Cisco EPN Manager サーバーのセットアップ

以降のトピックでは、Cisco EPN Manager をインストールした後に管理者が実行するタスクについて説明します。これらのタスクが完了したら、Cisco EPN Manager スタートアップ ガイドに説明されているように、ユーザーはログインして作業環境を設定できます。

Cisco EPN Manager のさまざまなタイプのユーザー（CLI ユーザーや Web GUI ユーザーなど）の詳細については、Cisco EPN Manager で CLI ユーザー インターフェイスを切り替える方法を参照してください。

（注） ベスト プラクティス：Cisco EPN Manager のセキュリティ強化の重要な情報を必ず確認してください。

サーバーのセットアップ タスク

タスク	参照先
バックアップ設定の確認	自動アプリケーション バックアップのセットアップ
必要な製品ライセンスおよびソフトウェア アップデートのインストール	ライセンスおよびソフトウェア アップデート

タスク	参照先
ソフトウェア アップデートの場合： • 製品ソフトウェア アップデート（重大な修正、デバイス サポート、アドオン）の通知を有効にする • Cisco EPN Manager がソフトウェア アップデートを確認する際に、クレデンシャルを Cisco.com に保存するかどうかを指定する。保存する場合、更新の確認時にユーザーにクレデンシャルについてのプロンプトを表示するかどうかを指定する	ソフトウェア アップデートに関する通知の有効化または無効化
サーバーとブラウザベースの GUI クライアントの間のやり取りを保護するためにサーバー上で HTTPS を設定する（HTTP も使用できますが、HTTPS が推奨されています）	Cisco EPN Manager サーバーの接続の保護
ハイ アベイラビリティの設定	ハイ アベイラビリティの設定と管理
データの保持および消去の調整	データの収集と消去
システムの問題を通知するサーバー関連のトラップでは、しきい値設定と重大度をカスタマイズし、設定した受信者に SNMP トラップ通知としてトラップを転送する	サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 SNMP トラップ通知としてのアラームおよびイベントの転送
時間をサーバーとネットワーク デバイスとの間で同期するための NTP（Network Time Protocol）のセットアップ	サーバーでの NTP の設定
サーバーとネットワーク デバイス間のファイル転送のためのサーバーにおける FTP/TFTP の設定	サーバーでの FTP/TFTP/SFTP サービスの有効化
Cisco EPN Manager サーバーのプロキシの設定	Cisco EPN Manager プロキシ サーバーの設定
電子メール サーバーの設定	SMTP 電子メール サーバーの設定
コンプライアンス機能を有効にする（デバイス設定からの逸脱を識別するためにこの設定を使用する場合）	コンプライアンス監査の有効化および無効化
Cisco EPN Manager がネットワーク内に存在するサービス、およびプロビジョニング ウィザードを使用してプロビジョニングされたサービスを検出するように、サービス検出機能を有効化にします。	サービス検出の有効化および無効化
シスコ製品の向上に寄与する製品フィードバックの設定	シスコサポート リクエストのデフォルトの設定

タスク	参照先
シスコ製品の向上に寄与する製品フィードバックの設定	シスコ製品フィードバックの設定

LDAP/Active Directory サーバーを設定して使用する

Cisco EPN Manager への LDAP サーバーの追加

LDAP ディレクトリにリストされ、EPNM に指定されていないユーザーを認証します。

（注） また、Cisco Identity Services Engine（ISE）を使用してユーザーを認証することもできます。詳細については、Cisco ISE と RADIUS または TACACS+ による外部認証を参照してください。

LDAP サーバーを追加するには、次の手順を実行します。

（注） Active Directory サーバーを追加するには、次と同じ手順を使用します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles, & AAA）]** を選択し、LDAP サーバーを選択します。

（注） このページに表示されている入力フィールドに入力する値には、次の制限が適用されます。

- 先頭または末尾にスペースがない。
- 入力文字列を「#」で始めることはできない。
- 特殊文字：「'+ * " ' / \ \\ < > ; ( ) \u0000（Unicode の Null 文字） \r」は入力できない。

ステップ 2 LDAP サーバーを選択した後、右側のペインで [+] アイコンをクリックして、追加する LDAP サーバーの詳細を作成します。

ステップ 3 LDAP サーバーの必要な詳細（サーバー アドレス、サーバー ポート、パスワード、IP アドレス、DNS 名など）を入力します。

ステップ 4 SSL 通信チャネルを使用する場合は、[セキュア認証を使用する（Use Secure Auth）]チェックボックスをオンにします。LDAP 証明書のインストールの詳細については、「Cisco EPN Manger での LDAP サーバーの設定」に記載されている方法を参照してください。

（注） Web サーバーの接続を保護するため、HTTPS をセットアップします。これは、SSL で LDAP を設定するための前提条件です。管理者は、各 LDAP サーバーのスキーマを設定できます。

ステップ 5 [管理 DN（Admin DN）] 文字列を入力します。

ステップ 6 パスワードと確認パスワードの詳細を入力します。

（注） LDAP 管理者は、文字列と確認パスワードを把握しています。

ステップ 7 次のフィールドにスキーマを入力します。通常、どの LDAP サーバーにもユーザーとグループの固有の設定と連結証明書のファイルがあります。

a) [サブジェクト名属性（Subject Name Attribute）]：この値は、特定のユーザー名が編成されている LDAP サーバー ユーザー プロファイル内の *uid* 属性を表します。

b) [グループ名属性（Group Name Attribute）]：この値は、グループ メンバ（管理者、モニター、コンフィギュレータ）に割り当てられているロールの権限を表し、LDAP サーバー グループ プロファイルの *description* 属性で示されます。ユーザー グループ名の値については、**[管理（Administration）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[ユーザー グループ（User Groups）]** ページを参照してください。

c) [グループ マップ属性（Group Map Attribute）]：この値は、グループとユーザー間の関連付けを表し、LDAP サーバーのグループ プロファイル内の *memberUid* 属性で示されます。

（注） LDAP または Active Directory で複数のユーザーロールを指定するには、同じ名前を持つ複数の属性を作成するか、または 1 つの属性を作成し、カンマで区切られた複数のユーザーロールをリストします。次に例を示します。

- 同じ名前の複数の属性を指定するには、次のコマンドを実行します。

```
description=Admin
description=Monitor Lite
```

- 1 つの属性と複数のユーザーロールを指定するには、次の手順を実行します。

```
description=Admin,Monitor Lite
```

d) [仮想ドメイン属性（Virtual Domain Attribute）]：この値は、ユーザーがアクセスできるネットワークセクションを表し、LDAP サーバーのユーザープロファイル内の *title* 属性に記述されます。この値は、**[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** ウィンドウに設定されている Cisco EPN Manager の仮想ドメインプロファイルと関連します。仮想ドメインに含める要素とその仮想ドメインへのアクセス権を付与するユーザーを選択できます。

（注） LDAP または Active Directory で複数の仮想ドメインを指定するには、同じ名前の複数の属性を作成するか、1つの属性を作成し、カンマで区切られた仮想ドメインをリストします。次に例を示します。

- 同じ名前の複数の属性を指定するには、次のコマンドを実行します。

```
description=VirtualDomain1
description=VirtualDomain2
```

- 1 つの属性と複数のユーザーロールを指定するには、次の手順を実行します。

```
description=VirtualDomain1,VirtualDomain2
```

e) [サブジェクト検索ベース（Subject Search Base）]：ユーザーが配置されている場所を検索するパスを指定します。

f) [グループ検索ベース（Group Search Base）]：グループの場所を検索するパスを指定します。

ステップ 8 [再試行（Retries）] フィールドに、ソース ファイルの LDAP 認証を実行する回数を入力します。

ステップ 9 [保存（Save）] をクリックします。

Cisco EPN Manger での LDAP サーバーの設定

Cisco EPN Managerは、単方向 SSL を使用して LDAP サーバーを接続します。つまり、LDAP サーバーの認証局（CA）ルート（および中間）証明書を Cisco EPN Manager にインストールする必要があります。これらの証明書は LDAP サーバーの CA から入手します。次の手順では、ルート（および中間）CA 証明書をインストールするステップについて説明します。

始める前に

LDAP 証明書が Cisco EPN Manager にインストールされていることを確認するには、次の手順を実行します。

1. 顧客が所有する LDAP サーバーの SSL 証明書のルート証明書と中間証明書を取得します。
2. Cisco EPN Manager サーバーとの SSH セッションの確立で説明したように、ssh を使用して CLI 管理者ユーザーとしてログインします。
3. LDAP サーバー証明書の CA ルート/中間証明書を Cisco EPN Manager のローカル ディレクトリにコピーします。たとえば、rootCA.pem を /localdisk/defaultRepo にコピーします。
4. Cisco EPN Manager Admin CLI で、Cisco EPN Manager にこの CA ルート証明書をインポートするコマンドを `EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}` として実行します（例：`EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias epnm40 repository defaultRepo certnew.cer truststore system`）。これにより、Java インポート信頼ストアに LDAP 証明書がインポートされます。
5. Cisco EPN Manager を再起動します。

（注） 2 台の LDAP サーバーと 2 台の Cisco EPN Manager サーバーがある場合（HA モード）、各 LDAP サーバーのルート/中間証明書をインストールしてから、HA のガイドラインに基づいて各 Cisco EPN Manager サーバーを再起動します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[AAA モード（AAA Mode）] を選択します。

ステップ 2 [LDAP] オプション ボタンを選択します。

ステップ 3 [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバーがダウンした場合にローカル データベースの使用が有効になります。

ステップ 4 外部 LDAP サーバーがダウンした場合にローカル認証に戻すには、次の手順を実行します。

a) [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] を選択します。

b) フォールバック条件（[サーバーが応答しないときのみ（Only on no server response）] または [認証に失敗したかサーバーが応答しないとき（On authentication failure or no server response）]）を指定します。

（注） ルートユーザーはローカルで認証されているため、ルートユーザーとしてログインできる必要があります。

ステップ 5 [保存（Save）] をクリックします。

（注） 別のブラウザを使用して、新しいユーザー名とパスワードで LDAP にログインします。

Cisco WAN Automation Engine と Cisco EPN Manager の統合

Cisco WAN Automation Engine（WAE）のプラットフォームは、ソフトウェア モジュールを相互接続し、ネットワークと通信し、外部アプリケーションとインターフェイスする API を提供するオープンでプログラマブルなフレームワークです。

Cisco WAE は、ネットワークの継続的なモニターリングと分析およびネットワーク上のトラフィック需要に基づく現在のネットワークのモデルを作成および維持するためのツールを提供します。このネットワーク モデルには、トポロジ、設定、トラフィック情報など、特定の時点でのネットワークに関するすべての関連情報が含まれています。この情報は、トラフィック要求、パス、ノードとリンクの障害、ネットワークの最適化、またはその他の変更によるネットワークへの影響を分析するための基礎として使用できます。

（注） 詳細については、『*Cisco WAN Automation Engine (WAE) Installation Guide*』と『*Cisco WAN Automation Engine (WAE) User Guide*』を参照してください。

Cisco EPN Manager では、明示的なパスを持つ単方向トンネルまたは双方向トンネルを作成すると、WAN Automation Engine（WAE）との統合により、Cisco EPN Manager から自動的に REST コールを使用して明示的なパスが提供されます。そのため、明示的なパスを手動で入力する必要がなくなります。WAE は、可能なネットワーク パスのリストを表示し、適切なパスを選択できるようにします。

WAE パラメータの設定

WAE パスの詳細を指定するには、次の手順を実行します。

始める前に

WAE パラメータを設定することを確認します。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。
2. 回線 VC を展開し、[WAE サーバー設定（WAE Server Settings）] を選択します。

3. 関連する WAE の詳細（バージョン 7.1.3 以降）とフィールドの詳細（[WAE サーバー IP（WAE Server IP）]、[WAE ポートアドレス（WAE Port Address）]、[WAE サーバーユーザー名（WAE Server User Name）]、[WAE サーバーパスワード（WAE Server Password）] など）を入力します。
4. [保存（Save）] をクリックして WAE サーバーの設定を保存するか、または [デフォルトにリセット（Reset to Defaults）] をクリックしてすべての入力をクリアします。

ステップ 1 必要なパラメータを持つ単方向トンネルまたは双方向トンネルを作成します。詳細については、MPLS TE トンネルの作成とプロビジョニングを参照してください。

ステップ 2 [パスの制約の詳細（Path Constraints Details）] 領域で、パスのタイプを [動作中（Working）] または [保護済み（Protected）] のいずれかとして選択します。フィールドと属性の説明については、パスの制約の詳細に関するフィールド参照：MPLS TE トンネルを参照してください。

ステップ 3 必要に応じて [新しいパス（New Path）] チェックボックスをオンにして、[WAEサーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。

ステップ 4 [WAE サーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。EPNM マネージャは、WAE ネットワークを取得するために REST 要求を WAE に送信します。
WAE は可能なネットワークのリストを返します。

ステップ 5 [WAE ネットワークの選択（Select WAE Network）] ドロップダウン リストから、ネットワークを選択します。
EPNM マネージャは、送信元、宛先、ネットワークなどの必要なすべてのパラメータを持つ REST 設定要求を WAE に送信します。返される最大パスのデフォルト値は 2 です。最大パス値は WAE を介して設定されます。WAE は、要求を満たす可能性のあるパスのリストを表示します。

ステップ 6 [WAE パスの選択（Select WAE Path）] ドロップダウン リストから、返された適切なパスを選択します。
EPNM は、マップ上に選択したパス オーバーレイを表示します。

ステップ 7 [パス名（Path Name）] フィールドにパスの名前を入力します。
最後に選択したパスを明示的なパスとして使用して、順序のプロビジョニングを続行できます。

ユーザー管理セットアップ タスク

タスク	参照先
管理権限を持つ Web GUI ユーザーを作成し、Web GUI root アカウントを無効にします。	管理者権限を持つ Web GUI ユーザーの作成 Web GUI ルート ユーザーの無効化および有効化
ユーザー認証および許可のセットアップ	外部認証の設定 ローカル認証の設定

タスク	参照先
ユーザー アカウントとユーザー グループの作成	ユーザーが実行できるタスク Web インターフェイスの制御
ユーザーセキュリティ設定の調整（ローカル認証のパスワード規則、アイドル時間のログアウト設定）	ローカル認証のためのグローバルパスワードポリシーの設定
ジョブを許可できるユーザーの指定	ジョブ承認者を設定してジョブを承認する
仮想ドメインを作成してデバイスアクセスを制御する	デバイスへのユーザーアクセスを制御するための仮想ドメインの作成
ユーザーが GUI クライアントにログインしたときに表示されるメッセージの作成	ログインバナー（ログインの免責事項）の作成

障害管理セットアップ タスク

タスク	参照先
アラームとイベントを電子メール形式で他の受信者に転送する	
アラームとイベントを SNMP トラップ形式で他の受信者に転送する	SNMP トラップ通知としてのアラームおよびイベントの転送
アラームとイベントの表示と検索用のグローバル設定を構成する • アラーム テーブルとイベント テーブルで確認済み、割り当て済み、およびクリア済みのアラームを非表示にする • 確認済みと割り当て済みのアラームを検索結果に含める • デバイス名をアラーム メッセージに含める	確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する
特定のイベントの重大度をカスタマイズする	アラーム重大度レベルの変更
特定のアラームの自動クリア間隔をカスタマイズする	アラームの自動クリア間隔の変更
アラームの [障害ソース（Failure Source）] フィールド内のテキストをユーザーにわかりやすくする	アラーム重大度レベルの変更
優先イベントの動作をカスタマイズする	完全優先ベントの動作の変更

タスク	参照先
一般イベント処理を制御する	汎用トラップ処理を有効または無効にする
ユーザーがシスコ サポート要求を作成できるかどうかとその方法を制御する	シスコサポート リクエストのデフォルトの設定

Web GUI セットアップ タスク（管理者）

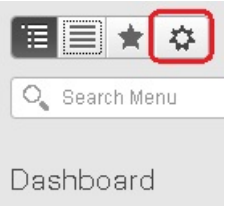
タスク	参照先
展開で使用しない機能またはメニュー項目の無効化	Web GUI メニューのカスタマイズによる Cisco EPN Manager 機能の無効化 （9 ページ）
システムモニターリング管理ダッシュボードのセットアップ	システム監視ダッシュボードを使用して、Cisco EPN Manager サーバーのヘルス、ジョブ、パフォーマンス、および API 統計をチェックする

Web GUI メニューのカスタマイズによる Cisco EPN Manager 機能の無効化

ルート、スーパーユーザー、または管理者ユーザー グループに属している場合は、特定のメニューが Web GUI に表示されなくなるように Cisco EPN Manager をカスタマイズできます。ユーザー グループとそのメンバーの表示を参照してください。これは、展開で Cisco EPN Manager のすべての機能は使用しない場合に役立ちます。メニューを無効にすると、ユーザーのロールに関係なく、すべてのユーザーの Web GUI に表示されなくなります。

機能全体と特定のメニューを無効にして Web GUI をカスタマイズするには、次の手順を実行します。現在無効になっている機能を再び有効にするには、同じ手順を使用しますが、機能のステータスを [有効（Enabled）] に切り替えます（または [すべて有効にする（Enable All）] をクリックします）。

ステップ 1 左側のサイドバー メニューの上に表示される歯車をクリックします。



ステップ 2 機能全体を無効にするには、次の手順を実行します。

1. [機能ナビゲーション グループ（Feature Navigation Groups）] 領域で機能を見つけますます。
2. 機能の [ステータス（Status）] 列でトグルをクリックして [無効（Disabled）] を表示します。
3. 無効にするメニューを確認するには、[メニューの詳細（Menu Details）] 領域のメニューをスクロールします。影響を受けているすべてのメニューが [無効（Disabled）] として表示されます。

ステップ 3 特定のメニューを無効にするには、次の手順を実行します。

1. [メニューの詳細（Menu Details）] 領域でメニューを見つけます。
2. メニューの [ステータス（Status）] 列でトグルをクリックして [無効（Disabled）] を表示します。サブメニューを含むメニューを無効にすると、サブメニューも無効になります。次に例を示します。
   - [グループ管理（Group Management）] を無効にすると、Cisco EPN Manager は [グループ管理（Group Management）] のサブメニューすべて（[ネットワーク デバイス グループ（Network Device Group）]、[コンピューティング デバイス グループ（Compute Device Groups）]、および [ポート グループ（Port Groups）]）を無効にします。
   - [コンピューティング デバイス グループ（Compute Device Groups）] サブメニューのみを無効にした場合も、Cisco EPN Manager は [グループ管理（Group Management）] の下のサブメニュー、[ネットワーク デバイス グループ（Network Device Groups）] と [ポート グループ（Port Groups）] サブメニューは表示します。
3. 無効にするメニューを確認するには、[メニューの詳細（Menu Details）] 領域のメニューをスクロールします。

ステップ 4 [保存（Save）] をクリックし、Web GUI からログアウトします。

ステップ 5 Web GUI にログインし直し、変更内容を検証します。