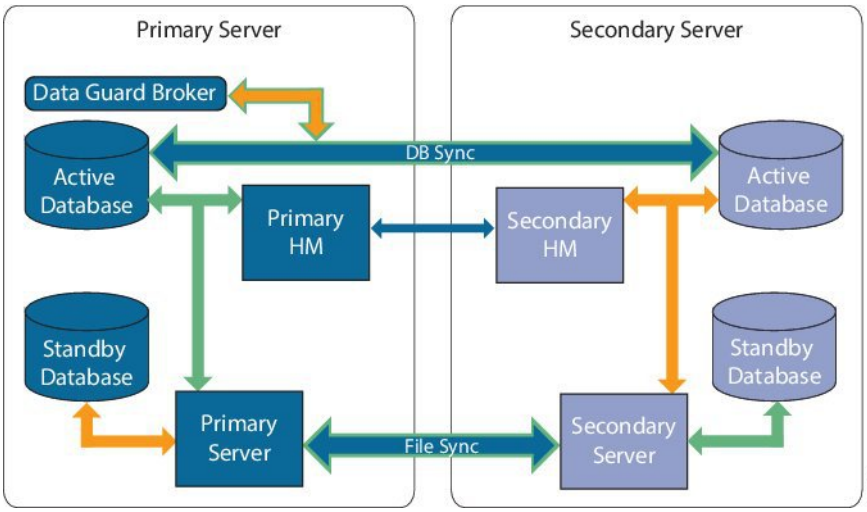
Cisco EPN Manager 4.1 の高可用性

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 サーバのペアを使用して、いずれかのサーバ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 サーバとセカンダリ サーバで構成され、両方のサーバ上にヘルス モニタ（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 サーバへのアクセスを復元する間はセカンダリ サーバ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 サーバの障害発生後 2 ～ 3 分以内にセカンダリ サーバがアクティブなロールを引き継ぎます。

プライマリ サーバに関する問題が解決し、サーバ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 サーバとセカンダリ サーバ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 User and Administrator Guide』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 サーバとセカンダリ サーバの場所	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
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
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 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を指す単一の IP アドレスです。また、プライマリ サーバとセカンダリ サーバ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 サーバとセカンダリ サーバは、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 サーバとセカンダリ サーバ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 User and Administrator Guide』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、プライマリサーバとセカンダリサーバ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 台のサーバの物理的な近接性に関わらず、サーバ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 サーバとセカンダリ サーバ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 サーバとセカンダリ サーバ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、ユーザは実際にアクティブなサーバを知らなくても、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。

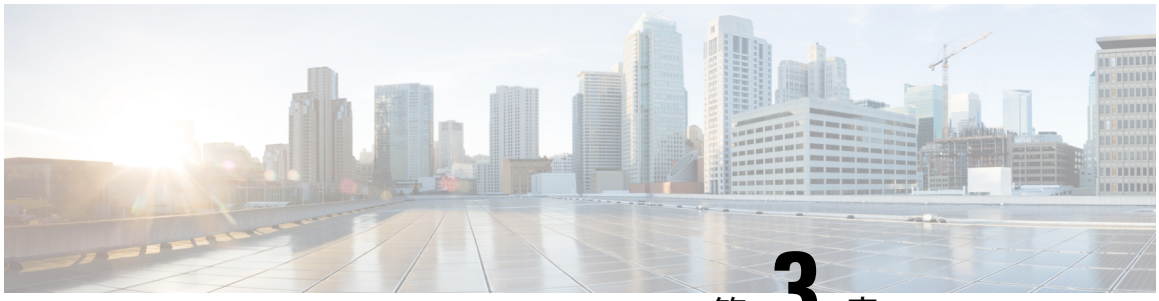
- 仮想 IP アドレス
- プライマリ サーバおよびセカンダリ サーバの IP アドレス
- プライマリ サーバとセカンダリ サーバに設定されているゲートウェイの IP アドレス

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 サーバとセカンダリ サーバに、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 サーバの IP アドレス：10.10.101.1
- セカンダリ サーバの 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 サーバとセカンダリ サーバ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 サーバとセカンダリ サーバの両方を含む 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 サーバに変更を加える必要はありません。プライマリ サーバとセカンダリ サーバを個別の 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、ユーザはアクティブなサーバ 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 4.1 へのアップグレード

有効なアップグレード パス （17 ページ）に記載されているいずれかを実行して、Cisco EPN Manager 4.1 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 4.1 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：現在インストールされている Cisco EPN Manager バージョンのすべてのデータをバックアップし、新しいサーバに Cisco EPN Manager 4.1 をインストールして、新しい Cisco EPN Manager 4.1 サーバにバックアップしたデータを復元します。

（注） Cisco EPN Manager 4.1 のインストールは、Cisco EPN Manager 4.0 OVA/ISO のインストールと、それに続く Cisco EPN Manager 4.1 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の Cisco EPN Manager 4.1 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 4.1 へのインストールパス
Cisco EPN Manager 4.0	**Cisco EPN Manager 4.0 > 4.1**
Cisco EPN Manager 4.0.1	**Cisco EPN Manager 4.0.1 > 4.1**
Cisco EPN Manager 4.0.2	**Cisco EPN Manager 4.0.2 > 4.1**

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 4.1 へのアップグレード（非 HA）

次のトピックで、標準展開（非高可用性）で以前のバージョンの Cisco EPN Manager から Cisco EPN Manager 4.1 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 4.1 へのアップグレード（高可用性） （19 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では、現在インストールされている Cisco EPN Manager バージョンのすべてのデータをバックアップし、新しいサーバに Cisco EPN Manager 4.1 をインストールして、新しい Cisco EPN Manager 4.1 サーバにバックアップしたデータを復元します。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

- 新しいサーバがバックアップ元のサーバ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 新しいサーバで、「Cisco EPN Manager 4.0 のインストール（非 HA）」の手順に従って Cisco EPN Manager 4.1 をインストールします。

ステップ 2 『Cisco Evolved Programmable Network Manager User and Administrator Guide』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を設定します。

ステップ 3 『Cisco Evolved Programmable Network Manager User and Administrator Guide』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に復元します。

Cisco EPN Manager 4.1 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 4.1 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 サーバとセカンダリ サーバの両方で 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Cisco EPN Manager 4.1 のインストールの前提条件 （2 ページ）に記載されている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。
- 新しいサーバが少なくともバックアップ元のサーバ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 User and Administrator Guide』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 User and Administrator Guide』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 高可用性展開での Cisco EPN Manager 4.1 のインストール （6 ページ）の説明に従い、Cisco EPN Manager 4.1 を新しい 2 台のサーバにインストールします。

ステップ 4 インストールが完了したら、新しいプライマリ サーバを設定して、以前のプライマリ サーバと同じリモート 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 User and Administrator Guide』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 5 プライマリ サーバ（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 User and Administrator Guide』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 サーバはプライマリ サーバと同期されます。

ステップ 6 プライマリ サーバ：

1. サーバ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 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、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 7 プライマリ サーバの **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。

1. Cisco EPN Manager を停止します。

```
ncs stop
```

2. Linux CLI ルート ユーザとしてログインします。
3. 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 8 復元が完了したら、プライマリ サーバ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 9 プライマリ サーバにセカンダリ サーバを登録して 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

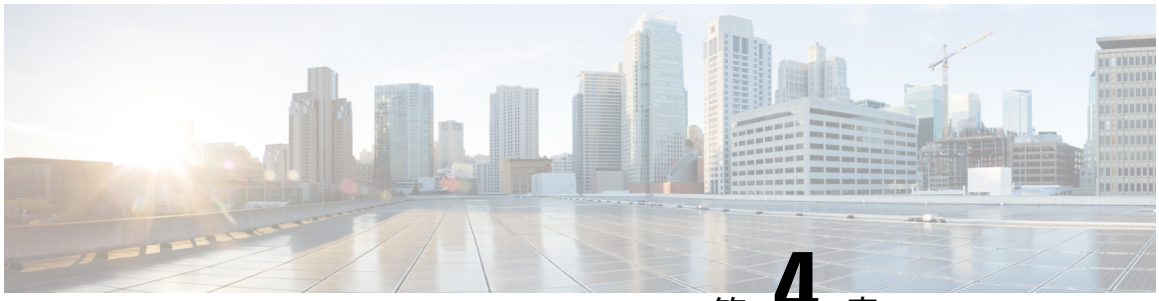
Programmable Network Manager User and Administrator Guide』のプライマリ サーバへのセカンダリ サーバの登録に関する項を参照してください。

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 User and Administrator Guide』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（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 User and Administrator Guide』のユーザ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 [Settings] > [Add Dashlet(s)] から手動で追加できます。

新しい [dashboard] 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 EPNM ISO 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 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 [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 User and Administrator Guide』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 User and Administrator Guide』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（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権限を持つ Cisco EPN Manager Web GUI ユーザを少なくとも 1 人作成し、Web GUI ルート ユーザを無効にします。このユーザの無効化については、『Cisco Evolved Programmable Network Manager User and Administrator Guide』のユーザ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 ユーザを無効にします。『Cisco Evolved Programmable Network Manager User and Administrator Guide』を参照してください。

次のタスク

サーバ、ユーザ、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 User and Administrator Guide』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 インターフェイスとユーザ タイプについては、『Cisco Evolved Programmable Network Manager User and Administrator Guide』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	Etc/GMT+6
Africa/Accra	America/St_Kitts	Etc/GMT+7

Africa/Addis_Ababa	America/St_Lucia	Etc/GMT+8
Africa/Algiers	America/St_Thomas	Etc/GMT+9
Africa/Asmara	America/St_Vincent	Etc/GMT0
Africa/Asmera	America/Swift_Current	Etc/GMT-0
Africa/Bamako	America/Tegucigalpa	Etc/GMT-1
Africa/Bangui	America/Thule	Etc/GMT-10
Africa/Banjul	America/Thunder_Bay	Etc/GMT-11
Africa/Bissau	America/Tijuana	Etc/GMT-12
Africa/Blantyre	America/Toronto	Etc/GMT-13
Africa/Brazzaville	America/Tortola	Etc/GMT-14
Africa/Bujumbura	America/Vancouver	Etc/GMT-2
Africa/Cairo	America/Virgin	Etc/GMT-3
Africa/Casablanca	America/Whitehorse	Etc/GMT-4
Africa/Ceuta	America/Winnipeg	Etc/GMT-5
Africa/Conakry	America/Yakutat	Etc/GMT-6
Africa/Dakar	America/Yellowknife	Etc/GMT-7
Africa/Dar_es_Salaam	Antarctica/Casey	Etc/GMT-8
Africa/Djibouti	Antarctica/Davis	Etc/GMT-9
Africa/Douala	Antarctica/DumontDUrville	Etc/Greenwich
Africa/El_Aaiun	Antarctica/Mawson	Etc/UCT
Africa/Freetown	Antarctica/McMurdo	Etc/Universal
Africa/Gaborone	Antarctica/Palmer	Etc/UTC
Africa/Harare	Antarctica/Rothera	Etc/Zulu
Africa/Johannesburg	Antarctica/South_Pole	Europe/Amsterdam
Africa/Kampala	Antarctica/Syowa	Europe/Andorra
Africa/Khartoum	Antarctica/Vostok	Europe/Athens
Africa/Kigali	rctic/Longyearbyen	Europe/Belfast
Africa/Kinshasa	Asia/Aden	Europe/Belgrade
Africa/Lagos	Asia/Almaty	Europe/Berlin

Africa/Libreville	Asia/Amman	Europe/Bratislava
Africa/Lome	Asia/Anadyr	Europe/Brussels
Africa/Luanda	Asia/Aqtau	Europe/Bucharest
Africa/Lubumbashi	Asia/Aqtobe	Europe/Budapest
Africa/Lusaka	Asia/Ashgabat	Europe/Chisinau
Africa/Malabo	Asia/Ashkhabad	Europe/Copenhagen
Africa/Maputo	Asia/Baghdad	Europe/Dublin
Africa/Maseru	Asia/Bahrain	Europe/Gibraltar
Africa/Mbabane	Asia/Baku	Europe/Guernsey
Africa/Mogadishu	Asia/Bangkok	Europe/Helsinki
Africa/Monrovia	Asia/Beirut	Europe/Isle_of_Man
Africa/Nairobi	Asia/Bishkek	Europe/Istanbul
Africa/Ndjamena	Asia/Brunei	Europe/Jersey
Africa/Niamey	Asia/Calcutta	Europe/Kaliningrad
Africa/Nouakchott	Asia/Choibalsan	Europe/Kiev
Africa/Ouagadougou	Asia/Chongqing	Europe/Lisbon
Africa/Porto-Novo	Asia/Chungking	Europe/Ljubljana
Africa/Sao_Tome	Asia/Colombo	Europe/London
Africa/Timbuktu	Asia/Dacca	Europe/Luxembourg
Africa/Tripoli	Asia/Damascus	Europe/Madrid
Africa/Tunis	Asia/Dhaka	Europe/Malta
Africa/Windhoek	Asia/Dili	Europe/Mariehamn
America/Adak	Asia/Dubai	Europe/Minsk
America/Anchorage	Asia/Dushanbe	Europe/Monaco
America/Anguilla	Asia/Gaza	Europe/Moscow
America/Antigua	Asia/Harbin	Europe/Nicosia
America/Araguaina	Asia/Ho_Chi_Minh	Europe/Oslo
America/Argentina/	Asia/Hong_Kong	Europe/Paris
America/Argentina/	Asia/Hovd	Europe/Podgorica

America/Argentina/Catamarca	Asia/Irkutsk	Europe/Prague
America/Argentina/Cordoba	Asia/Istanbul	Europe/Riga
America/Argentina/Jujuy	Asia/Jakarta	Europe/Rome
America/Argentina/La_Rioja	Asia/Jayapura	Europe/Samara
America/Argentina/Mendoza	Asia/Jerusalem	Europe/Samara
America/Argentina/Rio_Gallegos	Asia/Kabul	Europe/Sarajevo
America/Argentina/Salta	Asia/Kamchatka	Europe/Simferopol
America/Argentina/San_Juan	Asia/Karachi	Europe/Skopje
America/Argentina/San_Luis	Asia/Kashgar	Europe/Sofia
America/Argentina/Tucuman	Asia/Kathmandu	Europe/Stockholm
America/Argentina/Ushuaia	Asia/Katmandu	Europe/Tallinn
America/Aruba	Asia/Kolkata	Europe/Tirane
America/Asuncion	Asia/Krasnoyarsk	Europe/Tiraspol
America/Atikokan	Asia/Kuala_Lumpur	Europe/Uzhgorod
America/Atka	Asia/Kuching	Europe/Vaduz
America/Bahia	Asia/Kuwait	Europe/Vatican
America/Barbados	Asia/Macao	Europe/Vienna
America/Belem	Asia/Macau	Europe/Vilnius
America/Belize	Asia/Magadan	Europe/Volgograd
America/Blanc-Sablon	Asia/Makassar	Europe/Warsaw
America/Boa_Vista	Asia/Manila	Europe/Zagreb
America/Bogota	Asia/Muscat	Europe/Zaporozhye
America/Boise	Asia/Nicosia	Europe/Zurich
America/Buenos_Aires	Asia/Novosibirsk	Factory
America/Cambridge_Bay	Asia/Omsk	GB
America/Campo_Grande	Asia/Oral	GB-Eire
America/Cancun	Asia/Phnom_Penh	GMT
America/Caracas	Asia/Pontianak	GMT+0
America/Catamarca	Asia/Pyongyang	GMT0

America/Cayenne	Asia/Qatar	GMT-0
America/Cayman	Asia/Qyzylorda	Greenwich
America/Chicago	Asia/Rangoon	Hongkong
America/Chihuahua	Asia/Riyadh	HST
America/Coral_Harbour	Asia/Riyadh87	Iceland
America/Cordoba	Asia/Riyadh88	Indian/Antananarivo
America/Costa_Rica	Asia/Riyadh89	Indian/Chagos
America/Cuiaba	Asia/Saigon	Indian/Christmas
America/Curacao	Asia/Sakhalin	Indian/Cocos
America/Danmarkshavn	Asia/Samarkand	Indian/Comoro
America/Dawson	Asia/Seoul	Indian/Kerguelen
America/Dawson_Creek	Asia/Shanghai	Indian/Mahe
America/Denver	Asia/Singapore	Indian/Maldives
America/Detroit	Asia/Taipei	Indian/Mauritius
America/Dominica	Asia/Tashkent	Indian/Mayotte
America/Edmonton	Asia/Tbilisi	Indian/Reunion
America/Eirunepe	Asia/Tehran	Iran
America/El_Salvador	Asia/Tel_Aviv	Israel
America/Ensenada	Asia/Thimbu	Jamaica
America/Fort_Wayne	Asia/Thimphu	Japan
America/Fortaleza	Asia/Tokyo	Kwajalein
America/Glace_Bay	Asia/Ujung_Pandang	Libya
America/Godthab	Asia/Ulaanbaatar	MET
America/Goose_Bay	Asia/Ulan_Bator	Mexico/BajaNorte
America/Grand_Turk	Asia/Urumqi	Mexico/BajaSur
America/Grenada	Asia/Vientiane	Mexico/General
America/Guadeloupe	Asia/Vladivostok	Mideast/Riyadh87
America/Guatemala	Asia/Yakutsk	Mideast/Riyadh88
America/Guayaquil	Asia/Yekaterinburg	Mideast/Riyadh89

America/Guyana	Asia/Yerevan	MST
America/Halifax	Atlantic/Azores	MST7MDT
America/Havana	Atlantic/Bermuda	Navajo
America/Hermosillo	Atlantic/Canary	New_Salem
America/Indiana/Indianapolis	Atlantic/Cape_Verde	NZ
America/Indiana/Knox	Atlantic/Faeroe	NZ-CHAT
America/Indiana/Marengo	Atlantic/Faroe	Pacific/Apia
America/Indiana/Petersburg	Atlantic/Jan_Mayen	Pacific/Auckland
America/Indiana/Tell_City	Atlantic/Madeira	Pacific/Chatham
America/Indiana/Vevay	Atlantic/Reykjavik	Pacific/Easter
America/Indiana/Vincennes	Atlantic/South_Georgia	Pacific/Efate
America/Indiana/Winamac	Atlantic/St_Helena	Pacific/Enderbury
America/Indianapolis	Atlantic/Stanley	Pacific/Fakaofo
America/Inuvik	Australia/ACT	Pacific/Fiji
America/Iqaluit	Australia/Adelaide	Pacific/Funafuti
America/Jamaica	Australia/Brisbane	Pacific/Galapagos
America/Jujuy	Australia/Broken_Hill	Pacific/Gambier
America/Juneau	Australia/Canberra	Pacific/Guadalcanal
America/Kentucky/Louisville	Australia/Currie	Pacific/Guam
America/Kentucky/Monticello	Australia/Darwin	Pacific/Honolulu
America/Knox_IN	Australia/Eucla	Pacific/Johnston
America/La_Paz	Australia/Hobart	Pacific/Kiritimati
America/Lima	Australia/LHI	Pacific/Kosrae
America/Los_Angeles	Australia/Lindeman	Pacific/Kwajalein
America/Louisville	Australia/Lord_Howe	Pacific/Majuro
America/Maceio	Australia/Melbourne	Pacific/Marquesas
America/Managua	Australia/North	Pacific/Midway
America/Manaus	Australia/NSW	Pacific/Nauru
America/Marigot	Australia/Perth	Pacific/Niue

America/Martinique	Australia/Queensland	Pacific/Norfolk
America/Mazatlan	Australia/South	Pacific/Noumea
America/Mendoza	Australia/Sydney	Pacific/Pago_Pago
America/Menominee	Australia/Tasmania	Pacific/Palau
America/Merida	Australia/Victoria	Pacific/Pitcairn
America/Mexico_City	Australia/West	Pacific/Ponape
America/Miquelon	Australia/Yancowinna	Pacific/Port_Moresby
America/Moncton	Brazil/Acre	Pacific/Rarotong
America/Monterrey	Brazil/DeNoronha	Pacific/Saipan
America/Montevideo	Brazil/East	Pacific/Samoa
America/Montreal	Brazil/West	Pacific/Tahiti
America/Montserrat	Buenos_Aires	Pacific/Tarawa
America/Nassau	Canada/Atlantic	Pacific/Tongatapu
America/New_York	Canada/Central	Pacific/Truk
America/Nipigon	Canada/Eastern	Pacific/Wake
America/Nome	Canada/East-Saskatchewan	Pacific/Wallis
America/Noronha	Canada/Mountain	Pacific/Yap
America/North_Dakota/	Canada/Newfoundland	Poland
America/North_Dakota/Center	Canada/Pacific	Portugal
America/Panama	Canada/Saskatchewan	PRC
America/Pangnirtung	Canada/Yukon	PST8PDT
America/Paramaribo	CET	ROC
America/Phoenix	Chile/Continental	ROK
America/Port_of_Spain	Chile/EasterIsland	Singapore
America/Port-au-Prince	ComodRivadavia	Turkey
America/Porto_Acre	CST6CDT	UCT
America/Porto_Velho	Cuba	Universal
America/Puerto_Rico	EET	US/Alaska
America/Rainy_River	Egypt	US/Aleutian

America/Rankin_Inlet	Eire	US/Arizona
America/Recife	EST	US/Central
America/Regina	EST5EDT	US/Eastern
America/Resolute	Etc/GMT	US/East-Indiana
America/Rio_Branco	Etc/GMT+0	US/Hawaii
America/Rosario	Etc/GMT+1	US/Indiana-Starke
America/Santarem	Etc/GMT+10	US/Michigan
America/Santiago	Etc/GMT+11	US/Mountain
America/Santo_Domingo	Etc/GMT+12	US/Pacific
America/Sao_Paulo	Etc/GMT+2	US/Samoa
America/Scoresbysund	Etc/GMT+3	UTC
America/Shiprock	Etc/GMT+4	WET
America/St_Barthelemy	Etc/GMT+5	W-SU
		Zulu