サーバーの正常性と構成

Cisco EPN Manager サーバーの構成の表示

現在のサーバー時間、カーネル バージョン、オペレーティング システム、ハードウェア情報などの Cisco EPN Manager サーバーの構成情報を表示するには、以下の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。

ステップ 3 ダッシュボードの左上にある [システム情報（System Information）] をクリックして、[システム情報（System Information）] フィールドを展開します。

Cisco EPN Manager のホスト名の変更

Cisco EPN Manager では、サーバーへのインストール時にホスト名の入力を求めるプロンプトが表示されます。さまざまな理由により、Cisco EPN Manager サーバーに設定されたホスト名と他の場所に設定されたホスト名の間で不一致が発生することがあります。この問題は、Cisco EPN Manager を再インストールしなくてもサーバーでホスト名を変更すれば解決できます。次の手順を実行します。

（注） 状況によっては、ホスト名を変更した後にファイル `tnsnames.ora` と `listener.ora` でホスト名が正しく反映されていないことがあります。これを回避するには、作業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で次のファイルのバックアップを作成します。
   - /base/product/12.1.0/dbhome_1/network/admin/tnsnames.ora
   - /base/product/12.1.0/dbhome_1/network/admin/listener.ora
2. ホスト名を変更した後、2 つのバックアップファイルを使用して、新しく指定したホスト名が反映されるようにすべてのホスト名を編集します。
3. Oracle リスナーを再起動します（Cisco EPN Manager がダウンしている場合に Cisco EPN Manager の再起動が必要で、ステップ 2 を実行できる場合を除く）。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開き、**configure terminal** モードを開始します。

「CLI 経由の接続」を参照してください。

ステップ 2 次のコマンドを入力します。

```
Cisco_EPN_Manager_Server/admin(config)#hostname newHostName
```

newHostName には、Cisco EPN Manager サーバーに割り当てるホスト名を指定します。

ステップ 3 **ncs stop** および **ncs start** コマンドを使用して、Cisco EPN Manager サーバーを再起動します。

ステップ 4 SSL サーバー証明書用に設定されているホスト名を確認します。

- ホスト名がステップ 2 で指定したホスト名と同じであれば、ここで手順を終了します。
- ホスト名が違う場合は、ステップ 2 で指定したホスト名で新しい SSL サーバー証明書を作成し、インストールする必要があります。。

CLI 経由の接続

管理者は、コマンド ライン インターフェイス（CLI）経由で Cisco EPN Manager サーバーに接続できます。Cisco EPN Manager CLI 経由でのみアクセス可能なコマンドとプロセスを実行する場合は、CLI アクセス権が必要です。これらには、サーバーの起動および停止、ステータスの確認などを行うコマンドが含まれます。

始める前に

手順を開始する前に、次の点を確認してください。

- そのサーバーまたはアプライアンスへの CLI アクセス権を持っている管理ユーザーのユーザー ID とパスワードがわかっていること。明示的に禁止されていない限り、すべての管理ユーザーには CLI アクセス権が与えられます。
- Cisco EPN Manager サーバーの IP アドレスまたはホスト名がわかっていること。

ステップ 1 SSH クライアントを起動し、ローカル マシンのコマンド ラインから SSH セッションを開始するか、Cisco EPN Manager の物理アプライアンスまたは仮想アプライアンスの専用コンソールに接続します。

ステップ 2 該当する方法でログインします。GUI クライアントを使用している場合：CLI アクセス権を持つアクティブな管理者の ID と Cisco EPN Manager サーバーの IP アドレスまたはホスト名を入力します。その後で、接続を開始します。コマンドライン クライアントまたはセッションを使用している場合：[localhost]# ssh username@IPHost のようなコマンドを使用してログインします。username はサーバーへの CLI アクセス権を持つ Cisco EPN Manager 管理者のユーザー ID で、 IPHost は Cisco EPN Manager サーバーまたはアプライアンスの IP アドレスまたはホスト名です。コンソールを使用している場合：管理者ユーザー名を入力するためのプロンプトが表示されます。ユーザー名を入力します。

Cisco EPN Manager により、入力した管理者 ID のパスワードを要求されます。

ステップ 3 管理 ID パスワードを入力します。Cisco EPN Manager によって次のようなコマンド プロンプトが表示されます。

```
Cisco_EPN_Manager_Server/admin#
```

ステップ 4 コマンドを入力するために **configure terminal** モードを開始する必要がある場合は、プロンプトで次のコマンドを入力します。

```
Cisco_EPN_Manager_Server/admin#configure terminal
```

プロンプトが `Cisco_EPN_Manager_Server/admin#` から `Cisco_EPN_Manager_Server/admin/conf#` に変わります。

Cisco EPN Manager サーバーの接続の保護

データ セキュリティのため、Cisco EPN Manager は、標準の公開キー暗号化方式と Public Key Infrastructure（PKI）を使用して送信中のデータを暗号化します。これらの技術に関する詳細情報は、インターネットから入手できます。Cisco EPN Manager は次の接続で交換されるデータを暗号化します。

- Web サーバーと Web クライアント間
- CLI クライアントと Cisco EPN Manager CLI シェル インターフェイス間（SSH で処理）
- Cisco EPN Manager、AAA のようなシステム、および外部ストレージ間

Web サーバーと Web クライアント間の通信を保護するには、HTTPS メカニズムの一部として組み込まれる公開キー暗号化サービスを使用します。そのためには、Cisco EPN Manager Web サーバーの公開キーを生成し、それをサーバーに保存して、Web クライアントと共有する必要があります。これは、標準 PKI 証明書のメカニズムを使用して実現できます。このメカニズムを使用することによって、Web サーバーの公開キーを Web クライアントと共有するだけでなく、アクセスする Web サーバー（URL）に公開キーが必ず属することが保証されます。これにより、第三者が Web サーバーと見せかけて、Web クライアントが Web サーバーに送信する機密情報を収集することを防ぎます。

以下のトピックでは、Web サーバーを保護するために実行できるその他の手順について説明します。

- シスコでは、Cisco EPN Manager Web サーバーは証明書ベースの認証を使用して、Web クライアントを認証するようお勧めします。このセキュリティを強化する手順については、次を参照してください。 Web クライアントの証明書ベースの認証の設定
- CLI クライアントと Cisco EPN Manager CLI インターフェイスの間の接続を保護するには、Cisco EPN Manager サーバーの強化のセキュリティを強化する手順を参照してください。
- Cisco EPN Manager、AAA などのシステム、および外部ストレージの間の接続を保護するには、Cisco EPN Manager ストレージの強化の推奨事項を参照してください。

Web サーバーの接続を保護する HTTPS のセットアップ

HTTPS 操作では、公開キー暗号化アルゴリズムを使用して生成されたサーバー キーおよびサーバー キーを使用して生成された信頼チェーン証明書が使用されます。これらの証明書は、Cisco EPN Manager Web サーバーに適用されます。証明書の生成方法によっては、ブラウザが Web サーバーに初めて接続したときにこれらの証明書を信頼するようにクライアント ブラウザに要

求することが必要になる場合があります。HTTPS メカニズムは、サーバー マシンのセキュリティを確保します（これにより、他のすべての関連システムのセキュリティが強化されます）。

署名エンティティ	説明	次を参照してください。
認証局（CA）署名付き証明書	認証局（CA）は、これらの証明書を生成し、発行します。証明書は、証明書で識別されるエンティティ（サーバー、デバイスなど）の名前に公開キーをバインドします。Cisco EPN Manager サーバーからの証明書署名要求（CSR）ファイルを生成し、（サーバー キーを含む）CSR ファイルを CA に送信する必要があります。証明書を受信したら、Web サーバーにこれらを適用します。 これらの証明書は、外部 CA または内部 CA によって生成される場合があります。 • 外部 CA：外部 CA 組織は、通常は有料でアイデンティティを検証し、証明書を発行します（一般的なブラウザは、通常、外部 CA 組織によって発行されたルート証明書と中間証明書を使用して事前にインストールされます）。 • 内部 CA：組織内の証明書生成サーバーを使用します（料金はかかりません）。内部 CA は、外部の有料 CA とまったく同じように機能します。 この方法は、次の場合に使用できます。 • HA を使用しない導入 • 仮想 IP アドレスを使用する HA 導入（ブラウザベース クライアント間の SSL 接続を含む） （注） 導入によっては、ブラウザまたは OS 証明書ストアに CA 署名付きルートおよび中間証明書をインストールするようにユーザーに指示することが必要になる場合があります。これが必要かどうかは、組織の IT 管理者に確認してください。手順については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。	CA 署名済み Web サーバー証明書の生成および適用 （5 ページ）

CA 署名済み Web サーバー証明書の生成および適用

次のトピックでは、CA 署名付き証明書の生成および Cisco EPN Manager Web サーバーへの適用方法について説明します。手順は、HA を使用した導入かどうか、および HA を使用した導入の場合は HA を仮想 IP アドレスとともに使用しているかどうかに応じて若干異なります。

ルートおよび中間 CA 証明書をブラウザまたは OS の証明書ストアにインストールするようユーザーに指示することが必要な場合があります。これが必要かどうかは、組織の IT 管理者に確

認してください。手順については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。

展開タイプ	手順の概要
HA なしの導入	HA なしの導入の場合、次のトピックの説明に従って、証明書を要求し、Web サーバーにインポートし、Web サーバーを再起動して証明書を適用する必要があります。 1. CA 署名付き Web サーバー証明書の要求 （6 ページ） 2. CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし （8 ページ）
仮想 IP アドレスを使用しないハイ アベイラビリティ導入	仮想 IP を使用しない HA 導入の場合、プライマリとセカンダリ サーバーに個別の証明書を要求し、各サーバーに適切な証明書をインポートする必要があります。証明書を適用するためにサーバーを再起動する場合は、特定の順序で再起動する必要があります。全体の手順については、次のトピックを参照してください。 1. CA 署名付き Web サーバー証明書の要求 （6 ページ） 2. CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合） （10 ページ）
仮想 IP アドレスを使用するハイ アベイラビリティ導入	仮想 IP を使用する HA 導入の場合、両方のサーバーに単一の証明書を要求する必要があります。サーバーの HA を削除し、両方のサーバーに証明書をインポートしてから、サーバーを再起動して証明書を適用する必要があります（サーバーは特定の順序で再起動する必要があります）。最後に、プライマリ サーバーにセカンダリ サーバーを登録することによって HA を再設定します。全体の手順については、次のトピックを参照してください。 1. CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合） （12 ページ） 2. プライマリ サーバーとセカンダリ サーバー間の HA の設定方法

CA 署名付き Web サーバー証明書の要求

展開環境で使用する CA 署名付き Web サーバー証明書を要求するには、次の手順に従います。次の条件に該当する場合にはこの手順を使用する必要があります。

- 展開環境で HA が使用されていない
- 展開環境で HA が使用されているが、仮想 IP アドレッシングが使用されていない（両方のサーバーで次の手順を実行する必要があります）

（注） 展開環境で HA と仮想 IP アドレスを使用している場合は、CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合） （12 ページ）の手順を使用します。

始める前に

ご使用のマシンで SCP が有効であり、すべての関連ポートが開いていることを確認します。これは、サーバーとの間でファイルをコピーするために必要です。

ステップ 1 Cisco EPN Manager サーバーの証明書署名要求（CSR）ファイルを生成します。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) 以下のコマンドを入力して、デフォルトのバックアップ リポジトリ（defaultRepo）に CSR ファイルを生成します。

```
ncs key genkey -newdn -csr CertName.csr repository defaultRepo
```

CertName は任意の名前です。

ステップ 2 Cisco EPN Manager サーバーからローカル マシンに CSR ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) Cisco EPN Manager サーバーからローカル マシンにファイルをコピーします。次に例を示します。

```
scp /localdisk/defaultRepo/CertName.csr clientUserName@clientIP:/destinationFolder
```

ステップ 3 任意の認証局に CSR ファイルを送信します。

（注） 認証用の CSR ファイルを生成して送信した後は、同じ Cisco EPN Manager サーバーで新しいキーを生成する際に **genkey** コマンドを使用しないでください。生成した場合、署名付き証明書ファイルをインポートしようとしたときに、ファイルと Cisco EPN Manager サーバーの間でキーが一致しないためにエラーが発生します。

CA は、デジタル署名付き証明書を *CertFilename*.**cer** という名前の 1 つのファイルまたは複数ファイルのセットとして送信します。

ステップ 4 （仮想 IP アドレスを使用しない HA 展開環境）セカンダリ サーバーでこの手順を繰り返します。

次のタスク

CA から証明書を受信した場合は、証明書をインポートして適用します。展開環境に応じて、次のいずれかの手順を使用します。

- CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし （8 ページ）
- CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合） （10 ページ）

CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし

このトピックでは、HA を使用しない展開環境に CA 署名付き Web サーバー証明書をインポートして適用する方法について説明します。

始める前に

- CA 署名付き証明書が必要です。証明書を受け取るまでは、次に示す手順は実行できません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 2 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにします。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 2 ローカル マシンから Cisco EPN Manager サーバーのバックアップ リポジトリに CER ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ファイルをローカル マシンから取得し、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

ステップ 3 Cisco EPN Manager CLI admin ユーザーとして CER ファイルをインポートします。

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

ステップ 4 この証明書をアクティブにするため、Cisco EPN Manager を再起動します。Cisco EPN Manager の停止と再起動 （23 ページ）を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。

CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし

このトピックでは、HA を使用しない展開環境に CA 署名付き Web サーバー証明書をインポートして適用する方法について説明します。

始める前に

- CA 署名付き証明書が必要です。証明書を受け取るまでは、次に示す手順は実行できません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 2 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにします。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 2 ローカル マシンから Cisco EPN Manager サーバーのバックアップ リポジトリに CER ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ファイルをローカル マシンから取得し、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

ステップ 3 Cisco EPN Manager CLI admin ユーザーとして CER ファイルをインポートします。

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

ステップ 4 この証明書をアクティブにするため、Cisco EPN Manager を再起動します。Cisco EPN Manager の停止と再起動 （23 ページ）を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。

CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合）

このトピックでは、仮想 IP アドレスを使用しない HA 展開に CA 署名付き Web サーバー証明書をインポートして適用する方法を説明します（HA 展開で仮想 IP を使用している場合は、CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合） （12 ページ）を参照してください）。この手順は HA を使用する展開での手順と同様ですが、プライマリ サーバーとセカンダリ サーバーの両方で手順を実行しなければならないという点が異なります。

（注） サーバーは特定のシーケンスで再起動する必要があるため、サーバーを再起動するときは、以下の手順に忠実に従ってください。

始める前に

- CA 署名付き証明書が必要です。各サーバーの証明書を受信するまでは、以下の手順を実行することはできません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 プライマリ サーバーにプライマリ証明書をインポートします。

a) CA から受け取った CER ファイルが 1 つだけである場合は、ステップ 1(b) に進みます。 複数の（チェーン）証明書を受け取った場合は、それらの証明書を 1 つの CER ファイルに結合（連結）します。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

1. テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

2. この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

b) Cisco EPN Manager CLI 管理ユーザーとしてプライマリ Cisco EPN Manager サーバーにログインします。

c) ローカル マシンから CER ファイルを取得して、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

scp *clientUserName@clientIP:/fullPathToCERfile* **/localdisk/defaultRepo**

ステップ 2 セカンダリ サーバーで上記の手順を行います。

ステップ 3 セカンダリ サーバーで、CER ファイルをインポートします。

a) Cisco EPN Manager CLI 管理ユーザーとしてログインし、サーバーを停止します。

ncs stop

b) セカンダリ サーバーが停止していることを確認します。

c) CER ファイルをインポートします。

ncs key importsignedcert *CertFilename*.**cer repository** *RepoName*

（注） ステップ 5 に到達するまでは、セカンダリ サーバーを再起動しないでください。

ステップ 4 プライマリ サーバーで、CER ファイルをインポートします。

a) Cisco EPN Manager CLI 管理ユーザーとしてログインし、サーバーを停止します。

ncs stop

b) プライマリ サーバーが停止していることを確認します。

c) CER ファイルをインポートします。

ncs key importsignedcert *CertFilename*.**cer repository** *RepoName*

（注） ステップ 6 に到達するまでは、プライマリ サーバーを再起動しないでください。

ステップ 5 セカンダリ サーバーで、次のコマンドを実行します。

a) **ncs start** コマンドを実行してサーバーを再起動します。

b) セカンダリ サーバーが再起動したことを確認します。

c) **ncs status** コマンドを実行し、セカンダリ サーバーの HA ステータスが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] であることを確認します。

ステップ 6 プライマリ サーバーで、次のコマンドを実行します。

a) **ncs start** コマンドを実行してサーバーを再起動します。

b) プライマリ サーバーが再起動したことを確認します。

c) **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開していることを確認します。

プライマリ サーバーですべてのプロセスが稼働したら、セカンダリ サーバーとプライマリ サーバーの間で HA 登録が自動的にトリガーされます（また、登録されている電子メール アドレスに電子メールが送信されます）。自動 HA 登録は通常、数分で完了します。

ステップ 7 プライマリ サーバーとセカンダリ サーバーで **ncs ha status** コマンドを実行し、両方のサーバーの HA ステータスを確認します。次が表示されます。

- プライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）] です。
- セカンダリ サーバーの状態は [セカンダリ同期（Secondary Syncing）] です。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。

CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合）

仮想 IP アドレスを使用したハイ アベイラビリティ展開を使用している場合でも、証明書を要求する必要があるのは 1 回だけです。CA から証明書を受け取ったら、プライマリ サーバーとセカンダリ サーバーの両方にその同じ証明書をインストールします。この点が、IP アドレスを使用しない HA 展開との違いです。IP アドレスを使用しない HA 展開では、2 つの証明書要求を行って、一方の証明書をプライマリ サーバーにインストールし、もう一方の（異なる）証明書をセカンダリ サーバーにインストールします。

仮想 IP および HA の詳細については、次を参照してください。 HA での仮想 IP アドレッシングの使用

始める前に

ご使用のマシンで SCP が有効であり、すべての関連ポートが開いていることを確認します。これは、サーバーとの間でファイルをコピーするために必要です。

ステップ 1 1 つの CSR ファイルおよび秘密キーをプライマリ サーバーとセカンダリ サーバー用に生成します。秘密キーを両方のサーバーにインストールし、CSR ファイルを任意の認証局に送信します。次の例では、Linux で openssl を使用して、これらのファイルを作成する方法を説明しています。

a) デフォルトのバックアップ リポジトリで CSR ファイルを生成します。

```
openssl req -newkey rsa:2048 -nodes -keyout ServerKeyFileName -out CSRFileName -config
opensslCSRconfigFileName
```

引数の説明

- *ServerKeyFileName* は、秘密キー ファイルに使用するファイル名です。
- *CSRFileName* は、CA に送信する CSR 要求ファイルに使用するファイル名です。
- *openssl CSRconfigFileName* は、CSR ファイルを生成するために使用した openssl 設定が含まれるファイルの名前です。

b) テキスト エディタを使用して、openssl 設定が含まれるファイル（(a) の *openssl CSRconfigFileName*）を編集し、次のような内容にします。

```
[req]
 distinguished_name = req_distinguished_name
 req_extensions = v3_req

 [req_distinguished_name]
 countryName = Country
 countryName_default = US
 stateOrProvinceName = State
 stateOrProvinceName_default = CA
 localityName = City
 localityName_default = San Jose
 organizationName = Organization
 organizationName_default = Cisco Systems
 organizationalUnitName = Organizational Unit
 organizationalUnitName_default = CSG
 commonName = Common Name
 commonName_default = example.cisco.com
 commonName_max = 64

 [ v3_req ]
 # Extensions to add to a certificate request
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = @alt_names

 [alt_names]
 DNS.1 = example.cisco.com
 DNS.2 = example-pri.cisco.com
 DNS.3 = example-sec.cisco.com
 IP.1 = 209.165.200.224
 IP.2 = 209.165.200.225
 IP.3 = 209.165.200.226
```

この例では、次のようになります。

- 仮想 IP アドレスは 209.165.200.224 です。FQDN は **example.cisco.com** です。FQDN は、DNS サーバー名にも使用されます。
- プライマリ サーバーの IP アドレスは 209.165.200.225 です。そのホスト名は **example-pri** です。/etc/hosts およびその他のホスト名設定ファイルに、このホスト名を含める必要があります。
- セカンダリ サーバーの IP アドレスは 209.165.200.226 です。そのホスト名は **example-sec** です。

ステップ 2 任意の認証局に CSR ファイルを送信します。CA は、デジタル署名付き証明書を *CertFilename*.**cer** という名前の 1 つのファイルまたは複数ファイルのセットとして送信します。

ステップ 3 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 4 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにしま

す。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 4 プライマリ サーバーで、CER ファイルを各サーバー上のバックアップ リポジトリにコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ローカル マシンからファイルを取得して、サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

ステップ 5 セカンダリ サーバーで上記の手順を繰り返します。

ステップ 6 プライマリ サーバーで、Cisco EPN Manager CLI admin ユーザーとして HA 設定を削除します。

```
ncs ha remove
```

ncs ha status を実行して HA 設定が削除されていることを確認してから、次のステップに進んでください。

（注） HA が未割り当ての場合は、TOFU 証明書を手動で削除する必要があります。詳細については、任意の状態の TOFU エラーの解決を参照してください。

ステップ 7 プライマリ サーバーとセカンダリ サーバーの両方で、CER ファイルをインポートします。

```
ncs key importkey ServerKeyFileNameCertFilename.cer repository RepoName
```

ステップ 8 プライマリ サーバーとセカンダリ サーバーを再起動します。プライマリ サーバーとセカンダリ サーバーはまだ HA ペアとして設定されていないため、順番は重要ではありません。Cisco EPN Manager の停止と再起動 （23 ページ）を参照してください。

（注） サーバーが再起動しない場合、（インポート操作は成功したように見えても）連結した証明書ファイルではなく、誤って個々の証明書をインポートした可能性があります。この問題を解決するには、（正しい）連結された証明書ファイルを使用してインポート操作を繰り返してください。

ステップ 9 プライマリ サーバーとセカンダリ サーバーで **ncs status** コマンドを実行し、両方のサーバーのステータスを確認します。

ステップ 10 セカンダリ サーバーをプライマリ サーバーに HA 用に登録します。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （15 ページ）を参照してください。

ブラウザ/*OS* 信頼ストアに *CA* 署名付きルート証明書と中間証明書を追加する

ユーザーがブラウザまたは OS の証明書ストアに CA ルート証明書と中間 CA 証明書をインストールする必要があるかどうかを組織の IT 管理者に確認します。証明書のインストールが必要な状況で証明書がインストールされていないと、ユーザーのブラウザにブラウザが信頼されていないことを示す通知が表示されます。

ブラウザのタイプやバージョンによっては、以下の手順の細かい部分が多少異なる可能性があります。

始める前に

Internet Explorer ブラウザに証明書を追加する場合、クライアント マシンの管理者権限が必要になります。

ステップ 1 Firefox のブラウザでは、次の手順に従って、証明書をインポートします。

a) **[ツール（Tools）]**>**[オプション（Options）]** の順に選択し、左側のオプションから [詳細（Advanced）] をクリックします。
b) ウィンドウ上部にあるリストから [証明書（Certificates）] をクリックしてから、[証明書を表示（View Certificates）] をクリックします。この操作によって、ブラウザの [証明書マネージャ（Certificate Manager）] ダイアログボックスが開きます。
c) [証明書マネージャ（Certificate Manager）] ダイアログボックスで、[認証局（Authorities）] タブをクリックし、ダイアログの下部にある [インポート（Import）] をクリックします。
d) [...ファイルを選択してください（Select File...）] ダイアログボックスで、CA 署名付きルート証明書ファイルを参照し、[開く（Open）] をクリックします。
e) ファイルをインポートします。
f) CA 署名付き中間証明書ファイルについて、インポート手順を繰り返します。

ステップ 2 Internet Explorer ブラウザでは、Microsoft の証明書マネージャ ツールを使用して、証明書をインポートします。このツールを使用するには、ユーザーにクライアント マシンの管理者権限がなければなりません。

a) Windows 7 では、[スタート（Start）] をクリックします。
b) 検索テキスト ボックスに「certmgr.msc」と入力し、Enter キーを押します。
c) 検索結果のプログラムのアイコンをクリックすると、Microsoft 証明書マネージャが起動します。

d) 証明書マネージャの GUI の左側の列で、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。
e) [証明書（Certificates）] を右クリックし、**[すべてのタスク（All Tasks）] > [インポート（Import）]** を選択します。
f) [次に（Next）] をクリックし、CA 署名付きルート証明書ファイルを参照し、インポートします。
g) CA 署名付き中間証明書ファイルについてインポート手順を繰り返します。ただし、証明書をインポートする最初の手順として [中間証明書機関（Intermediate Certification Authorities）] を選択します。

（注） CA 署名付き証明書がインストールされていない場合、Cisco EPN Manager はアラートを表示します。

HTTPS サーバー ポートの変更

多くのデバイスで設定情報のリレーに HTTPS が使用されるため、Cisco EPN Manager では HTTPS がデフォルトで有効になっています（HTTP は Cisco EPN Manager で使用されないため、デフォルトでは無効になっています）。必要に応じて、次の手順に従って HTTPS サーバーのポートを変更できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[一般（General）] > [サーバー（Server）]** を選択します。
ステップ 2 [HTTPS] 領域に新しいポート番号を入力し、[保存（Save）] をクリックします。
ステップ 3 Cisco EPN Manager を再起動し、変更を適用します。Cisco EPN Manager の停止と再起動 （23 ページ） を参照してください。

証明書の検証設定

TLS/HTTPS 接続のようなセキュアなトランザクション時のユーザー認証（証明書ベースの認証が有効になっている場合）では、Cisco EPNM は外部エンティティから証明書を受信します。Cisco EPNM はこれらの証明書を検証して証明書の整合性と証明書の所有者のアイデンティティを確認する必要があります。証明書の検証機能により、ユーザーは他のエンティティから受信した証明書を検証する方法を制御できます。

証明書の検証が適用されると、他のエンティティから受信した証明書は、その証明書が Cisco EPNM によって信頼されている認証局（CA）が署名している場合にのみ、Cisco EPNM によって受け入れられます。信頼ストアは、ユーザーが信頼できる CA 証明書を維持できる場所です。署名付き証明書チェーンが信頼ストア内のいずれかの CA 証明書がルートでない場合、検証は失敗します。

信頼ストアの管理

ユーザーは信頼ストア内の信頼できる CA を管理できます。Cisco EPNM は、さまざまな信頼ストア、つまり、pubnet、system、devicemgmt、および user を提供します。

- pubnet：パブリックネットワーク内のサーバーに接続したときにリモートホストから受信した証明書の検証中に使用されます。
- system：ネットワーク内のシステムに接続したときにリモートシステムから受信した証明書の検証中に使用されます。
- devicemgmt：管理対象デバイスから受信した証明書の検証中に使用されます。
- user：ユーザー証明書の検証に使用されます（証明書ベースの認証が有効になっている場合）。

信頼ストアを管理する *CLI*

次に、信頼ストアを管理するために使用される CLI を示します。

- 信頼ストアへの CA 証明書のインポート （17 ページ）
- 信頼ストアでの CA 証明書の表示 （17 ページ）
- 信頼ストアからの CA 証明書の削除 （17 ページ）

信頼ストアへの CA 証明書のインポート

次に、信頼ストアに CA 証明書をインポートするコマンドを示します。

```
ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository
<Repository-name><certificate-file> truststore {devicemgmt | pubnet |
system | user}
```

信頼ストアでの CA 証明書の表示

次に、信頼ストアで CA 証明書を表示するコマンドを示します。

```
ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt
| pubnet | system | user}
```

信頼ストアからの CA 証明書の削除

次に、信頼ストアから CA 証明書を削除するコマンドを示します。

```
ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore
{devicemgmt | pubnet | system | user}
```

Cisco EPN Manager サーバーとの SSH セッションの確立

サーバーに接続するときには、admin ユーザーとして SSH を使用してログインします。（詳細については、ユーザー インターフェイス、ユーザー タイプ、およびそれらの間の遷移を参照してください）。

ステップ 1 SSH セッションを開き、Cisco EPN Manager admin ユーザーとしてログインします。

- コマンド ラインから次のように入力します。*server-ip* は Cisco EPN Manager です。

```
ssh admin server-ip
```

- SSH クライアントを開き、**admin** としてログインします。

（注） ユーザーは、SSH または PuTTY に接続する新しいアルゴリズムを作成してカスタマイズできるようになりました。

ステップ 2 admin パスワードを入力します。プロンプトが次のように変化します。

```
(admin)
```

管理ユーザーが実行できる操作のリストを表示するには、プロンプトで **?** と入力します。

admin コンフィギュレーション モードを開始するには、次のコマンドを入力します（プロンプトの変化に注意してください）。

```
(admin) configure terminal
(config)
```

サーバーでの NTP の設定

Network Time Protocol（NTP）は、ネットワーク内のすべてのデバイスと Cisco EPN Manager サーバーで正しく同期される必要があります。ネットワーク全体の NTP 同期の管理で障害が発生した場合、Cisco EPN Manager で異常な結果が発生する可能性があります。これには、Cisco EPN Manager バックアップに使用する任意のリモート FTP サーバー、セカンダリ Cisco EPN Manager 高可用性サーバーなど、すべての Cisco EPN Manager 関連サーバーが含まれます。

Cisco EPN Manager サーバーのインストール時にデフォルトおよびセカンダリの NTP サーバーを指定します。また、Cisco EPN Manager の **ntp server** コマンドを使用して、インストール後に NTP サーバーのリストを追加または変更することもできます。

（注） Cisco EPN Manager は NTP サーバーとして設定できません。NTP クライアントとしてだけ機能します。最大 5 台の NTP サーバーを設定できます。

ステップ 1 Cisco EPN Manager サーバーに管理者ユーザーとしてログインし、コンフィギュレーション モードを開始します。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）を参照してください。

ステップ 2 次の方法のいずれかのコマンドを使用して、NTP サーバーを設定します。

認証されていない NTP サーバーのセットアップの場合：

```
ntp server ntp-server-IP
```

認証済み NTP サーバーのセットアップの場合：

```
ntp server ntp-server-IP ntp-key-id ntp-type password
```

ここで、

- *ntp server IP* は、Cisco EPN Manager サーバーにクロック同期を提供するサーバーの IP アドレスまたはホスト名です
- *ntp-key-id* は、認証済み NTP サーバーの MD5 キー ID MD5 キーです。
- *ntp-type* は、プレーンまたはハッシュのいずれかにすることができます。
- *password* は NTPv4 サーバーの MD5 プレーン テキスト パスワードです。

Cisco EPN Manager プロキシ サーバーの設定

サーバーのプロキシと、そのローカル認証サーバー（設定されている場合）のプロキシを設定するには、次の手順に従います。ネットワークとインターネットの間のセキュリティバリアとしてプロキシ サーバーを使用する場合、次の手順に従ってプロキシを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [プロキシ（Proxy）] タブをクリックします。

ステップ 3 [プロキシの有効化（Enable Proxy）] チェックボックスをオンにし、Cisco.com に接続してプロキシとして機能するサーバーに関する必須情報を入力します。

ステップ 4 [認証プロキシ（Authentication Proxy）] チェックボックスをオンにし、プロキシ サーバーのユーザー名とパスワードを入力します。

ステップ 5 [接続のテスト（Test Connectivity）] をクリックして、プロキシ サーバーに接続できることを確認します。

ステップ 6 [保存（Save）] をクリックします。

SMTP 電子メール サーバーの設定

Cisco EPN Manager で（アラーム、ジョブ、レポートなどの）電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メール サーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[メールと通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** を選択します。

ステップ 2 [プライマリ SMTP サーバー（Primary SMTP Server）] で、Cisco EPN Manager が使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力し、プライマリ SMTP サーバーのホスト名を入力します。

（注） 仮想 IP アドレスを [ホスト名/IP（Hostname/IP）] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 3 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。SMTP サーバーのユーザー名とパスワード。

ステップ 4 [送信者および受信者（Sender and Receivers）] で、Cisco EPN Manager の正当なメール アドレスを入力します。

ステップ 5 完了したら、[保存（Save）] をクリックします。

サーバーでの FTP/TFTP/SFTP サービスの有効化

FTP/TFTP/SFTP は、デバイス設定およびソフトウェア イメージ ファイルの管理のために、サーバーとデバイスの間でファイルを転送する目的で使用されます。また、これらのプロトコルは、高可用性導入環境において、セカンダリ サーバーにファイルを転送するためにも使用されます。これらのサービスは、通常はデフォルトで有効になっています。FIPS モードで Cisco EPN Manager をインストールした場合、これらはデフォルトで無効になります。このページを使用してこれらのサービスを有効にすると、Cisco EPN Manager は FIPS に準拠しなくなります。

SFTP は、セキュリティで保護されたバージョンのファイル転送サービスです。デフォルトでこれが使用されます。FTP は、セキュリティで保護されていないファイル転送サービス バージョンです。TFTP は、セキュリティで保護されていない、単純なサービス バージョンです。FTP または TFTP のいずれかを使用するには、サーバーの追加後にサービスを有効化する必要があります。

FTP/TFTP/SFTP パスワードを変更するには、FTP ユーザー パスワードの変更 （24 ページ）を参照してください。

ステップ 1 FTP、TFTP、または SFTP サーバーを使用するように Cisco EPN Manager を設定します。

a) **[管理（Administration）] > [サーバー（Servers）] > [TFTP/FTP/SFTP サーバー（TFTP/FTP/SFTP Servers）]** を選択します。

b) [コマンドの選択（Select a command）] ドロップダウン リストから、[TFTP/FTP/SFTP サーバーの追加（Add TFTP/FTP/SFTP Server）] を選択し、[移動（Go）] をクリックします。

- **[サーバータイプ（Server Type）]** ドロップダウンリストから、**[FTP]**、**[TFTP]**、**[SFTP]**、または **[すべて（All）]** を選択します。
- サーバーのユーザー定義名を入力します。
- サーバーの IP アドレスを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 FTP または TFTP を使用する場合には、Cisco EPN Manager サーバーでそれを有効化します。

a) **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[サーバー（Server）]** を選択します。
b) [FTP] または [TFTP] エリアに移動します。
c) [有効（Enable）] をクリックします。
d) **[保存（Save）]** をクリックします。

ステップ 3 Cisco EPN Manager を再起動し、変更を適用します。Cisco EPN Manager の停止と再起動 （23 ページ） を参照してください。

（注） [ハイアベイラビリティ設定（High Availability setup）] では、FTP または TFTP サービスがプライマリサーバーで有効になっている場合は、ハイアベイラビリティを設定する前にセカンダリサーバーでも有効にする必要があります。これは、コンフィギュレーションファイルを編集し、変更を適用するためにサーバーを再起動することで、セカンダリサーバーで手動で実行する必要があります。

セカンダリサーバーで実行する必要があるステップを次に示します。

- セカンダリサーバーで FTP または TFTP を有効にするには、次のようにします。
  1. 次のプロパティを `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml` ファイルで値を「**true**」に設定します。
     - <entry key="FtpEnable">true</entry>
     - <entry key="TftpEnable">true</entry>
  2. Cisco EPN Manager セカンダリサーバーを再起動します。
- セカンダリサーバーで FTP または TFTP を無効にするには、次の手順を実行します。
  1. 次のプロパティを `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml` ファイルで値「**false**」に設定します。
     - <entry key="FtpEnable">false</entry>
     - <entry key="TftpEnable">false</entry>
  2. Cisco EPN Manager セカンダリサーバーを再起動します。

ログイン バナー（ログインの免責事項）の作成

すべてのユーザーに対してログイン前に表示するメッセージがある場合は、ログインの免責事項を作成します。テキストは GUI クライアント ログイン ページのログイン フィールドとパスワード フィールドの下に表示されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** を選択します。

ステップ 2 ログインの免責事項テキストを入力（または編集）します。

（注） 改行文字は無視されます。

変更はすぐに反映されます。

Cisco EPN Manager の停止と再起動

Cisco EPN Manager製品ソフトウェアのアップグレード、ログファイルの設定変更、セキュアポート設定のハンギング、レポートファイルの圧縮、サービス検出設定の変更、LDAP 設定の構成の後などに、再起動が必要です。Cisco EPN Manager サーバーを停止すると、すべてのユーザー セッションが終了します。

サーバーを停止するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs stop
```

サーバーを再起動するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs start
```

ネットワーク要素との通信に適用するグローバル SNMP の設定

[SNMP の設定（SNMP Settings）] ページは、サーバーが SNMP を使用してデバイスにアクセスおよびモニターする方法を制御します。これらの設定によって、デバイスが到達不能であると判断される条件が決まります。このページで行う変更はグローバルに適用され、再起動されても、バックアップと復旧が行われても保存された状態に維持されます。

（注） デフォルトのネットワーク アドレスは 0.0.0.0 です。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[ネットワークとデバイス（Network and Device）] > [SNMP]** を選択します。

ステップ 2 （任意）SNMP を使用して取得されたメディエーション トレース レベル ログのデータ値を表示するには、[トレース表示値（Trace Display Values）] チェックボックスをオンにします。

ステップ 3 [バックオフ アルゴリズム（Backoff Algorithm）] ドロップダウン リストからアルゴリズムを選択します。

- [指数（Exponential）]：SNMP の初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。

- [一定（Constant）]：SNMP の試行時に、毎回同じ待機時間（タイムアウト）が適用されます。このオプションは、必要な再試行回数が多い、不安定なネットワークで役立ちます。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 4 [到達可能性再試行回数（Reachability Retries）] と [到達可能性タイムアウト（Reachability Timeout）] のグローバル値を設定する場合は、[到達可能性パラメータを使用（Use Reachability Parameters）] チェックボックスをオンにします。このオプションを選択すると、Cisco EPN Manager はデフォルトでここで設定された値になります。

（注） [到達可能性パラメータを使用（Use Reachability Parameters）] チェックボックスがオンになっていない場合、Cisco EPN Manager はデバイスで指定されているタイムアウトと再試行回数を使用します。

- [到達可能性再試行回数（Reachability Retries）]：デバイスの到達可能性を判別するにはグローバル再試行回数を入力します。

  このフィールドは、[到達可能性パラメータを使用（Use Reachability Parameters）] チェック ボックスをオンにした場合にのみ編集できます。スイッチポートトレースが完了するまでに長い時間がかかる場合は、[到達可能性再試行回数（Reachability Retries）] の値を小さくします。

- [到達可能性タイムアウト（Reachability Timeout）]：デフォルト値は 2 秒です。このフィールドは編集できません。

ステップ 5 [PDU取得ごとの最大変数バインド（Maximum VarBinds per Get PDU）] フィールドおよび [PDU設定ごとの最大変数バインド（Maximum VarBinds per Set PDU）] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。これらのフィールドを使用することで、SNMP に関連した障害が発生したときに、必要な変更を加えることができます。ネットワークでの PDU フラグメンテーションに問題がある場合は、この数を 50 に減らすと、通常はフラグメンテーションが解消されます。

ステップ 6 必要に応じて [テーブルごとの最大行数（Maximum Rows per Table）] の値を調整します。

ステップ 7 [保存（Save）] をクリックします。

管理パスワードの管理

FTP ユーザー パスワードの変更

Cisco EPN Manager では、FTP を使用して他のサーバーにアクセスするために、ID として **ftp-user** を使用します。管理権限を持つユーザーは、FTP パスワードを変更できます。

ステップ 1 admin ユーザーとして Cisco EPN Manager サーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）。

ステップ 2 Cisco EPN Manager サーバーの FTP パスワードを変更するには、次のように入力します。

ncs password ftpuser *username* **password** *password*

例

```
(admin) ncs password ftpuser FTPuser password FTPUserPassword
Initializing...
Updating FTP password.
This may take a few minutes.
Successfully updated location ftpuser
```

Web GUI ルート ユーザー パスワードの変更

Cisco EPN Manager は**ルート** ID を使用して、Web GUI へのルート アクセス権が必要な特別なタスクを実行します

始める前に

Web GUI ルート ユーザー パスワードを変更するには、現在のパスワードを知っている必要があります。

ステップ 1 **ルート** ユーザーとして Cisco EPN Manager 管理 CLI にログインします（管理 CLI の詳細については、ユーザー インターフェイスとユーザー タイプを参照してください）。

ステップ 2 次のコマンドを入力します（*newpassword* は新しい Web GUI ルート パスワードです）。

ncs password root password *newpassword*

（注） 入力する新しいパスワードは、現在のパスワードポリシーに従う必要があります。詳細については、ローカル認証のためのグローバル パスワード ポリシーの設定を参照してください。

例

```
ncs password root password NewWebGUIRootPassword
Password updated for web root password
```

仮想アプライアンスの管理者パスワードの回復

このトピックでは、Cisco EPN Manager 仮想マシン（別名 OVA）の管理パスワードを回復してリセットする方法を説明します。

はじめる前に

次の条件が満たされていることを確認します。

- Cisco EPN Manager サーバーに対する物理アクセス。
- ソフトウェアのバージョンに適切なインストール ISO イメージのコピー。

- VMware vSphere クライアントへのアクセスと、vSphere インベントリ、データストア、およびオブジェクトの各機能へのアクセス。このようなアクセスがない場合は、VMware 管理者にお問い合わせください。vSphere クライアントから ESX に直接アクセスしないでください。

ステップ 1 Cisco EPN Manager OVA サーバーで、VMware vSphere クライアントを起動します。

ステップ 2 次のように、OVA 仮想マシン上のデータストアにインストール ISO イメージをアップロードします。

a) vSphere インベントリで、[**Datastores**] をクリックします。
b) [**Objects**] タブで、ファイルをアップロードするデータストアを選択します。
c) **Navigate to the datastore file browser**アイコンをクリックします。
d) 必要に応じて、[**Create a new folder**] アイコンをクリックして新しいフォルダを作成します。
e) 作成したフォルダを選択するか、既存のフォルダを選択して、[**Upload a File**] アイコンをクリックします。

[クライアント統合アクセス制御（Client Integration Access Control）] ダイアログ ボックスが表示されたら、[**Allow**] をクリックしてプラグインからオペレーティング システムにアクセスできるようにし、ファイルのアップロードに進みます。

f) ローカル コンピュータで、ISO ファイルを検索して、そのファイルをアップロードします。
g) データストア ファイル ブラウザを更新して、アップロードされたファイルを一覧表示します。

ステップ 3 ISO イメージがデータストアにアップロードされたら、次のように、それをデフォルトのブート イメージにします。

a) VMware vSphere クライアントを使用して、導入済みの OVA を右クリックして **Power > Shut down guest** を選択します。
b) **[Edit] [Settings] [>] [Hardware]** を選択してから、**[CD/DVD] [drive] [1]** を選択します。
c) [**Device Type**] で [**Datastore ISO File**] を選択してから、[**Browse**] ボタンを使用して、データストアにアップロードした ISO イメージ ファイルを選択します。
d) **[Device] [Status,]** で **[Connect] [at] [power] [on]** を選択します。
e) [**Options**] タブをクリックして [**Boot Options**] を選択します。[**Force BIOS Setup**] で、**Next time VM boots, force entry into BIOS setup Screen** を選択します。これにより、仮想マシンを再起動すると、仮想マシンの BIOS からブートが開始されます。
f) **OK** をクリックします。
g) VMware vSphere クライアントで、導入済みの OVA を右クリックして **Power > Power On** を選択します。
h) BIOS セットアップ メニューでデバイスのブート順序を制御するオプションを探して、**DVD/CDROM** を一番上に移動します。

ステップ 4 次の手順に従って、サーバー管理者パスワードをリセットします。

a) BIOS 設定を保存して、BIOS セットアップ メニューを終了します。仮想マシンが ISO イメージからブートし、ブート オプションのリストが表示されます。
b) キーボードとモニターを使用して OVA にアクセスしている場合は **3**、コマンド ラインまたはコンソール経由でアクセスしている場合は **4** を入力します。vSphere クライアントに、管理者ユーザー名のリストが表示されます。

c) パスワードをリセットする管理者ユーザー名の横に表示された番号を入力します。
d) 新しいパスワードを入力し、2 回目の入力でそれを確認します。
e) **Y** と入力し、変更を保存してリブートします。
f) 仮想マシンがリブートしたら、vSphere クライアントを使用して、CD アイコンをクリックし、[**Disconnect ISO image**] を選択します。

ステップ 5 新しい管理パスワードを使ってログインします。

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

システム監視ダッシュボードは、Cisco EPN Manager サーバーの設定とパフォーマンスに関する情報を提供します。ダッシュボードにアクセスするには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します（ユーザー ID がこのダッシュボードにアクセスするための管理者権限を持っている必要があります）。[概要（Overview）] タブや[パフォーマンス（Performance）] タブに表示されるダッシュレットをカスタマイズするには、事前定義のダッシュレットをダッシュボードに追加するに記載された手順に従ってください。

[Dashboard] タブ	説明
概要	バックアップおよびデータ消去ジョブ、Cisco EPN Manager システム アラーム、およびサーバー CPU、ディスク、メモリの使用状況統計。この情報をチェックするために別々の時間枠を指定できます。 サーバー タイム、カーネル バージョン、オペレーティング システム、ハードウェア情報などを表示するには、ダッシュボードの左上にある [システム情報（System Information）] をクリックして、その情報を含むフィールドを開きます。 [概要（Overview）] ダッシュボードからダッシュレットを追加または削除できます。
パフォーマンス	サーバーの syslog とトラップ、および入出力。[パフォーマンス（Performance）] ダッシュボードから、このデータの異なる時間枠を指定したり、ダッシュレットを追加または削除したりできます。

[管理者（Admin）]	• [状況（Health）]：システム アラーム、実行中のジョブの数、ログインしたユーザーの数、およびデータベースの使用状況の分布。履歴情報の異なる時間枠を指定できます。 • [API ヘルス（API Health）]：すべての API サービスとともにそれらの応答時間統計を一覧表示します。 • [サービスの詳細（Service Details）]：特定のサービスの統計（応答カウントと時間傾向）、クライアントあたりのコール数（クライアントはIPアドレスで識別されます）。チェックするサービスを選択できます。

Cisco EPN Manager サーバーのパフォーマンスの改善

OVA サイズの確認

Cisco EPN Manager が、ご利用のシステム リソース、またはインストールした OVA のサイズに推奨されるデバイス/インターフェイス/フロー数の 80% 以上を使用している場合、パフォーマンスに悪影響が及ぶ可能性があります。インストール マニュアルで指定されているデバイス、インターフェイス、およびフロー レコードの推奨値を OVA が超えていないことを確認します。これらの推奨値は、指定されている各 OVA サイズの最大値です。管理ダッシュボードでこれらを確認できます（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 （27 ページ）を参照）。容量の問題に対処するには、サーバーのディスク容量に関する問題の管理 （29ページ）を参照してください。

データベースの圧縮

ステップ 1 admin ユーザーとして サーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）。

ステップ 2 次のコマンドを入力して、アプリケーション データベースを圧縮します。

```
(admin)# ncs cleanup
```

ステップ 3 プロンプトが表示されたら、ディープ クリーンアップ オプションに対し **[Yes]** を選択します。

サーバーのディスク容量に関する問題の管理

Cisco EPN Manager は、サーバーのディスク容量が少なくなると、次のしきい値でアラームをトリガーします。

- 60% の使用率でメジャー アラームをトリガーする
- 65% の使用率でクリティカル アラームをトリガーする

アラートを受信した場合は、次のアクションを実行することを検討してください。

- データベースの圧縮 （28 ページ）の説明に従って、既存のデータベース領域を解放します。
- バックアップをローカル リポジトリに保存する場合は、リモート バックアップ リポジトリの使用を検討してください。「NFS ベースのリモート リポジトリの設定」を参照してください。
- データの収集と消去の説明に従って、ネットワーク インベントリ、パフォーマンス、レポート、その他のクラスのデータの保持期間を短縮します。
- ディスク容量を追加します。VMware OVA テクノロジーを使用すれば、簡単に既存のサーバーのディスク容量を増やすことができます。物理ディスク容量を拡張する場合は、Cisco EPN Manager サーバーをシャット ダウンしてから、VMware 指定の手順を実行する必要があります。仮想アプライアンスを再起動すると、Cisco EPN Manager は追加されたディスク容量を自動的に利用します（データの収集と消去を参照）。
- 1 レベル上の OVA の RAM、ディスク容量、およびプロセッサの最小要件を満たす新しいサーバーをセットアップします。既存のシステムをバックアップして、より高いレベルのサーバー上の仮想マシンに復元します。

ネットワークチーム（リンク集約）の設定

Cisco EPN Manager では、冗長性を維持するために NIC チーミングを作成できます。これにより、1 つの IP アドレスを持つ 1 つの論理インターフェイスに最大 256 の物理インターフェイスをバインドできます。これは、いずれかのインターフェイスがダウンした場合でも接続が中断されないことを意味します。論理インターフェイスでは、通常のインターフェイス操作を実行できます。

（注） チーミングは、NBI に使用される Eth 0/Gigabitethernet 0 ポートではサポートされません。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 論理インターフェイスを設定してから、コンフィギュレーション モードを終了します。

```
config# interface interfaceName
config-InterfaceName# ip addressIP_addresssubnet_mask
config-InterfaceName# member interface1
config-InterfaceName# member interface2
config-InterfaceName# exit
config# exit
```

ここで、

- *interfaceName* には、論理インターフェイスの名前（Team0 など）を指定します。
- *IP_address*、*subnet_mask* には、論理インターフェイスに割り当てる IP アドレスとサブネットマスクを指定します。
- *interface1*、*interface2* には、論理インターフェイスにバインドする物理インターフェイスの名前（GigabitEthernet 1、GigabitEthernet 2 など）を指定します。

ステップ 4 論理インターフェイスの作成を確認します。

```
show interface interfaceName
```

ネットワークトラフィックをフィルタ処理するための IP アクセスリストの作成または変更

Cisco EPN Manager は、*default* という名前の事前設定されたデフォルト IP アクセスリストを維持します。このリストは変更できませんが、NIC に割り当てたり、割り当てを解除することができます。

新しい IP アクセスリストを作成するか変更して、Cisco EPN Manager への入力ネットワークトラフィックをフィルタ処理できます。デフォルトの動作では、IP アクセスリストで明示的に指定されていない限り、ネットワークトラフィックはブロックされます。新しい IP アクセスリストを作成するには、次の手順を実行します。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 ポートおよびプロトコルの情報を指定して IP アクセスリストを作成してから、コンフィギュレーション モードを終了します。

```
config-InterfaceName# ip access-list listname
config-ACL-listname# permit protocol1 port1
config-ACL-listname# permit protocol2 port2
config-ACL-listname# exit
config# exit
```

ここで、

- *listname*：新しい IP アクセスリストの名前（test_acl など）。
- **permit**：ネットワークトラフィックをルーティングするためのプロトコルとポートの情報を追加するコマンド。

（注） ポートを通過する特定の種類のネットワークトラフィックをブロックする場合は、permit コマンドの no 形式を使用します。

ステップ 4 4. 新しく作成された IP アクセスリストを表示するには、次のコマンドを使用します。

```
show running-config
```

インターフェイスへの IP アクセスリストの割り当て

IP アクセスリストをインターフェイスに割り当てるには、次の手順に従います。アクセスグループ（リスト）がすでに NIC に割り当てられている場合に新しいものを割り当てると、Cisco EPN Manager によって古いリストが新しいリストに置き換えられます。

重要 異なるインターフェイスに異なるアクセスリストを使用するには、インターフェイスに割り当てられている IP アドレスが同じネットワークまたはサブネットにないことを確認します。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （17 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 3. インターフェイスに IP アクセスリストを割り当てます。

```
config# interface interfaceName
config-InterfaceName# ip access-group acl_name  in
config-InterfaceName# exit
config# exit
```

ここで、

- *interfaceName*：インターフェイスの名前。
- **ip access-group**：IP アクセスリストをインターフェイスに追加するコマンド。

- *acl_name* : インターフェイスに割り当てる IP アクセスリスト。
- **in** ：受信の場合。

（注） 現時点では、この方向のみがサポートされています。

ステップ 4 4. アクセスリストがデバイスに割り当てられているかどうかを確認します。

```
show running-config
```

例

```
config# interface GigabitEthernet 0
config-GigabitEthernet-0# ip access-group test_acl
```

システムの問題を示すサーバー内部 SNMP トラップの使用

Cisco EPN Manager は、システム コンポーネントに関する潜在的な問題を示す内部 SNMP トラップを生成します。これには、ハードウェア コンポーネントの障害、ハイ アベイラビリティ状態の変化、バックアップ ステータスなどが含まれます。障害トラップは、障害または状態の変化が検出されるとすぐに生成され、クリアリング トラップは、障害が修正されると生成されます。TCA（CPU、メモリ、ディスクの高い使用率に関するトラップなど）では、しきい値を超えるとトラップが生成されます。

サーバーの内部 SNMP トラップの完全なリストについては、『Cisco Evolved Programmable Network Manager のサポート対象アラーム』に記載されています。Cisco EPN Manager は通知宛先のポート 162 にトラップを送信します。このポートは現時点ではカスタマイズできません。

以下のトピックの説明に従って、これらのトラップをカスタマイズしたり、管理したりできます。

- 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 （32 ページ）
- サーバー内部 SNMP トラップをトラブルシュートする （33 ページ）

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

トラップの重大度または（TCA の場合）しきい値を調整することで、サーバーの内部 SNMP トラップをカスタマイズできます。また、トラップを無効化/有効化することもできます。サーバーの内部 SNMP トラップは、「*Cisco Evolved Programmable Network* でサポートされているアラーム」で確認できます。

（注） Cisco EPN Manager は SNMPv2 通知も SNMPv3 通知も送信しません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）] > [システム イベントの設定（System Event Configuration）]** を選択します。

ステップ 2 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントの重大度（Event Severity）] を [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、およびメモリの使用率や、その他のハードウェアのトラップに対しては、[しきい値値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。（しきい値設定が NA と表示されるイベントのしきい値は設定できません）。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) [EPNM ユーザーセッション（EPNM User Sessions）] イベントの場合、[しきい値（Threshold）] の値を 1 ～ 150 の範囲で入力します。デフォルトでは、このしきい値の値は 5 です。

e) バックアップしきい値と証明書の有効期日（重要）に対しては、[しきい値値（Threshold）] に日数（*x* ～ *y*）を入力します。ここで、*x* は最小の日数、*y* は最大の日数です。

f) トラップを生成するかどうかを制御するには、[イベントステータス（Event Status）] を設定します。

ステップ 3 **[その他の設定（Other Settings）]** で、**[アラーム反復の作成とクリア（Create and Clear Alarm Iteration）]** に必要な値を入力します。

ステップ 4 トラップの変更内容を保存するには、（テーブルの下にある）[保存（Save）] をクリックします。

ステップ 5 アラームとイベントの最新のリストを表示するには、**[モニター（Monitor）] > [モニターリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 6 サーバーの内部 SNMP トラップの受信者を設定するには、を参照してくださいアラーム通知先の設定）。

サーバー内部 SNMP トラップをトラブルシュートする

「Cisco Evolved Programmable Network Manager のサポート対象アラーム」では、サーバーの内部 SNMP トラップの完全なリスト、その推定原因、および問題を解決するための推奨処置が提供されています。必要な情報がこのドキュメントに記載されていない場合は、次の手順に従って、Cisco EPN Manager サーバーの問題をトラブルシュートし、詳細情報を入手してください。

ステップ 1 Cisco EPN Manager サーバーから通知レシーバに ping を実行し、Cisco EPN Manager と管理アプリケーション間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して Cisco EPN Manager にログインします。**Administration > Logging** を選択してログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

- ncs_nbi.log：これは Cisco EPN Manager が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これはその他の最新の Cisco EPN Manager アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。
- hm-#-#.log：これはすべてのヘルス モニター アクティビティのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポート ケースを開き、疑わしいログ ファイルをケースに添付してください。シスコ サポート ケースの登録 を参照してください。

シスコサポート リクエストのデフォルトの設定

デフォルトでは、Cisco EPN Manager GUI のさまざまな部分からシスコサポート リクエストを作成できます。必要に応じて、送信者の電子メールアドレスやその他の電子メールの特性を設定できます。これらを設定しない場合、ユーザーがケースを登録するときに情報を入力できます。

ユーザーが GUI クライアントからリクエストを作成できないようにするには、その機能を無効にします。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [サポート リクエスト（Supporte Request）] タブをクリックします。

ステップ 3 必要なインタラクション タイプを選択します。

- [サーバーから直接インタラクションを有効にしてください（Enable interactions directly from the server）]：Cisco EPN Manager サーバーから直接サポート ケースを作成する場合は、このオプションを指定します。サポート プロバイダへの電子メールは、Cisco EPN Manager サーバーに関連付けられているメール アドレス、または指定したメール アドレスから送信されます。
- [クライアントシステムを介したインタラクションのみ（Interactions via client system only）]：サポート ケースに必要な情報をクライアント マシンにダウンロードする場合は、このオプションを指定します。この場合、ダウンロードしたサポート ケースの詳細および情報をサポート プロバイダに電子メールで送信する必要があります。

ステップ 4 テクニカル サポート プロバイダを選択します。

- [Cisco] をクリックし、シスコ テクニカル サポートにサポート ケースを登録し、各自の Cisco.com クレデンシャルを入力し、[接続のテスト（Test Connectivity）] をクリックして次のサーバーへの接続を確認します。
  - Cisco EPN Manager メール サーバー
  - シスコ サポート サーバー
  - フォーラム サーバー
- [サードパーティ サポート プロバイダ（Third-party Support Provider）] をクリックして、サードパーティ サポート プロバイダへのサービス要求を作成します。プロバイダの電子メールアドレス、件名、Web サイト URL を入力します。

シスコ製品フィードバックの設定

シスコ製品の向上のために、Cisco EPN Manager は以下のデータを収集してシスコに送信します。

- 製品情報：製品タイプ、ソフトウェア バージョン、インストール済みライセンス。
- システム情報：サーバーのオペレーティング システムおよび利用可能なメモリ。
- ネットワーク情報：ネットワーク上のデバイスの数とタイプ。

この機能はデフォルトでイネーブルになっています。データは日単位、週単位、または月単位で収集され、HTTPS を使用してシスコ クラウドの REST URL に送信されます。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（General）] > [改善にご協力ください（Help Us Improve）]** を選択します。

- シスコが収集するデータの種類を確認するには、[シスコが収集するデータについて（What data is Cisco collecting?）] をクリックします。
- この機能を無効にするには、[今回は協力しない（Not at this time, thank you）] を選択し、[保存（Save）] をクリックします。

バックアップのモニターリング

ファイル名、サイズ、使用可能なサイズ、データなど、Cisco EPN Manager のバックアップ情報を表示するには、次の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。このタブに [バックアップ情報（Backup Information）] ダッシュレットが表示されます。

（注） バックアップ ダッシュレットの情報は、バックアップ リポジトリがローカルの場合にのみ使用できます。