# 展開



# Cisco ISE 展開の用語

次の用語は Cisco ISE 展開シナリオの説明に一般に使用されるものです。

- サービス：サービスは、ネットワーク アクセス、プロファイラ、ポスチャ、セキュリティ グループ アクセス、モニタリング、トラブルシューティングなどの、ペルソナが提供する固有の機能です。
- ノード：Cisco ISE ソフトウェアを実行する個別インスタンスです。Cisco ISE はアプライアンスとして使用でき、VMware で実行できるソフトウェアとしても使用できます。Cisco ISE ソフトウェアを実行する各インスタンス、アプライアンス、または VMware はノードと呼ばれます。
- ペルソナ：ノードのペルソナによって、そのノードが提供するサービスが決まります。Cisco ISE ノードは、管理、ポリシー サービス、モニタリング、および pxGrid のペルソナのいずれかを担うことができます。管理者ポータルで使用できるメニュー オプションは、Cisco ISE ノードが担当するロールおよびペルソナによって異なります。
- 展開モデル：展開が分散か、スタンドアロンか、スタンドアロンのハイ アベイラビリティ（基本的な 2 ノード構成）かを決定します。

# 分散 Cisco ISE 展開のペルソナ

Cisco ISE ノードは、管理、ポリシー サービス、またはモニタリングのペルソナを担当できます。

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。導入の各ノードは、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。分散デプロイメントでは、ネットワーク上で次の組み合わせのノードを使用できます。

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理ノード
- 自動フェールオーバー用の管理ノードのヘルス チェック用の非管理ノードの 1 つまたはペア
- プライマリ管理ノード（PAN）自動フェールオーバー用のヘルス チェック ノードのペアまたは単一のヘルス チェック ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード（PSN）

# Cisco ISE ノードの設定

Cisco ISE ノードをインストールすると、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナによって提供されるすべてのデフォルト サービスがそのノードで実行されます。このノードはスタンドアロン状態となります。Cisco ISE ノードの管理者ポータルにログインして設定する必要があります。スタンドアロン Cisco ISE ノードのペルソナまたはサービスは編集できません。ただし、プライマリおよびセカンダリ Cisco ISE ノードのペルソナおよびサービスは編集できます。最初にプライマリ ISE ノードを設定し、その後、セカンダリ ISE ノードをプライマリ ISE ノードに登録する必要があります。

ノードに初めてログインする場合は、デフォルトの管理パスワードを変更し、有効なライセンスをインストールする必要があります。

設定済みの Cisco ISE または本番環境では、ホスト名とドメイン名を変更しないことを推奨します。これが必要な場合は、初期展開時にアプライアンスのイメージを再作成し、変更を加え、詳細を設定します。

### 始める前に

Cisco ISE での分散展開の設定方法に関する基礎を理解しておく必要があります。「分散展開を設定する場合のガイドライン」を参照してください。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 2** 設定する Cisco ISE ノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

**ステップ 3** 必要に応じて値を入力し、[保存（Save）] をクリックします。

# プライマリ PAN の設定

分散展開を設定するには、最初に Cisco ISE ノードをプライマリ PAN として設定する必要があります。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

当初は [登録（Register）] ボタンが無効になっています。このボタンを有効にするには、プライマリ PAN を設定する必要があります。

**ステップ 2** 現在のノードの隣にあるチェックボックスをオンにして [編集（Edit）] をクリックします。

**ステップ 3** [プライマリにする（Make Primary）] をクリックして、プライマリ PAN を設定します。

**ステップ 4** [保存（Save）] をクリックしてノード設定を保存します。

### 次のタスク

1. 展開にセカンダリ ノードを追加します。
2. 必要に応じて、プロファイラ サービスを有効にし、プローブを設定します。

# セカンダリ Cisco ISE ノードの登録

ISE ノードをプライマリ PAN に登録して、マルチノード展開を形成することができます。プライマリ PAN 以外の展開内のノードは、セカンダリ ノードと呼ばれます。ノードを登録する際に、ノード上で有効にする必要があるペルソナとサービスを選択できます。登録されたノード

は、プライマリ PANから管理することができます（たとえば、ノードのペルソナ、サービス、証明書、ライセンス、パッチの適用などの管理）。

ノードが登録されると、プライマリ PAN は設定データをセカンダリ ノードにプッシュし、セカンダリ ノード上のアプリケーション サーバが再起動します。これが完了すると、プライマリ PAN で行われた設定の追加変更がセカンダリ ノードに複製されます。セカンダリ ノードで変更が複製されるのにかかる時間は、ネットワーク遅延、システムへの負荷などのさまざまな要因によって決まります。

### 始める前に

プライマリ PAN と登録されているノードが相互に DNS 解決可能であることを確認します。登録されているノードが信頼できない自己署名証明書を使用している場合は、証明書の詳細が記載された証明書の警告がプロンプト表示されます。証明書を受け入れると、プライマリ PAN の信頼できる証明書ストアに追加され、ノードとの TLS 通信が可能になります。

ノードが自己署名されていない証明書（たとえば外部 CA によって署名された証明書）を使用している場合、そのノードの関連する証明書チェーンをプライマリ PAN の信頼できる証明書ストアに手動でインポートする必要があります。信頼できる証明書ストアにセカンダリ ノードの証明書をインポートする場合は、セカンダリ ノードの証明書を検証するように PAN の [ISE 内の認証用に信頼する（Trust for Authentication within ISE）] チェックボックスをオンにします。

セッション サービスが有効になっているノード（ネットワーク アクセス、ゲスト、ポスチャなど）を登録する場合は、それをノード グループに追加できます。詳細についてはポリシー サービス ノード グループの作成 （65 ページ）を参照してください。

---

**ステップ 1** プライマリ PAN にログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** [登録（Register）] をクリックして、セカンダリ ノードの登録を開始します。

**ステップ 4** 登録するスタンドアロン ノードの DNS 解決可能な完全修飾ドメイン名（FQDN）を入力します（hostname.domain-name の形式（たとえば、abc.xyz.com））。プライマリ PAN の FQDN と登録されているノードは、互いに解決可能でなければなりません。

**ステップ 5** [ユーザ名（Username）] フィールドおよび [パスワード（Password）] フィールドに、セカンダリ ノードの UI ベースの管理者クレデンシャルを入力します。

**ステップ 6** [Next] をクリックします。

プライマリ PAN は、登録されているノードを使用して TLS 通信を（初めて）確立しようとします。

- ノードが信頼できる証明書を使用している場合は、手順 7 に進むことができます。
- ノードが信頼されていない自己署名証明書を使用している場合は、証明書の警告メッセージが表示されます。証明書の警告メッセージには、ノード上の実際の証明書と照合できる証明書に関する詳細（発行先、発行元、シリアル番号など）が表示されます。[証明書のインポートと続行（Import Certificate and Proceed）] オプションを選択して、この証明書を信頼し、登録を続行することができます。Cisco ISE は、そのノードのデフォルトの自己署名証明書をプライマリ PAN の信頼できる証明書ストアにインポートします。デフォルトの自己署名証明書を使用しない場合は、[登録のキャンセル（Cancel

Registration）] をクリックし、そのノードの関連する証明書チェーンをプライマリ PAN の信頼できる証明書ストアに手動でインポートします。信頼できる証明書ストアにセカンダリ ノードの証明書をインポートする場合は、セカンダリ ノードの証明書を検証するように PAN の [ISE 内の認証用に信頼する（Trust for Authentication within ISE）] チェックボックスをオンにします。

- ノードが CA 署名付き証明書を使用する場合は、証明書の信頼が設定されるまで登録を続行できないというエラー メッセージが表示されます。

**ステップ 7** ノード上で有効にするペルソナとサービスを選択し、[保存（Save）] をクリックします。

---

ノードが登録されると、プライマリ PAN でアラーム（ノードが展開に追加されたことを確認するアラーム）が生成されます。このアラームは [アラーム（Alarms）] ページで表示できます。登録済みノードを同期して再起動したら、プライマリ PAN で使用されているのと同じクレデンシャルを使用してセカンダリ ノードの GUI にログインできます。

### 次のタスク

- ゲストユーザのアクセスと許可、ロギングなどの時間依存タスクの場合は、ノード間のシステム時刻が同期されていることを確認します。
- セカンダリ PAN を登録し、内部 Cisco ISE CA サービスを使用する場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーをバックアップし、セカンダリ PAN に復元する必要があります。

  参照先 Cisco ISE CA 証明書およびキーのバックアップと復元

# 複数の展開シナリオのサポート

Cisco ISE は企業インフラストラクチャ全体に展開することが可能で、802.1X 有線、無線、およびバーチャル プライベート ネットワーク（VPN）がサポートされます。

Cisco ISE アーキテクチャでは、1 台のマシンがプライマリ ロール、もう 1 台の「バックアップ」マシンがセカンダリ ロールとなる環境において、スタンドアロン展開と分散（別名「ハイアベイラビリティ」または「冗長」）展開の両方がサポートされます。Cisco ISE は、個別の設定可能なペルソナ、サービス、およびロールを特徴としており、これらを使用して、Cisco ISE サービスを作成し、ネットワーク内の必要な箇所に適用できます。これにより、フル機能を備え統合されたシステムとして動作する包括的な Cisco ISE 展開が実現します。

Cisco ISE ノードは、1 つ以上の管理ペルソナ、モニタリング ペルソナ、およびポリシー サービス ペルソナとして展開できます。各ペルソナは、ネットワーク ポリシー管理トポロジ内の異なる部分で重要な役割を担います。Cisco ISE を管理ペルソナとしてインストールすると、集中型ポータルからネットワークを設定および管理することによって、効率と使いやすさを向上させることができます。

# Cisco ISE 分散展開

複数の Cisco ISE ノードがある展開は、分散展開と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、展開に複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散展開では、管理およびモニタリング アクティビティは一元化され、処理はポリシー サービス ノード間で分配されます。パフォーマンスのニーズに応じて、導入環境の規模を変更できます。展開の各 Cisco ISE ノードは、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。

## Cisco ISE 展開の設定

『*Cisco Identity Services Engine Hardware Installation Guide*』で説明されているように Cisco ISE をすべてのノードにインストールした後、ノードはスタンドアロン状態で稼働します。次に、1 つのノードをプライマリ PAN として定義する必要があります。プライマリ PAN の定義時に、そのノードで管理ペルソナおよびモニタリング ペルソナを有効にする必要があります。任意で、プライマリ PAN でポリシー サービス ペルソナを有効にできます。プライマリ PAN のペルソナ定義のタスクの完了後に、他のセカンダリ ノードをプライマリ PAN に登録し、セカンダリ ノードのペルソナを定義できます。

すべての Cisco ISE システムおよび機能に関連する設定は、プライマリ PAN でだけ実行する必要があります。プライマリ PAN で行った設定の変更は、展開内のすべてのセカンダリ ノードに複製されます。

分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のモニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。

## プライマリ ISE ノードからセカンダリ ISE ノードへのデータ レプリケーション

1 つの Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータ レプリケーション チャネルをすぐに作成し、複製のプロセスを開始します。複製は、プライマリ ノードからセカンダリ ノードに Cisco ISE 設定データを共有するプロセスです。複製によって、展開を構成するすべての Cisco ISE ノードの設定データの整合性を確実に維持できます。

通常、最初に ISE ノードをセカンダリ ノードとして登録したときに、完全な複製が実行されます。完全な複製の実行後は差分複製が実行され、PAN での設定データに対する新しい変更（追加、変更、削除など）がセカンダリ ノードに反映されます。複製のプロセスでは、展開内のすべての Cisco ISE ノードが同期されます。Cisco ISE 管理者ポータルの展開のページから [ノード ステータス（Node Status）] 列で複製のステータスを表示できます。セカンダリ ノードとして Cisco ISE ノードを登録するか、または PAN との手動同期を実行すると、要求されたアクションが進行中であることを示すオレンジのアイコンがノード ステータスに表示されます。こ

れが完了すると、ノード ステータスは、セカンダリ ノードが PAN と同期されたことを示す緑に変わります。

# Cisco ISE ノードの登録解除

展開からノードを削除するには、ノードの登録を解除する必要があります。プライマリ PAN からセカンダリ ノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わり、プライマリ ノードとセカンダリ ノード間の接続が失われます。複製の更新は、登録解除されたスタンドアロン ノードに送信されなくなります。

PSN の登録が取り消されると、エンドポイント データは失われます。スタンドアロン ノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンドアロン ノードになったときに、このデータ バックアップを復元します。
- PSN のペルソナを管理者（セカンダリ PAN）に変更し、管理者ポータルの展開ページからデータを同期してから、ノードを登録解除します。この時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ管理ノードを追加できます。

（注） プライマリ PAN は登録解除できません。

# 分散展開を設定する場合のガイドライン

分散環境で Cisco ISE を設定する前に、次の内容をよく読んでください。

- ノードタイプ、ISE ノード、を選択します。管理、ポリシー サービス、およびモニタリング機能の場合は、ISE ノードを選択する必要があります。
- すべてのノードで、同じ Network Time Protocol（NTP）サーバを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ中に同じ NTP サーバ名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE のインストール時に Cisco ISE 管理パスワードを設定します。以前の Cisco ISE 管理のデフォルトのログイン クレデンシャル（admin/cisco）は無効になっています。初期セットアップ中に作成したユーザ名とパスワードを使用するか、または後でパスワードを変更した場合はそのパスワードを使用します。
- ドメイン ネーム システム（DNS）サーバを設定します。DNS サーバに、分散展開に含まれるすべての Cisco ISE ノードの IP アドレスと完全修飾ドメイン名（FQDN）を入力します。解決できない場合は、ノード登録が失敗します。
- DNS サーバに、分散展開のすべての Cisco ISE ノードの逆引き DNS ルックアップを設定します。設定しなかった場合、Cisco ISE ノードの登録時および再起動時に、展開に関する問

題が発生することがあります。すべてのノードで逆引き DNS ルックアップが設定されていない場合、パフォーマンスが低下する可能性があります。

- （任意）プライマリ PAN からセカンダリ Cisco ISE ノードを登録解除して、Cisco ISE をアンインストールします。
- プライマリ モニタリング ノードをバックアップし、新しいセカンダリ モニタリング ノードにデータを復元します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。
- プライマリ PAN と、セカンダリ ノードとして登録しようとしているスタンドアロン ノードで、同じバージョンの Cisco ISE が実行されていることを確認します。
- 新しいノードを展開に追加する際に、ワイルドカード証明書の発行元証明書チェーンが新しいノードの信頼できる証明書に含まれていることを確認します。新しいノードが展開に追加されると、ワイルドカード証明書が新しいノードに複製されます。

# プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション

分散展開を構成する Cisco ISE ノードで使用可能なメニュー オプションは、ノードで有効なペルソナによって異なります。すべての管理およびモニタリング アクティビティは、プライマリ PAN を介して実行する必要があります。その他のタスクについては、セカンダリ ノードを使用する必要があります。このため、セカンダリ ノードのユーザ インターフェイスでは、ノードで有効なペルソナに基づく限定されたメニュー オプションが提供されます。

1 つのノードが、ポリシー サービス ペルソナとアクティブ ロールのモニタリング ペルソナを担当するなど、複数のペルソナを担当する場合、ポリシー サービス ノードおよびアクティブ モニタリング ノードにリストされているメニュー オプションがそのノードで使用可能となります。

次の表に、さまざまなペルソナとなる Cisco ISE ノードで使用可能なメニュー オプションを示します。

表 *1 : Cisco ISE* ノードおよび使用可能なメニュー オプション

| Cisco ISE ノード | 使用可能なメニュー オプション |
|---|---|
| すべてのノード | • システム時刻と NTP サーバ設定の表示および設定。<br>• サーバ証明書のインストール、証明書署名要求の管理。すべてのサーバ証明書を一元的に管理するプライマリ PAN 経由で、展開内のすべてのノードに対し、サーバ証明書の操作を実行できます。<br>（注） 秘密キーは、ローカル データベースに格納されず、関連ノードからコピーされません。秘密キーは、ローカル ファイル システムに格納されます。 |
| プライマリ PAN | すべてのメニューおよびサブメニュー。 |
| アクティブ モニタリング ノード | • モニタリング データにアクセスします（プライマリ モニタリング ノードとアクティブ モニタリング ノードの両方から）。<br>（注） [操作（Operations）] メニューはプライマリ PAN からのみ表示できます。Cisco ISE 2.1 以降では、[操作（Operations）] メニューはモニタリング ノードに表示されません。 |
| ポリシー サービス ノード | Active Directory 接続への参加、脱退、およびテストを行うオプション。各ポリシー サービス ノードが別個に Active Directory ドメインに参加している必要があります。最初にドメイン情報を定義し、PAN を Active Directory ドメインに参加させる必要があります。次に、他のポリシー サービス ノードを Active Directory ドメインに個別に参加させます。 |

| Cisco ISE ノード | 使用可能なメニュー オプション |
|---|---|
| セカンダリ PAN | セカンダリ PAN をプライマリ PAN に昇格させるオプション。<br>（注） プライマリ PAN にセカンダリ ノードを登録した後は、いずれのセカンダリ ノードの管理者ポータルにログインする場合にも、プライマリ PAN のログイン クレデンシャルを使用する必要があります。 |

# 展開とノードの設定

## 展開とノードの設定

[展開ノード（Deployment Nodes）] ページを使用すると、Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノードを設定し、展開を設定することができます。

### 展開ノードリストウィンドウ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト（Deployment Nodes List）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** です。

| フィールド名 | 使用上のガイドライン |
|---|---|
| ホスト名（**Hostname**） | ノードのホスト名を表示します。 |
| ノード タイプ（**Node Type**） | ノード タイプを表示します。次のいずれかを設定できます。<br>• Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノード |
| ペルソナ（**Personas**） | （ノード タイプが Cisco ISE の場合にのみ表示）Cisco ISE ノードが担当してきたペルソナがリストされます。[管理（Administration）]、[ポリシー サービス（Policy Service）] などがあります。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| ロール（**Role**） | このノードで管理ペルソナまたはモニタリング ペルソナが有効になっている場合、これらのペルソナが担当しているロール（プライマリ、セカンダリ、またはスタンドアロン）が示されます。ロールは、次のうちの 1 つまたは複数にできます。<br>• [PRI（A）] : プライマリ PAN を意味します<br>• [SEC（A）] : セカンダリ PAN を意味します<br>• [PRI（M）] : プライマリ モニタリング ノードを意味します<br>• [SEC（M）] : セカンダリ モニタリング ノードを意味します |
| **Services** | （ポリシー サービス ペルソナが有効な場合にのみ表示）この Cisco ISE ノードで実行されているサービスがリストされます。サービスは次のいずれか 1 つとなります。<br>• セッション（Session）<br>• プロファイリング<br>• すべて（All） |

| フィールド名 | 使用上のガイドライン |
|---|---|
| ノード ステータス（**Node Status**） | データ レプリケーション用の展開内の各 ISE ノードのステータスを示します。<br>• [緑（接続）（Green（Connected））]：すでに展開に登録されている ISE ノードがプライマリ PAN と同期していることを示します。<br>• [赤（切断）（Red（Disconnected））]：ISE ノードに到達できないか、ISE ノードがダウンしているか、またはデータレプリケーションが行われていないことを示します。<br>• [オレンジ（進行中）（Orange（In Progress））]：ISE ノードがプライマリ PAN に新規に登録されているか、手動同期操作を実行したか、または ISE ノードがプライマリ PAN と同期していないことを示します。<br>詳細については、[ノード ステータス（Node Status）] カラムで各 ISE ノードのクイック ビュー アイコンをクリックします。 |

**関連トピック**

Cisco ISE 分散展開 （6 ページ）
Cisco ISE 展開の用語 （1 ページ）
Cisco ISE ノードの設定 （2 ページ）
セカンダリ Cisco ISE ノードの登録

## ノードの一般設定

次の表で、Cisco ISE ノードの [全般設定 (General Settings)] ウィンドウのフィールドについて説明します。このウィンドウでは、ペルソナをノードに割り当て、そのサービスを実行するように設定できます。このタブのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開ノード（Deployment Node）] > [編集（Edit）] > [全般設定（General Settings）]** です。

*表 2: ノードの一般設定*

| フィールド名 | 使用上のガイドライン |
|---|---|
| ホスト名（**Hostname**） | Cisco ISE ノードのホスト名を表示します。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **FQDN** | Cisco ISE ノードの完全修飾ドメイン名を表示します。たとえば、ise1.cisco.com などです。 |
| **IP アドレス** | Cisco ISE ノードの IP アドレスを表示します。 |
| ノード タイプ（**Node Type**） | ノード タイプを表示します。 |
| ペルソナ（**Personas**） | |
| 管理（**Administration**） | Cisco ISE ノードに管理ペルソナを担当させる場合は、このチェックボックスをオンにします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。<br><br>ロール（Role）：管理ペルソナが展開で担当しているロールを表示します。[スタンドアロン（Standalone）]、[プライマリ（Primary）]、[セカンダリ（Secondary）] のいずれかの値になります。<br><br>プライマリにする（Make Primary）：ノードをプライマリ Cisco ISE ノードにする場合にこのボタンをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このページのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードにスタンドアロン ロールが割り当てられている場合、[プライマリにする（Make Primary）] ボタンがノードの横に表示されます。ノードにセカンダリ ロールが割り当てられている場合、[プライマリに昇格（Promote to Primary）] ボタンがノードの横に表示されます。ノードにプライマリ ロールがあり、そのノードを使用して登録されている他のノードがない場合は、ノードの横に[スタンドアロンにする（Make Standalone）] ボタンが表示されます。このボタンをクリックすると、プライマリ ノードをスタンドアロン ノードにすることができます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| モニタリング | |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | Cisco ISE ノードにモニタリング ペルソナを担当させ、ログ コレクタとして機能させる場合は、このチェックボックスをオンにします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。<br>VMware プラットフォームで Cisco ISE ノードをログ コレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。<br><br>モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に 2 つのモニタリング ノードがある場合は、Cisco ISE に、プライマリ-セカンダリ ロールを設定する他のモニタリング ノードの名前が表示されます。これらのロールを設定するには、次のいずれかを選択します。<br><br>• プライマリ（Primary）：現在のノードをプライマリ モニタリング ノードにする場合。<br><br>• セカンダリ（Secondary）：現在のノードをセカンダリ モニタリング ノードにする場合。<br><br>• なし（None）：モニタリング ノードにプライマリ/セカンダリ ロールを担当させない場合。<br><br>モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよび |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | セカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリングノードのロールを [なし（None）]に変更した場合、他方のモニタリングノードのロールも同様に [なし（None）] になり、それによって高可用性ペアがキャンセルされます。モニタリングノードとしてノードを指定すると、そのノードが **[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]** >**[リモートロギング ターゲット（Remote Logging Targets）]** ウィンドウで syslog ターゲットとして表示されます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| ポリシー サービス（**Policy Service**） | |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | 次のサービスの 1 つまたはすべてを有効にするには、このチェックボックスをオンにします。<br>• [セッションサービスの有効化（Enable Session Services）] : ネットワーク アクセス サービス、ポスチャサービス、ゲスト サービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。このポリシー サービス ノードが属するグループを、[ノードをノード グループに含める（Include Node in Node Group）] ドロップダウン リストから選択します。CA サービスと EST サービスは、セッション サービスが有効になっているポリシーサービスノードでのみ実行できることに注意してください。<br>[ノードをノードグループに含める（Include Node in Node Group）] については、このポリシーサービスモードをどのグループにも含めない場合は [なし（None）] を選択します。<br>同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。<br>多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、『』の「ポリシー サービス ノード グループの作成」のセクションポリシー サービス ノード グループの作成（65 ページ）を参照してください。<br>• プロファイリング サービスの有効化（Enable Profiling Service）：プロファイラ サービスを有効にするには、このチェックボックスをオンにします。プロファイリング サービスを有効にする場合は、[Profiling Configuration（プロファイリング設定）] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシー サービス ノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーション サーバがいつ再起動したかを確認するには、CLI で show application status ise コマンドを使用します。<br>• 脅威中心型NACサービスの有効化（Enable Threat Centric NAC Service）：脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能を有効にするには、このチェックボックスをオンにします。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | • SXPサービスの有効化（Enable SXP Service）：ノードで SXP サービスを有効にするには、このチェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。<br><br>NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス（Use Interface）] ドロップダウン リストに表示されます。<br><br>• デバイス管理サービスの有効化（Enable Device Admin Service）：TACACS ポリシーセット、ポリシー結果などを作成し、ネットワークデバイスの設定を制御および監査するには、このチェックボックスをオンにします。<br><br>• パッシブIDサービスの有効化（Enable Passive Identity Service）：ID マッピング機能を有効にするには、このチェックボックスをオンにします。この機能を使用すると、Cisco ISE ではなくドメイン コントローラ（DC）で認証されるユーザをモニタすることができます。Cisco ISE がユーザのネットワーク アクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory（AD）ドメイン コントローラからユーザ認証情報を収集することができます。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **pxGrid** | pxGridペルソナを有効にするには、このチェック ボックスをオンにします。Cisco pxGridは、Cisco ISE セッション ディレクトリから Cisco Adaptive Security Appliance（ASA）などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます（たとえば、ISEとサードパーティ ベンダー間でのタグやポリシー オブジェクトの共有）。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。 |

**関連トピック**

分散 Cisco ISE 展開のペルソナ （2 ページ）
管理ノード （33 ページ）
ポリシー サービス ノード （43 ページ）
モニタリング ノード （47 ページ）
pxGrid ノード （55 ページ）
プライマリおよびセカンダリの Cisco ISE ノードの同期 （64 ページ）
ポリシー サービス ノード グループの作成 （65 ページ）
ISE pxGrid ノードの展開 （58 ページ）
ノード ペルソナとサービスの変更 （64 ページ）
自動フェールオーバー用のモニタリング ノードの設定 （54 ページ）

## プロファイリング ノードの設定

次の表では、プロファイラ サービスのプローブの設定に使用できる [プロファイリング設定（Profiling Configuration）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [ISE ノード（ISE Node）] > [編集（Edit）] > [プロファイリング設定（Profiling Configuration）]** です。

表 *3:* プロファイリング ノードの設定

| フィールド名 | 使用上のガイドライン |
|---|---|
| **NetFlow** | ルータから送信された NetFlow パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに NetFlow を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。<br>• [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。<br>• [ポート（Port）] : NetFlow エクスポートがルータから受信した NetFlow リスナー ポート番号を入力します。デフォルト ポートは 9996 です。 |
| **DHCP** | IP ヘルパーから DHCP パケットをリッスンするために、ポリシーサービスペルソナを担当した Cisco ISE ノードごとに DHCP を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。<br>• [ポート（Port）] : DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。<br>• [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。<br>• [ポート（Port）] : DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。 |
| **DHCP SPAN** | DHCP パケットを収集するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP SPAN を有効にする場合は、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **HTTP** | HTTPパケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとにHTTP を有効にする場合は、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。 |
| 『**RADIUS**』 | IOS センサー対応デバイスから RADIUS セッション属性、さらに CDP 属性と LLDP 属性を収集するために、ポリシー サービス ペルソナを担当した ISE ノードごとに RADIUS を有効にする場合は、このチェックボックスをオンにします。 |
| ネットワーク スキャン（**NMAP**）（**Network Scan (NMAP)**） | NMAP プローブをイネーブルにするには、このボックスをオンにします。 |
| **DNS** | FQDN の DNS ルックアップを実行するために、ポリシー サービス ペルソナを担当した ISE ノードごとに DNS を有効にする場合は、このチェックボックスをオンにします。秒単位でタイムアウト時間を入力します。<br>（注） DNSプローブを分散展開内の特定のCisco ISE ノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMPのいずれかのプローブを有効にする必要があります。DNSルックアップの場合、上記のいずれかのプローブを DNS プローブとともに起動する必要があります。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **SNMP クエリ（SNMP Query）** | 指定した間隔でネットワーク デバイスをポーリングするために、ポリシー サービス ペルソナを担当したISEノードごとにSNMPクエリーを有効にする場合は、このチェックボックスをオンにします。[再試行（Retries）]、[タイムアウト（Timeout）]、[イベント タイムアウト（Event Timeout）]、任意の [説明（Description）] の各フィールドに値を入力します。<br>（注） SNMPクエリープローブの設定に加えて、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] の場所にある他のSNMP設定も行う必要があります。ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスでシスコ デバイス プロトコル（CDP）およびLink Layer Discovery Protocol（LLDP）をグローバルに有効にしていることを確認します。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **SNMP トラップ（SNMP Trap）** | ネットワーク デバイスから linkUp、linkDown、MAC 通知トラップを受信するために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP トラップ プローブを有効にする場合は、このチェックボックスをオンにします。次のいずれかを選択します。<br>• [リンクトラップクエリ（Link Trap Query）]：SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。<br>• [MAC トラップクエリ（MAC Trap Query）]：SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）]：ISE ノードのインターフェイスを選択します。<br>• [ポート（Port）]：使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。 |
| **Active Directory** | 定義された Active Directory サーバをスキャンして、Windows ユーザに関する情報を探します。 |
| **pxGrid** | ISE で pxGrid を介してエンドポイント属性を収集（プロファイリング）できるようになります。 |

**関連トピック**

Cisco ISE プロファイリング サービス
プロファイリング サービスによって使用されるネットワーク プローブ
Cisco ISE ノードでのプロファイリング サービスの設定

# ロギングの設定

次の各ページでは、デバッグ ログの重大度の設定、外部ログ ターゲットの作成が可能です。また、Cisco ISE がこれらの外部ログ ターゲットにログ メッセージを送信できるようにできます。

# リモート ロギング ターゲットの設定

次の表では、外部の場所（syslogサーバ）を作成してロギングメッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

**表 *4:* リモート ロギング ターゲットの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| [名前（Name）] | 新しいターゲットの名前を入力します。 |
| ターゲット タイプ（Target Type） | ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。 |
| 説明 | 新しいターゲットの簡単な説明を入力します。 |
| [IPアドレス（IP Address）] | ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。ISEは、ロギング用に IPv4 と IPv6 形式をサポートします。 |
| [ポート（Port）] | 宛先マシンのポート番号を入力します。 |
| ファシリティ コード（Facility Code） | ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。 |
| 最大長（Maximum Length） | リモートログターゲットメッセージの最大長を入力します。有効なオプションは200～1024バイトです。 |
| サーバダウン時のバッファ メッセージ（Buffer Message When Server Down） | TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISEは、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| バッファ サイズ（MB）（Buffer Size (MB)） | 各ターゲットのバッファ サイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。 |
| 再接続タイムアウト（秒）（Reconnect Timeout (Sec)） | サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。 |
| CA 証明書の選択（Select CA Certificate） | クライアント証明書を選択します。 |
| サーバ証明書有効性を無視（Ignore Server Certificate validation） | ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。 |

**関連トピック**

- Cisco ISE ロギング メカニズム
- Cisco ISE システム ログ
- リモート syslog メッセージの形式
- Cisco ISE メッセージ カタログ
- 収集フィルタ
- イベント抑制バイパス フィルタ
- リモート syslog 収集場所の設定
- 収集フィルタの設定

## ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）]ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギングカテゴリ（Logging Categories）] です。

**表 *5:* ロギング カテゴリの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| [名前（Name）] | ロギング カテゴリの名前を表示します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ログの重大度レベル（Log Severity Level） | 次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。<br>• [重大（FATAL）]：緊急事態。 このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します<br>• [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。<br>• [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。 これがデフォルトの条件です。<br>• [情報（INFO）]：このオプションは、情報メッセージを示します。<br>• [デバッグ（DEBUG）]：このオプションは、診断バグ メッセージを示します。 |
| ローカル ロギング（Local Logging） | ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。 |
| ターゲット（Target） | 左アイコンと右アイコンを使用して[使用可能（Available）]と[選択済み（Selected）]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能（Available）]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み（Selected）]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。 |

**関連トピック**

リモート syslog メッセージの形式
Cisco ISE メッセージ コード
リモート syslog 収集場所の設定
メッセージ コードの重大度レベルの設定

# 管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

## 管理者パスワード ポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワードポリシー（Administrator Password Policy）] ページのフィールドを示します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワード ポリシー（Password Policy）]** です。

**表 *6 :* 管理者パスワード ポリシーの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 最小長（Minimum Length） | パスワードの最小長（文字数）を設定します。デフォルトは 6 文字です。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| パスワードに使用できない文字（Password may not contain） | [管理者名またはその文字の逆順は使用できません（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。 |
| | [「cisco」またはその文字の逆順は使用できません（"cisco" or its characters in reverse order）]：このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。 |
| | [この単語またはその文字の逆順は使用できません（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。 |
| | [4 回以上連続する繰り返し文字は使用できません（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字の使用を制限します。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| | [辞書の単語、その文字の逆順、または文字の置き換えは使用できません（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。<br>「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa$$w0rd などです。<br>• [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。<br>デフォルトでは、このオプションが選択されています。<br>• [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。 |
| 必須の文字（Required Characters） | 管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。<br>• 小文字の英文字<br>• 大文字の英文字<br>• 数字（Numeric characters）<br>• 英数字以外の文字（Non-alphanumeric characters） |

| フィールド | 使用上のガイドライン |
|---|---|
| パスワード履歴（Password History） | 同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。<br>また、以前のパスワードと異なる必要がある文字数を指定します。<br>ユーザがパスワードを再使用できない日数を入力します。 |
| パスワードライフタイム（Password Lifetime） | 次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。<br>• パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間（日数）（Time (in days) before the administrator account is disabled if the password is not changed.）（使用可能な範囲は 0 ～ 2,147,483,647 日です）。<br>• 管理者アカウントが無効になるまでのリマインダ（日数）。（Reminder (in days) before the administrator account is disabled.） |
| ネットワーク デバイスの機密データの表示 | |
| 管理者パスワードが必要（Require Admin Password） | 共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。 |
| パスワードのキャッシュ期間（Password cached for） | 管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。 |

**関連トピック**

Cisco ISE 管理者
新しい管理者の作成

# セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** です。

**表 *7:* セッション タイムアウトおよびセッション情報の設定**

| フィールド | 使用上のガイドライン |
|---|---|
| セッションのタイムアウト（Session Timeout） | |
| セッション アイドル タイムアウト（Session Idle Timeout） | アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。 |
| セッション情報（Session Info） | |
| 無効化（Invalidate） | 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。 |

**関連トピック**

管理者アクセスの設定
管理者のセッション タイムアウトの設定
アクティブな管理セッションの終了

# 管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。認証、許可、監査などの機能に関連したすべてのシステム関連設定を処理します。分散環境では、最大 2 つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、またはセカンダリのロールのいずれかを担当できます。

# 管理ノードのハイ アベイラビリティ

ハイ アベイラビリティ構成では、プライマリ管理ノード（PAN）がアクティブな状態です。セカンダリ PAN（バックアップ PAN）はスタンバイ状態です。これは、セカンダリ PAN がプライマリ PAN からすべての設定更新を受信するものの、ISE ネットワークではアクティブではないことを意味します。

Cisco ISE は、手動および自動フェールオーバーをサポートします。自動フェールオーバーでは、プライマリ PAN がダウンした場合にセカンダリ PAN の自動プロモーションが開始されま

す。自動フェールオーバーでは、ヘルス チェック ノードと呼ばれる非管理セカンダリ ノードが必要です。ヘルス チェック ノードは、プライマリ PAN の正常性を確認します。プライマリ PAN がダウンまたは到達不能であることが検出された場合、ヘルス チェック ノードがセカンダリ PAN のプロモーションを開始して、プライマリ ロールが引き継がれます。

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。

次の表に、プライマリ PAN がダウンし、セカンダリ PAN がまだ引き継がれていない場合に影響を受ける機能を示します。

| 機能 | プライマリ PAN のダウン時に使用できるかどうか（可/不可） |
|---|---|
| 既存の内部ユーザの RADIUS 認証 | 可 |
| 既存または新しい AD ユーザの RADIUS 認証 | 可 |
| プロファイル変更がない既存のエンドポイント | 可 |
| プロファイル変更がある既存のエンドポイント | 不可 |
| プロファイリングで学習した新しいエンドポイント。 | 不可 |
| 既存のゲスト：LWA | 可 |
| 既存のゲスト：CWA | 可（自動デバイス登録機能を持つホットスポット、BYOD、CWA などのデバイス登録に有効なフローを除く） |
| ゲストのパスワード変更 | 不可 |
| ゲスト：AUP | 不可 |
| ゲスト：ログイン失敗の最大回数の適用 | 不可 |
| 新しいゲスト（Sponsored-Guest またはアカウント登録） | 不可 |
| ポスチャ（Posture） | 可 |
| 内部 CA による BYOD | 不可 |
| 登録済みの既存のデバイス | 可 |

| 機能 | プライマリ PAN のダウン時に使用できるかどうか（可/不可） |
|---|---|
| MDM オンボーディング | 不可 |
| pxGrid サービス | 不可 |

内部認証局による証明書のプロビジョニングをサポートするには、プロモーションの後に、元のプライマリ PAN のルート証明書とそのキーを新しいプライマリ ノードにインポートする必要があります。セカンダリ ノードからプライマリ PAN へのプロモーションの後に追加された PSN ノードでは、自動フェールオーバー後に証明書のプロビジョニングが機能しません。

# ハイ アベイラビリティのヘルス チェック ノード

プライマリ PAN のヘルス チェック ノードをアクティブ ヘルス チェック ノードと呼びます。セカンダリ PAN のヘルス チェック ノードをパッシブ ヘルス チェック ノードと呼びます。アクティブ ヘルス チェック ノードは、プライマリ PAN のステータスを検査し、管理ノードの自動フェールオーバーを管理します。ヘルス チェック ノードとして 2 つの非管理 ISE ノードを使用することをお勧めします。1 つはプライマリ PAN、もう 1 つはセカンダリ PAN です。1 つだけヘルス チェック ノードを使用する場合、そのノードがダウンすると、自動フェールオーバーは発生しません。

両方の PAN が同じデータセンターにある場合、1 つの非管理 ISE ノードをプライマリ PAN とセカンダリ PAN の両方のヘルス チェック ノードとして使用できます。単一のヘルス チェック ノードがプライマリ PAN とセカンダリ PAN の両方の状態を検査する場合、そのノードはアクティブ/パッシブ両方の役割を担います。

ヘルス チェック ノードは非管理ノードです。つまり、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。管理ノードと同じデータセンター内の PSN ノードをヘルス チェック ノードとして指定することをお勧めします。ただし、2つの管理ノードが同じ場所（LANまたはデータセンター）にない小規模または一元化された展開では、管理ペルソナを持っていないノード（PSN/pxGrid/MnT）をヘルス チェック ノードとして使用できます。

自動フェールオーバーを無効にし、プライマリ PAN の障害発生時に手動でセカンダリ ノードを昇格させることを選択した場合には、チェック ノードは不要です。

### セカンダリ PAN のヘルス チェック ノード

セカンダリ PAN のヘルス チェック ノードはパッシブ モニタです。セカンダリ PAN がプライマリ PAN として昇格するまで、このノードはアクションを実行しません。セカンダリ PAN がプライマリ ロールを引き継ぐと、関連するヘルス チェック ノードは管理ノードの自動フェールオーバーを管理するアクティブ ロールを担います。以前のプライマリ PAN のヘルス チェック ノードはセカンダリ PAN のヘルス チェック ノードになり、受動的にモニタリングを行います。

### ヘルス チェックの無効化と再起動

ノードがヘルス チェック ロールから削除された場合、または自動フェールオーバー設定が無効な場合、ヘルス チェック サービスはそのノードで停止します。自動フェールオーバー設定が指定されたハイアベイラビリティ ヘルス チェック ノードでイネーブルになると、ノードは管理ノードの正常性のチェックを再度開始します。ノードでハイアベイラビリティ ヘルス チェック ロールを指定または削除しても、そのノードのいずれのアプリケーションが再起動されることはありません。ヘルス チェック アクティビティのみが開始または停止します。

ハイアベイラビリティのヘルス チェック ノードを再起動すると、プライマリ PAN の以前のダウンタイムが無視され、再びヘルス ステータスのチェックが開始されます。

## ヘルス チェック ノード

アクティブなヘルス チェック ノードは、設定したポーリング間隔でプライマリ PAN のヘルス ステータスをチェックします。ヘルス チェック ノードはプライマリ PAN に要求を送信し、それに対する応答が設定内容に一致する場合は、プライマリ PAN が良好な状態であると見なします。そうでなければ、ヘルス チェック ノードはプライマリ PAN が不良な状態であると見なします。プライマリ PAN の状態が設定済みフェールオーバー期間を超えて継続的に不良である場合、ヘルス チェック ノードはセカンダリ PAN へのフェールオーバーを開始します。

ヘルス チェックの任意の時点で、フェールオーバー期間中に不良と報告されたヘルス ステータスがその後で良好になったことが検出されると、ヘルス チェック ノードはプライマリ PAN のステータスを良好としてマークし、ヘルス チェック サイクルをリセットします。

プライマリ PAN ヘルス チェックからの応答は、そのヘルス チェック ノードで使用可能な設定値に照らして検証されます。応答が一致しない場合、アラームが発生します。ただし、プロモーション要求はセカンダリ PAN に行われます。

### ヘルス ノードの変更

ヘルス チェックに使用している ISE ノードを変更できますが、考慮すべき点がいくつかあります。

たとえば、ヘルス チェック ノード（H1）が非同期になり、他のノード（H2）がプライマリ PAN のヘルス チェック ノードになったとします。この場合、プライマリ PAN がダウンした時点で、同じプライマリ PAN を検査している別のノード（H2）があることを N1 が認識する方法はありません。その後、H2 がダウンしたりネットワークから切断されたりした場合に、実際のフェールオーバーが必要になります。しかし、セカンダリ PAN はプロモーション要求を拒否する権限を保持します。したがって、セカンダリ PAN がプライマリ ロールに昇格すると、H2 からのプロモーション要求が拒否されてエラーが発生します。プライマリ PAN のヘルス チェック ノードは、非同期になった場合でもプライマリ PAN の状態を引き続き検査します。

## セカンダリ PAN への自動フェールオーバー

プライマリ PAN が使用できなくなったときにセカンダリ PAN を自動的に昇格させるように ISE を設定できます。この設定は、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** ページのプライマリ管理ノード（プライマリ PAN）で行うことができます。

フェールオーバー時間は、「**フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover**）」で設定された回数と「**ポーリング間隔（Polling Interval**）」で設定された秒数をかけて得られる値として定義されます。デフォルト設定では、この時間は10分です。セカンダリ PAN からプライマリへの昇格には、さらに 10 分かかります。つまりデフォルトでは、プライマリ PAN の障害発生からセカンダリ PAN の動作開始までの時間は 20 分です。

セカンダリ PAN がフェールオーバー コールを受信すると、実際のフェールオーバーに進む前に、次の検証が行われます。

- ネットワークでプライマリ PAN が使用不能になっている。
- 有効なヘルス チェック ノードからフェールオーバー要求が受信された。
- この PAN に関するフェールオーバー要求である。

すべての検証に合格すると、セカンダリ PAN はプライマリ ロールに自身を昇格させます。

次に、セカンダリ PAN の自動フェールオーバーが試行されるシナリオのサンプルを示します（ただしこれに限定されません）。

- ポーリング期間中に、プライマリ PAN の正常性が「フェールオーバーの前に障害が発生したポール数（Number of failure polls before failover）」の値に対して一貫して良好でない。
- プライマリ PAN 上の Cisco ISE サービスが手動で停止され、フェールオーバー時間にわたって停止状態のままである。
- ソフト停止またはリブート オプションを使ってプライマリ PAN がシャットダウンされ、設定済みのフェールオーバー時間にわたってシャットダウン状態のままである。
- プライマリ PAN が突然ダウン（電源オフ）し、フェールオーバー時間にわたってダウン状態のままである。
- プライマリ PAN のネットワーク インターフェイスがダウンした（ネットワークポートが閉じた、またはネットワークサービスがダウンした）、あるいは他の理由でヘルスチェックノードから到達不能になり、設定済みのフェールオーバー時間にわたってダウン状態のままである。

### ヘルス チェック ノードの再起動

再起動すると、ハイアベイラビリティのヘルスチェックノードでは、プライマリ PAN の以前のダウンタイムが無視され、再びヘルスステータスがチェックされます。

### セカンダリ PAN への自動フェールオーバーの場合の個人所有デバイスの持ち込み

プライマリ PAN がダウンしている場合、プライマリ PAN ルート CA チェーンによってすでに発行された証明書が存在するエンドポイントに対して認証が中断されることはありません。これは、展開内のすべてのノードに、信頼と検証のための証明書チェーン全体が含まれているためです。

ただし、セカンダリ PAN がプライマリに昇格されるまで、新しい BYOD デバイスはオンボードされません。BYOD のオンボードには、アクティブなプライマリ PAN が必要です。

元のプライマリ PAN が復帰するか、セカンダリ PAN が昇格すると、新しい BYOD エンドポイントは問題なくオンボードされます。

障害が発生したプライマリ PAN をプライマリ PAN として再結合できない場合は、新たに昇格したプライマリ PAN（元のセカンダリ PAN）でルート CA 証明書を再生成します。

既存の証明書チェーンの場合、新しいルート CA 証明書をトリガーすると、下位 CA 証明書が自動的に生成されます。新しい下位証明書が生成された場合でも、以前のチェーンによって生成されたエンドポイント証明書は引き続き有効です。

# 自動フェールオーバーが回避された場合のシナリオ例

次に、ヘルス チェック ノードによる自動フェールオーバーが回避された場合、またはセカンダリ ノードへのプロモーション要求が拒否された場合を表すシナリオの例を示します。

- プロモーション要求を受信するノードがセカンダリ ノードでない。
- プロモーション要求に正しいプライマリ PAN の情報がない。
- プロモーション要求が不正なヘルス チェック ノードから受信された。
- プロモーション要求が受信されたが、プライマリ PAN が起動していて良好な状態である。
- プロモーション要求を受信するノードが同期していない。

# PAN 自動フェールオーバー機能の影響を受ける機能

次の表に、PAN の自動フェールオーバーの設定が展開でイネーブルの場合にブロックされる機能、または追加の設定変更を必要とする機能を示します。

| 機能 | 影響の詳細 |
|---|---|
| ブロックされる操作 | |

| 機能 | 影響の詳細 |
| --- | --- |
| アップグレード | CLI によるアップグレードがブロックされます。<br><br>PAN の自動フェールオーバー機能は、Cisco ISE の以前のバージョンからリリース 1.4 にアップグレードした後の構成で使用できます。デフォルトでは、この機能は無効になっています。<br><br>自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。 |
| バックアップの復元 | CLI による復元およびユーザ インターフェイスがブロックされます。<br><br>PAN の自動フェールオーバーの設定が復元前にイネーブルであった場合は、正常に復元した後に再設定する必要があります。 |
| ノード ペルソナの変更 | ユーザ インターフェイスによる次のノード ペルソナの変更がブロックされます。<br><br>• 両方の管理ノード内の管理ペルソナ。<br><br>• PAN のペルソナ。<br><br>• PAN の自動フェールオーバー機能をイネーブルにした後の、ヘルス チェック ノードの登録解除。 |

| 機能 | 影響の詳細 |
| --- | --- |
| その他の CLI 操作 | CLIによる次の管理操作がブロックされます。<br>• パッチのインストールおよびロールバック<br>• DNS サーバの変更<br>• eth1、eth2、およびeth3インターフェイスの IP アドレスの変更<br>• eth1、eth2、およびeth3インターフェイスのホスト エイリアスの変更<br>• タイムゾーンの変更 |
| 他の管理ポータル操作 | ユーザ インターフェイスによる次の管理操作がブロックされます。<br>• パッチのインストールおよびロールバック<br>• HTTPS 証明書の変更。<br>• 管理者認証タイプの変更（パスワードベースの認証から証明書ベースの認証へ、およびその逆）。 |
| すでに最大数のデバイスに接続しているユーザは接続できません。 | 障害の発生したPANに一部のセッションデータが格納されていため、PSN によってこれを更新できません。 |
| **PAN の自動フェールオーバーをディセーブルにする必要がある操作** | |
| CLI の操作 | PAN の自動フェールオーバーの設定がイネーブルの場合、CLI による次の管理操作では警告メッセージが表示されます。サービス/システムがフェールオーバー ウィンドウ内で再起動されない場合、これらの操作によって自動フェールオーバーが起動する場合があります。そのため、以下の操作の実行時には、PAN の自動フェールオーバーの設定を無効にすることを推奨します。<br>• 手動による ISE サービスの停止<br>• 管理 CLI を使用したソフト リロード（リブート） |

# 自動フェールオーバー用のプライマリ PAN の設定

### 始める前に

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。

**ステップ 1** プライマリ PAN のユーザ インターフェイスにログインします。

**ステップ 2** **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[PAN のフェールオーバー（PAN Failover）]** の順に選択します。

**ステップ 3** プライマリ PAN の自動フェールオーバーをイネーブルにするには、[PAN の自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスをオンにします。

セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシー サービス ペルソナ、モニタリング ペルソナ、または pxGrid ペルソナ、あるいはそれらの組み合わせのみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

**ステップ 4** 使用可能なすべてのセカンダリ ノードを含む [プライマリ ヘルス チェック ノード（Primary Health Check Node）] ドロップダウン リストから、プライマリ PAN のヘルス チェック ノードを選択します。

このノードは、プライマリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

**ステップ 5** 使用可能なすべてのセカンダリ ノードを含む [セカンダリ ヘルス チェック ノード（Secondary Health Check Node）] ドロップダウン リストから、セカンダリ PAN のヘルス チェック ノードを選択します。

このノードは、セカンダリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

**ステップ 6** 管理ノードのステータスがチェックされるまでの [ポーリング間隔（Polling Interval）] 時間を指定します。有効な範囲は 30 ～ 300 秒です。

**ステップ 7** [フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover）] の数を指定します。

フェールオーバーは、管理ノードのステータスが障害が発生したポール数として指定された数に対して良好でない場合に発生します。有効な範囲は 2 ～ 60 です。

**ステップ 8** [保存（Save）] をクリックします。

### 次のタスク

セカンダリ PAN のプライマリ PAN へのプロモーション後に、次の操作を実行します。

- 手動で古いプライマリ PAN を同期して、展開内に戻します。
- 手動で同期されていない他のセカンダリ ノードを同期して、展開内に戻します。

# セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗し、PAN の自動フェールオーバーを設定していないした場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

### 始める前に

プライマリ PAN に昇格するように管理ペルソナで設定された 2 番目の Cisco ISE ノードがあることを確認します。

**ステップ 1** セカンダリ PAN のユーザ インターフェイスにログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** [ノードの編集（Edit Node）] ページで、[プライマリに昇格（Promote to Primary）] をクリックします。

セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシー サービス ペルソナまたはモニタリング ペルソナ、あるいはその両方のみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

**ステップ 4** [保存（Save）] をクリックします。

### 次のタスク

元はプライマリ PAN であったノードが復帰した場合は、自動的にレベル下げされ、セカンダリ PAN になります。このノード（元のプライマリ PAN）で手動で同期を実行し、ノードを展開に戻す必要があります。

セカンダリ ノードの [ノードの編集（Edit Node）] ページでは、オプションが無効なためペルソナまたはサービスを変更できません。変更を加えるには、管理者ポータルにログインする必要があります。

# 新しい ISE 展開のプライマリ PAN として既存の ISE 展開のノードを再利用

既存の ISE 展開のノードを新しい ISE 展開のプライマリ PAN で再利用する場合は、次の手順を実行する必要があります。

**ステップ 1** お使いの ISE バージョンに応じた ISE インストール ガイドの説明のとおりに、ISE ユーティリティ「システムの消去の実行」を最初に実行します。 https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

**ステップ 2** ISE インストール ガイドの説明のとおりに、ISE の新規インストールを実行します。

**ステップ 3** プライマリ PAN の設定 （3 ページ）を参照して、スタンドアロンノードをプライマリ管理ノードとして設定します。

# プライマリ PAN にサービスを復元する

Cisco ISE は、元のプライマリ PAN への自動フォールバックをサポートしていません。セカンダリ PAN への自動フェールオーバーが開始された後、元のプライマリ PAN をネットワークに戻す場合には、それをセカンダリ PAN として設定する必要があります。

# 管理ノードの自動フェールオーバーのサポート

Cisco ISE は、管理ペルソナの自動フェールオーバーをサポートしています。自動フェールオーバー機能をイネーブルにするには、分散セットアップで少なくとも 2 つのノードが管理ペルソナを引き継ぎ、1 つのノードが非管理ペルソナを引き継ぐ必要があります。プライマリ管理ノード（PAN）がダウンした場合は、セカンダリ管理ノードの自動プロモーションが開始されます。この場合、非管理セカンダリ ノードが各管理ノードのヘルス チェック ノードとして指定されます。ヘルス チェック ノードは、設定された間隔で PAN の正常性を確認します。PAN の正常性について受信されたヘルス チェック応答がダウンまたは到達不能により良好でない場合、ヘルス チェック ノードは、設定されたしきい値まで待機した後、プライマリ ロールを引き継ぐようにセカンダリ管理ノードのプロモーションを開始します。セカンダリ管理ノードの自動フェールオーバー後に使用できなくなる機能がいくつかあります。Cisco ISE は、元の PAN へのフォールバックをサポートしていません。詳細については、「管理ノードのハイアベイラビリティ」の項を参照してください。

# ポリシー サービス ノード

ポリシーサービスモード（PSN）は Cisco ISE ノードであり、ポリシーサービスペルソナを使用して、ネットワークアクセス、ポスチャ、ゲストアクセス、クライアント プロビジョニング、およびプロファイリングの各サービスを提供します。

分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。このペルソナはポリシーを評価し、すべての決定を行います。通常、1 つの分散デプロイメントに複数のポリシー サービス ノードが存在します。

同じ高速ローカル エリア ネットワーク（LAN）またはロード バランサの背後に存在するポリシー サービス ノードはすべて、グループ化してノード グループを形成することができます。ノード グループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

# ポリシー サービス ノードのハイ アベイラビリティ

ノード障害を検出し、障害が発生したノードで URL がリダイレクトされたすべてのセッションをリセットするために、2 つ以上のポリシー サービス ノードを同じノード グループに配置できます。ノード グループに属しているノードがダウンすると、同じノード グループの別のノードが、障害が発生したノードで URL がリダイレクトされたすべてのセッションに関する許可変更（CoA）を発行します。

同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。

多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。

ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、「ポリシー サービス ノード グループの作成 （65 ページ）」を参照してください。

# PSN 間で均等に要求を分散するためのロード バランサ

展開内に複数のポリシー サービス ノードがある場合、ロード バランサを使用して要求を均等に分散できます。ロードバランサは、その背後にある機能ノードに要求を分散します。ロードバランサの背後に PSN を展開する詳細とベスト プラクティスについては、『Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP』を参照してください。

# ポリシー サービス ノードでのセッション フェールオーバー

アクティブな URL にリダイレクトされたセッションがあるポリシー サービス ノードがダウンすると、エンドポイントが中間状態となります。リダイレクトエンドポイントが通信していたポリシー サービス ノードのダウンを検出した場合でも、許可を再開することはできません。

ポリシー サービス ノードがノード グループに属している場合は、ノード グループ内のノード間でハートビート メッセージが交換され、ノードの障害が検出されます。ノードに障害が発生した場合、ノード グループのピアの 1 つによって、障害が発生したノードのアクティブな URL にリダイレクトされたセッションが学習され、それらのセッションへの接続を解除するための CoA が発行されます。

その結果、同じノード グループで使用可能な別のポリシー サービス ノードによって、セッションが処理されます。セッション フェールオーバーでは、ダウンしたポリシー サービス ノードから使用可能なポリシー サービス ノードにセッションが自動的に移動しませんが、セッションを移動するための CoA が発行されます。

# ポリシー サービス ノード グループ内のノード数

ノード グループに含めることができるノードの数は、展開要件によって異なります。ノード グループを使用すると、確実に、ノードの障害が検出され、許可されたがポスチャされていないセッションに関する CoA がピアによって発行されます。ノード グループのサイズはあまり大きくする必要はありません。

ノードグループのサイズが増加すると、ノード間で交換されるメッセージおよびハートビートの数が大幅に増加します。その結果、トラフィックも増加します。ノードグループ内のノードの数を少なくすることで、トラフィックを削減でき、同時にポリシー サービス ノードの障害を検出するのに十分な冗長性が提供されます。

ノード グループ クラスタに含めることができるポリシー サービス ノードの数にはハード制限はありません。

# ライト データ ディストリビューション

ライト データ ディストリビューションを使用すると、ユーザセッション情報を保存し、展開の PSN 全体で複製できるため、ユーザセッションの詳細について、PAN または MnT ノードから完全に独立できます。

ライト データ ディストリビューションは、次の 2 つのディレクトリから構成されています。

- Radius セッションディレクトリ
- エンドポイント オーナー ディレクトリ

さらに、[詳細設定（Advanced Settings）] から次のオプションを設定できます。

- バッチ サイズ（Batch Size）：セッション更新をバッチで送信できます。この値は、ライト データ ディストリビューション インスタンスから展開内の他の PSN に各バッチで送信するレコードの数を指定します。このフィールドを 1 に設定すると、セッション更新はバッチで送信されません。デフォルト値は 10 です。
- TTL：この値は、ライト データ ディストリビューションの更新が完了するまでバッチのセッションが待機する最大時間を指定します。デフォルト値は、1000 ミリ秒です。

PSN 間の接続不良の場合（PSN がダウンした場合など）、セッションの詳細を MnT セッション ディレクトリから取得し、今後使用するために保存されます。

大規模展開では、最大2,000,000セッション レコードを保持できます。小規模展開では、1,000,000 セッション レコードを保存できます。セッションのアカウンティングの停止要求を受信すると、対応するセッション データがすべてのライト データ ディストリビューション インスタンスから削除されます。保存されているレコードの数が上限を超えると、タイムスタンプに基づいて最も古いセッションが削除されます。

（注）

- セッションの IPv6 プレフィックス長が 128 ビット未満で、インターフェイス ID が指定されていない場合、IPv6プレフィックスは拒否されるため、複数のセッションで同じキーが使用されることはありません。
- ライト データ ディストリビューションは、ノード間通信に ISE メッセージングサービスを使用します。ISE メッセージング サービスは、さまざまな証明書（内部 CA のチェーンで署名された証明書）を使用します。ISE メッセージング サービスで問題が発生する場合は、ISE メッセージング サービス証明書を再生成する必要があります。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）] の順に選択します。このセクションで、[証明書（Certificate(s)）] の [ISEメッセージングサービス（ISE Messaging service）] を選択します。[ISEメッセージングサービス証明書の生成（generate ISE messaging service certificate）] をクリックします。

# Radius セッションディレクトリ

[RADIUS セッションディレクトリ（RADIUS Session Directory）] は、ユーザセッション情報を保存し、展開の PSN 全体に複製するために使用されます。[RADIUS セッションディレクトリ（RADIUS Session Directory）] には、認可変更（CoA）に必要なセッション属性のみが保存されます。

この機能は、Cisco ISE リリース 2.7 以降ではデフォルトで有効になっています。この機能を有効または無効にするには、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ライト データ ディストリビューション（Light Data Distribution）]** を選択し、[RADIUS セッションディレクトリ（RADIUS Session Directory）] チェックボックスをオンまたはオフにします。

# エンドポイント オーナー ディレクトリ

Cisco ISE リリース 2.6 までは、エンドポイントのプローブがその特定のエンドポイントの要求を最初に処理したものとは異なるポリシーサービスノード（PSN）で受信されると、エンドポイントのオーナーが新しい PSN に変更されます。これにより、エンドポイントの所有権のフラッピングが発生します。

Cisco ISE リリース2.7 では、[エンドポイント オーナーディレクトリ（Endpoint Owner Directory）] を使用して、Cisco ISE に接続している各 MAC アドレスの PSN FQDN を保存し、このデータを展開内の PSN 全体に複製します。これにより、すべての PSN がすべてのエンドポイントのオーナーを認識するため、エンドポイントの所有権のフラッピングが回避されます。エンドポイントの所有権は、そのエンドポイントの RADIUS 認証が別の PSN で成功した場合にのみ変更されるようになりました。

さらに、静的なエンドポイントの割り当てが着信プローブで受信された同じエンドポイントの属性よりも優先されるため、属性のオーバーライドの問題が回避されます。

この機能は、Cisco ISE リリース 2.7 以降ではデフォルトで有効になっています。必要な場合、これを無効にして、エンドポイント オーナー ディレクトリを使用していない古いメカニズムにフォールバックできます。[エンドポイント オーナー ディレクトリ（Endpoint Owner Directory）] は、プロファイリングでも使用されます。このオプションを無効にすると、レガシープロファイラのオーナーディレクトリが使用されます。この機能を有効または無効にするには、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ライト データ ディストリビューション（Light Data Distribution）]** を選択し、[エンドポイント オーナー ディレクトリの有効化（Enable Endpoint Owner Directory）] チェックボックスをオンまたはオフにします。

# モニタリング ノード

モニタリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシー サービス ノードからのログ メッセージを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度な監視およびトラブルシューティング ツールを提供します。このペルソナのノードは、収集するデータを集約して関連付けて、意味のある情報をレポートの形で提供します。

Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担うことができるこのペルソナを持つノードを最大 2 つ使用してハイ アベイラビリティを実現できます。プライマリ モニタリング ノードおよびセカンダリ モニタリング ノードの両方で、ログ メッセージを収集します。プライマリ モニタリング ノードがダウンした場合、プライマリ PAN はモニタリング データを収集するセカンダリ ノードを指定します。ただし、セカンダリ ノードがプライマリに自動的に昇格されることはありません。このためには、MnT ロールの手動変更必要があります。

分散セットアップでは、少なくとも 1 つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニタリング ペルソナとポリシー サービス ペルソナを有効にしないことを推奨します。最適なパフォーマンスを実現するために、ノードをモニタリング専用とすることを推奨します。

展開内の PANから [モニタリング（Monitoring）] メニューにアクセスできます。

## MnT ロールの手動変更

プライマリ PAN から MnT ロールを手動で変更できます（プライマリからセカンダリとセカンダリからプライマリの両方）。

**ステップ 1** プライマリ PAN のユーザ インターフェイスにログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** ロールを変更する MnT ノードをノード リストから選択します。

**ステップ 4** [編集（Edit）] をクリックします。

**ステップ 5** [モニタリング（Monitoring）] セクションで、[プライマリ/セカンダリ（Primary/ Secondary）] にロールを変更します。

**ステップ 6** [保存（Save）] をクリックします。

（注） そのノードで有効になっている他のすべてのペルソナおよびサービスを無効にする場合は、[専用MnT（Dedicated MnT）] オプションを有効にします。このオプションを有効にすると、設定データ レプリケーションプロセスがそのノードで停止します。これにより、モニタリング ノードのパフォーマンスが向上します。このオプションを無効にすると、手動同期がトリガーされます。

# Cisco ISE メッセージングを介した syslog

Cisco ISE 2.6 は、[MnTにUDP Syslogを伝送するためにISEメッセージングサービスを使用（Use ISE Messaging Service for UDP Syslogs delivery to MnT）] オプションによって、組み込みの UDP syslog 収集ターゲット（LogCollector および LogCollector2）用の MnT WAN 存続可能性を提供します。このオプションは、Cisco ISE 2.6 First Customer Ship（FCS）ではデフォルトで無効になっています。このオプションは、Cisco ISE リリース 2.6 累積パッチ 2 以降ではデフォルトで有効になっています。

UDP syslog に ISE メッセージングサービスを使用すると、MnT ノードにアクセスできなくても、運用データは一定期間保持されます。MnT WAN 存続可能性の期間は約 2 時間 30 分です。

このサービスは、TCP ポート 8671 を使用します。それに応じてネットワークを設定し、展開内の他のすべての ISE ノードから各 ISE ノードの TCP ポート 8671 への接続を許可してください。また、 Light Session Directory（『*Cisco Identity Service Engine Administrator Guide*』の「Set Up Cisco ISE in a Distributed Environment」の章の「Light Session Directory」の項を参照）、およびプロファイラ永続キューも ISE メッセージングサービスを使用しています。

（注） 展開で ISE 展開に TCP/Secure syslog を使用する場合、機能は以前のリリースと同じままです。

### キューリンクアラーム

ISE メッセージングサービスは、内部 CA チェーンによって署名された別の証明書を使用します。**[管理（Administration）] > [アラーム（Alarms）]** ウィンドウに、`queue-link alarm` が表示される場合があります。このアラームは、展開へのノードの登録、PPAN からのノード、非同期状態のノード、またはアプリケーションサービスが再起動しているノードでの同期などの導入操作を実行している場合に想定されます。アラームを解決するには、次のことを確認します。

- すべてのノードが接続され、同期されている。
- すべてのノードと ISE メッセージングサービスが機能している。
- ISE メッセージング サービス ポートは、ファイアウォールなどの外部エンティティによってブロックされていない。

- 各ノードの ISE メッセージング証明書チェーンが破損しておらず、証明書の状態が良好である。

上記の前提条件が満たされている場合は、次のアクションによって queue-link アラームがトリガーされます。

- PAN または PSN のドメイン名またはホスト名の変更。
- 新しい展開でのバックアップの復元。
- アップグレード後に古いプライマリ PAN を新しいプライマリ PAN に昇格。

queue-link アラームを解決するには、ISE ルート CA チェーンを再生成します。[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[証明書の管理（Certificate Management）]>[証明書署名要求（Certificate Signing Requests）] の順に選択します。[証明書署名要求（CSR）の生成（Generate Certificate Signing Requests（CSR））] をクリックします。[証明書の使用先（Certificate(s) will be used for）] ドロップダウンリストから [ISEルートCA（ISE Root CA）] を選択します。[ISEルートCA証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

MnT への UDP Syslog の伝送用に ISE メッセージングサービスを有効または無効にするには：

**ステップ 1** [管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ログ設定（Log Settings）] の順に選択します。**ISE ルート CA**

**ステップ 2** UDP syslog の伝送に ISE メッセージング サービスを使用するか、使用しない場合は、[MnTにUDP Syslogを伝送するためにISEメッセージングサービスを使用（Use ISE Messaging Service for UDP Syslogs delivery to MnT）] オプションをオンにするか、オフにします。

**ステップ 3** [保存（Save）] をクリックします。

# モニタリング ノードでの自動フェールオーバー

モニタリング ノードはハイ アベイラビリティを提供しませんが、アクティブ スタンバイを提供します。ポリシー サービス ノード（PSN）は、プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方に操作監査データをコピーします。

### 自動フェールオーバー プロセス

プライマリ モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードがすべてのモニタリング情報およびトラブルシューティング情報を引き継ぎます。

セカンダリ モニタリング ノードをプライマリ ノードに手動で変換するために、MnT ロールの手動変更。セカンダリ ノードが昇格された後にプライマリ ノードが復旧した場合、プライマリ ノードはセカンダリ ロールを担当します。セカンダリ ノードが昇格されなかった場合、プライマリ モニタリング ノードは、復旧後にプライマリ ロールを再開します。

⚠

**注意** プライマリ ノードがフェールオーバー後に復旧すると、セカンダリのバックアップを取得してデータを復元し、プライマリ ノードを最新の状態にします。

### モニタリング ノードのアクティブ/スタンバイ ペアを設定するためのガイドライン

ISE ネットワークでは 2 つのモニタリング ノードを指定して、アクティブ/スタンバイ ペアを設定できます。プライマリ モニタリング ノードをバックアップし、新しいセカンダリ モニタリング ノードにデータを復元することを推奨します。これにより、プライマリが新しいデータを複製するため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期されます。アクティブ/スタンバイ ペアには、次のルールが適用されます。

- すべての変更は、プライマリ モニタリング ノードに記録されます。セカンダリ ノードは読み取り専用です。
- プライマリ ノードで行った変更は、セカンダリ ノードに自動的に複製されます。
- プライマリ ノードとセカンダリ ノードは両方とも、他のノードがログを送信するログ コレクタとしてリストされます。
- Cisco ISE ダッシュボードは、モニタリングおよびトラブルシューティングの主要なエントリ ポイントとなります。PAN からのモニタリング情報は、ダッシュボードに表示されます。プライマリ ノードがダウンした場合、セカンダリ ノードでモニタリング情報が利用できます。
- モニタリング データのバックアップおよび消去は、標準 Cisco ISE ノードのバックアップ プロセスでは行われません。プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定し、それぞれに同じリポジトリを使用する必要があります。

### モニタリング ノードのフェールオーバー シナリオ

次のシナリオは、モニタリング ノード数に応じてアクティブ/スタンバイまたは単一ノード構成に適用されます。

- モニタリング ノードのアクティブ/スタンバイ構成では、プライマリ管理ノード（PAN）は、常にプライマリ モニタリング ノードに接続してモニタリング データを収集します。プライマリ モニタリング ノードに障害が発生した後に、PAN はスタンバイ モニタリング スタンバイ ノードに接続します。プライマリ モニタリング ノードからスタンバイ モニタリング ノードへのフェールオーバーは、プライマリ モニタリング ノードのダウンから 5 分以上経過した後に行われます。

  ただし、プライマリ ノードに障害が発生した後、スタンバイ ノードはプライマリ ノードになりません。プライマリ ノードが復旧すると、管理ノードは再開されたプライマリ ノードからのモニタリング データの収集を再び開始します。
- プライマリ モニタリング ノードがダウンしたときに、スタンバイ モニタリング ノードをアクティブ ステータスに昇格する場合は、MnT ロールの手動変更、既存のプライマリ モ

ニタリング ノードを登録解除して、スタンバイ モニタリング ノードをプライマリに昇格することができます。既存のプライマリ モニタリング ノードを登録解除すると、スタンバイ ノードがプライマリ モニタリング ノードになり、PAN は新しく昇格されたプライマリ ノードに自動的に接続します。

- アクティブ/スタンバイ ペアで、セカンダリ モニタリング ノードを登録解除するか、またはセカンダリ モニタリング ノードがダウンした場合、既存のプライマリ モニタリング ノードが現在のプライマリ ノードのままになります。
- ISE 展開内にモニタリング ノードが 1 つだけ存在する場合、そのノードはプライマリ モニタリング ノードとして機能し、PAN にモニタリング データを提供します。ただし、新しいモニタリング ノードを登録して展開内でプライマリ ノードにすると、既存のプライマリ モニタリング ノードは自動的にスタンバイ ノードになります。PAN は、新しく登録されたプライマリ モニタリング ノードに接続し、モニタリング データを収集します。

# モニタリング データベース

モニタリング機能によって利用されるデータ レートおよびデータ量には、これらの目的専用のノード上に別のデータベースが必要です。

ポリシー サービスと同様に、モニタリングには専用のデータベースがあり、この項で説明するトピックのようなメンテナンス タスクを実行する必要があります。

## モニタリング データベースのバックアップと復元

モニタリング データベースは、大量のデータを処理します。時間が経つにつれ、モニタリング ノードのパフォーマンスと効率は、そのデータをどう管理するかによって変わってきます。効率を高めるために、データを定期的にバックアップして、それをリモートのリポジトリに転送することを推奨します。このタスクは、自動バックアップをスケジュールすることによって自動化できます。

（注） 消去操作の実行中には、バックアップを実行しないでください。消去操作の実行中にバックアップが開始されると、消去操作が停止または失敗します。

セカンダリ モニタリング ノードを登録する場合は、最初にプライマリ モニタリング ノードをバックアップしてから、新しいセカンダリ モニタリング ノードにデータを復元することを推奨します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。

## モニタリング データベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、モニタリング データベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク領

域使用率しきい値（ディスク領域のパーセンテージ）に達したときに使用されます。このオプションでは、各月は 30 日で構成されます。デフォルトの 3 ヵ月は 90 日間です。

# モニタリング データベースの消去に関するガイドライン

次に、モニタリングデータベースのディスク使用に関連して従うべきガイドラインをいくつか示します。

- モニタリング データベースのディスク使用量がしきい値設定の 80% を超えた場合、データベース サイズが割り当てられたディスク サイズを超過したことを示すクリティカル アラームが生成されます。ディスク使用量が 90% より大きい場合は、別のアラームが生成されます。

  消去プロセスが実行され、ステータス履歴レポートが作成されます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [展開ステータス（Deployment Status）] > [データ消去の監査（Data Purging Audit）]** を選択して表示できます。消去の完了時に情報（INFO）アラームが生成されます。

- 消去は、データベースの使用済みディスク領域のパーセンテージにも基づきます。モニタリング データベースの使用済みディスク領域がしきい値（デフォルトは 80%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、過去 7 日間のモニタリング データのみを削除します。ディスク領域が 80% 未満になるまで繰り返しプロセスを続行します。消去では、処理の前にモニタリングデータベースのディスク領域制限が常にチェックされます。

# 運用データの消去

ISE MnT 運用（OPS）データベースには、ISE レポートに生成される情報が含まれています。最近の ISE リリースでは、ISE admin CLI コマンド **application configure ise** を実行した後に、[M&T運用データを消去（Purge M&T Operational Data）] と [M&Tデータベースをリセット（Reset M&T Database）] のオプションを使用します。

パージオプションは、データのクリーンアップに使用します。また、保持する日数を尋ねるプロンプトを表示します。リセットオプションを使用すると、データベースが工場出荷時の初期状態にリセットされるため、バックアップされているすべてのデータが完全に削除されます。ファイルがファイルシステム領域を過度に消費している場合、データベースをリセットすることができます。

（注） リセットオプションを使用すると、再起動するまで、ISEサービスが一時的に利用できなくなります。

[運用データの消去（Operational Data Purging）] ページ（[管理（Administration）] > [システム（System）]> [メンテナンス（Maintenance）]> [運用データの消去（Operational Data Purging）]）には、[データベースの使用状況（Database Utilization）] 領域と [データを今すぐ消去（Purge Data Now）] 領域があります。[データベースの使用状況（Database Utilization）] 領域には、使

用可能なデータベース容量の合計と、保存されている RADIUS および TACACS データが表示されます。ステータスバーをマウスオーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。RADIUS データと TACACS データを保持できる期間を [データ保存期間（Data Retention Period）] 領域に指定できます。データは毎朝午前4時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにして、リポジトリを選択して作成し、暗号キーを指定できます。

[データを今すぐ消去（Purge Data Now）] 領域では、すべての RADIUS および TACACS データを消去するか、またはデータ消去までに保存できる日数を指定できます。

（注） 消去前にリポジトリにエクスポートできるテーブルは、RADIUS 認証およびアカウンティング、TACACS 認証およびアカウンティング、RADIUS エラー、および設定が誤っているサプリカントの各テーブルです。

**関連トピック**

古い運用データの消去 （53 ページ）

# 古い運用データの消去

運用データはサーバに一定期間集められています。すぐに削除することも、定期的に削除することもできます。データ消去の監査レポートを表示して、データ消去が成功したかどうかを確認できます。

### 始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [データ保持期間（Data Retention Period ）] 領域で次の操作を行います。

  1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。
  2. [リポジトリ（Repository）] 領域で、[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、データを保存するリポジトリを選択します。詳細については、「リポジトリの作成」の項を参照してください。
  3. [暗号キー（Encryption Key）] テキスト ボックスに必要なパスワードを入力します。
  4. [保存（Save）] をクリックします。

（注） 設定した保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日に設定し、この値が診断テーブルの既存のしきい値（たとえば、5 日のデフォルト）未満の場合、データはこのページで設定した値（3 日）に従って消去されます。

- [データを今すぐ消去（Purge Data Now）] 領域で、次の操作を行います。

1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
2. [消去（Purge）] をクリックします。

# 自動フェールオーバー用のモニタリング ノードの設定

展開に 2 つのモニタリング ISE ノードがある場合は、自動フェールオーバーのプライマリ-セカンダリ ペアを設定して、Cisco ISE モニタリング サービスのダウンタイムを回避します。プライマリ-セカンダリ ペアによって、プライマリ ノードに障害が発生した場合に、セカンダリ モニタリング ノードが自動的にモニタリングを提供します。

### 始める前に

- 自動フェールオーバー用のモニタリング ノードを設定するには、モニタリング ノードが Cisco ISE ノードとして登録されている必要があります。
- 両方のノードでモニタリング ロールおよびサービスを設定し、必要に応じてこれらのノードにプライマリ ロールおよびセカンダリ ロールの名前を付けます。
- プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定します。バックアップおよび消去を正しく動作させるには、両方のノードに同じリポジトリを使用します。消去は、冗長ペアのプライマリ ノードおよびセカンダリ ノードの両方で行われます。たとえば、プライマリ モニタリング ノードでバックアップおよび消去用に 2 つのリポジトリが使用されている場合、同じリポジトリをセカンダリ ノードに指定する必要があります。

  システム CLI の **repository** コマンドを使用してモニタリング ノードのデータ リポジトリを設定します。

⚠

**注意** スケジュール バックアップと消去をモニタリング冗長ペアのノードで正しく動作させるには、CLI を使用して、プライマリ ノードとセカンダリ ノードの両方で同じリポジトリを設定します。リポジトリは、2 つのノードの間で自動的に同期されません。

Cisco ISE ダッシュボードで、モニタリング ノードの準備ができていることを確認します。[システム概要（System Summary）] ダッシュレットに、サービスが準備完了の場合は左側に緑色のチェック マークが付いたモニタリング ノードが表示されます。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 2** [展開ノード（Deployment Nodes）] ページで、アクティブとして指定するモニタリング ノードの隣にあるチェックボックスをオンにし、**Edit** をクリックします。

**ステップ 3** [全般設定（General Settings）] タブをクリックし、[ロール（Role）] ドロップダウン リストから [プライマリ（Primary）] を選択します。

1 つのモニタリング ノードをプライマリとして選択すると、もう 1 つのモニタリング ノードが自動的にセカンダリとなります。スタンドアロン展開の場合、プライマリおよびセカンダリのロール設定は無効になります。

**ステップ 4** **Save** をクリックします。アクティブ ノードおよびスタンバイ ノードが再起動します。

# pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッション ディレクトリからの状況依存情報を、ISE エコ システムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。また、pxGrid フレームワークは、Cisco ISE とサード パーティのベンダー間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用でき、その他の情報交換にも使用できます。また、pxGrid では、サードパーティ システムが適応型ネットワーク制御アクション（EPS）を起動して、ネットワーク イベントまたはセキュリティ イベントに応答してユーザ/デバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイント プロファイルは、エンドポイント プロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング（IP-SGT マッピング）を発行および受信登録できます。SXP バインディングの詳細については、セキュリティ グループ タグの交換プロトコルを参照してください。

ハイ アベイラビリティ設定で、Cisco pxGrid サーバは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバの PAN をアクティブにするには、手動で昇格する必要があります。[pxGrid サービス（pxGrid Services）] ページ（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）を調べ、pxGrid ノードが現在アクティブであるか、スタンバイ状態であるかを確認できます。

XMPP（Extensible Messaging and Presence Protocol）クライアントの場合、pxGrid ノードはアクティブ/スタンバイの高可用性モードで動作します。つまり、pxGridサービスはアクティブ ノード上では「実行中」状態で、スタンバイ ノードでは「無効」状態です。

セカンダリ pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ pxGrid ノードがネットワークに戻された場合、元のプライマリ pxGrid ノードは引き続きセカンダリ ロールを持ち、現在のプライマリ ノードがダウンしない限り、プライマリ ロールに昇格されません。

（注） 時々、元のプライマリ pxGrid ノードがプライマリ ロールに自動的に昇格されることがあります。

ハイ アベイラビリティ展開では、プライマリ pxGrid ノードがダウンすると、セカンダリ pxGrid ノードに切り替えるのに約 3 ～ 5 分かかることがあります。プライマリ pxGrid ノードに障害が発生した場合は、キャッシュ データを消去する前に、クライアントはスイッチオーバーが完了するまで待機することを推奨します。

pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更通知。
- pxgrid-cm.log：パブリッシャ/サブスクライバおよびクライアントとサーバ間のデータ交換アクティビティの更新。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログ。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関する情報。

（注） ノードで pxGrid サービスが無効になっている場合、ポート 5222 はダウンしますが、（Web クライアントで使用される）ポート 8910 は機能し、引き続き要求に応答します。

（注） Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、 のアップグレード ライセンスを最近インストールしている場合には、Base インストールで特定の拡張 pxGrid サービスが使用可能である可能性があります。

（注） パッシブ ID ワーク センターを使用するには pxGrid を定義する必要があります。詳細については、PassiveID ワークセンターを参照してください。

# pxGrid クライアントおよび機能の管理

Cisco ISE に接続するクライアントは、pxGrid サービスを使用する前に、アカウントを登録し、承認を受ける必要があります。pxGrid クライアントは、クライアントになるために pxGrid SDK を介してシスコから利用可能な pxGrid クライアントライブラリを使用します。Cisco ISE は、自動および手動承認の両方をサポートします。クライアントは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された pxGrid サーバのホスト名または IP アドレスに接続できます。

pxGrid の「機能」は、クライアントの pxGrid 上の情報トピックまたはチャネルであり、これらは公開および登録されます。Cisco ISE では、ID、適応型ネットワーク制御、SGA などの機能のみがサポートされます。クライアントが新しい機能を作成すると、その機能は **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]** に表示されます。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャから入手してください。

（注） pxGrid セッション グループが EPS グループの一部であるため、EPS ユーザ グループに割り当てられたユーザはセッション グループで操作を実行できます。ユーザが EPS グループに割り当てられると、ユーザは pxGrid クライアントのセッションのグループに加入できます。

### 関連トピック

pxGrid 証明書の生成 （60 ページ）

# pxGrid クライアントの有効化

### 始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。**[管理（Administration）] > [展開（Deployment）]** を選択し、必要なノードにチェックマークを付け、[編集（Edit）] をクリックします。設定画面で [パッシブ ID サービスを有効にする（Enable Passive Identity Service）] をオンにします。

**ステップ 1** **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。

**ステップ 2** クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

**ステップ 3** [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

# pxGrid 機能の有効化

### 始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- pxGrid クライアントをイネーブルにします。

**ステップ 1** **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。

**ステップ 2** 右上の [機能別に表示（View by Capabilities）] をクリックします。

**ステップ 3** 有効にする機能を選択し、[有効（Enable）] をクリックします。

**ステップ 4** [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

# ISE pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

### 始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。
- Cisco pxGrid サービスは、Cisco ISE SNS 3415/3495 アプライアンス上または VMware で実行されます。
- すべてのノードは、pxGrid 用に CA 証明書を使用するように設定されています。アップグレード前にデフォルトの証明書を pxGrid に使用する場合、アップグレード後にこの証明書は内部 CA 証明書に置き換えられます。
- 分散展開を使用しているか、または Cisco ISE 1.2 からアップグレードする場合は、証明書で [pxGrid 使用（pxGrid Usage）] オプションを有効にする必要があります。[pxGrid 使用（pxGrid Usage）] オプションを有効にするには、**[管理（Administration）] > [証明書（Certificates）] > [システム証明書（Certificates）]** に移動します。展開に使用される証明書を選択し、[編集（Edit）] をクリックします。pxGrid を確認します。[pxGrid コントローラ（pxGrid Controller）] チェックボックスの証明書を使用します。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 2** [展開ノード（Deployment Nodes）] ページで、pxGrid サービスを有効にするノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

**ステップ 3** [全般設定（General Settings）] タブをクリックし、[pxGrid] チェックボックスをオンにします。

**ステップ 4** [保存（Save）] をクリックします。

以前のバージョンからアップグレードするとき、[保存（Save）]オプションが無効になる場合があります。このことは、ブラウザ キャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存（Save）] オプションを有効にするには、ブラウザ キャッシュを消去します。

# Cisco pxGrid ライブ ログ

[ライブ ログ（Live Logs）] ページには、すべての pxGrid 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベント タイプとタイムスタンプが含まれています。

**[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブ ログ（Live Log）]** の順に移動して、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

# pxGrid の設定

### 始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

**ステップ 1** [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] を選択します。

**ステップ 2** 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認（Automatically Approve New Accounts）：このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可（Allow Password Based Account Creation）：このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワード ベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

**ステップ 3** [保存（Save）] をクリックします。

[pxGrid の設定（pxGrid Settings ）] ページで [テスト（Test）] オプションを使用して、pxGrid ノードでヘルス チェックを実行します。pxgrid/pxgrid-test.log ファイルで詳細を確認できます。

# pxGrid 証明書の生成

### 始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- PxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。

**ステップ 1** [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] の順に選択します。

**ステップ 2** [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム（CN）を入力する必要があります。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。
- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- ルート証明書チェーンのダウンロード（Download root certificate chain）：ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

[証明書テンプレート（Certificate Templates）] リンクから証明書テンプレートをダウンロードし、必要に応じて、テンプレートを編集できます。

**ステップ 3** （[単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] オプションを選択した場合は必須）pxGrid クライアントの FQDN を入力します。

**ステップ 4** （オプション）この証明書の説明を入力できます。

**ステップ 5** サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- IP アドレス（IP address）：この証明書に関連付ける pxGrid クライアントの IP アドレスを入力します。
- FQDN：pxGrid の完全修飾ドメイン名を入力します。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

**ステップ 6** [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンド エンティティの証明書と秘密キーを格納するバイナリ形式。

**ステップ 7** 証明書のパスワードを入力します。

**ステップ 8** [作成（Create）] をクリックします。

作成した証明書は、ISE の **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** に表示され、ブラウザのダウンロード ディレクトリにダウンロードされます。

# pxGrid クライアントの権限の制御

pxGrid クライアントの権限を制御するために、pxGrid 許可ルールを作成できます。これらのルールを使用して、pxGrid クライアントに提供されるサービスを制御します。

さまざまな種類のグループを作成し、pxGrid クライアントに提供されるサービスをこれらのグループにマッピングできます。[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して、新しいグループを追加します。[権限（Permissions）] ウィンドウで、事前定義されたグループ（EPS や ANC など）を使用する事前定義された許可ルールを表示できます。事前定義されたルールでは [操作（Operations）] フィールドだけを更新できることに注意してください。

pxGrid クライアントの許可ルールを作成するには、以下の手順を実行します。

**ステップ 1** [管理（Administration）] タブから、[pxGridサービス（pxGrid Services）] > [権限（Permissions）] を選択します。

**ステップ 2** [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**

- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

**ステップ 3** [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **<ANY>**
- **パブリッシュ**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

（注） このオプションを選択すると、カスタム操作を指定できます。

**ステップ 4** [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

（EPS や ANC などの）事前定義されたグループ、および（[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して）手動で追加されたグループが、このドロップダウン リストに表示されます。

# 展開内のノードの表示

[展開ノード（Deployment Nodes）] ページで、展開を構成するすべての Cisco ISE ノード、プライマリ ノードおよびセカンダリ ノードを表示できます。

**ステップ 1** プライマリ Cisco ISE 管理者ポータルにログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** 左側のナビゲーション ペインで、 [展開（Deployment）] をクリックします。

展開を構成するすべての Cisco ISE ノードが表示されます。

# モニタリングノードからのエンドポイント統計データのダウンロード

モニタリング ノードからネットワークに接続するエンドポイントの統計データをダウンロードできます。ロード、CPU使用率、認証トラフィック データを含む主要パフォーマンス メトリック（KPM）が使用可能で、ネットワークの問題の監視およびトラブルシューティングに使用できます。日次 KPM 統計情報または過去 8 週間の KPM 統計情報をそれぞれダウンロードするには、Cisco ISE コマンドライン インターフェイス（CLI）から、**application configure ise** コマンドを使用し、オプション 12 または 13 を使用します。

このコマンドの出力では、エンドポイントに関する次のデータが提供されます。

- ネットワーク上のエンドポイントの総数
- 正常な接続を確立したエンドポイントの数
- 認証に失敗したエンドポイントの数。
- 毎日の接続済みの新しいエンドポイントの総数
- 毎日のオンボーディングしたエンドポイントの総数

出力には、タイムスタンプの詳細、展開内の各ポリシー サービス ノード（PSN）を介して接続したエンドポイントの総数、エンドポイントの総数、アクティブエンドポイント、負荷、および認証トラフィックの詳細も含まれています。

このコマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

# データベースのクラッシュまたはファイルの破損の問題

Cisco ISE は、データ損失が発生する停電またはその他の理由により、Oracle データベース ファイルが破損している場合にクラッシュすることがあります。インシデントに応じて、データ損失から回復するには、次の手順を実行します。

- 展開で PAN が破損した場合は、セカンダリ PAN をプライマリ PAN に昇格する必要があります。
- 小規模な展開またはその他の理由により、SPAN を昇格できない場合は、利用可能な最新のバックアップを復元します。
- PSN が破損した場合は、次の手順を実行して、登録解除、設定のリセット、ノードの再登録を行います。
- スタンドアロン ボックスの場合、利用可能な最新のバックアップを復元します。

（注） 最新の設定変更が失われないようにするために、スタンドアロンボックスからバックアップを定期的に取得します。

# モニタリングのためのデバイス設定

モニタリングノードにより、ネットワーク上のデバイスからのデータが受信および使用されて、ダッシュボードに表示されます。モニタリングノードとネットワークデバイス間の通信を有効にするには、スイッチと NAD を正しく設定する必要があります。

# プライマリおよびセカンダリの Cisco ISE ノードの同期

Cisco ISE の設定に変更を加えることができるのは、プライマリ PAN からのみです。設定変更はすべてのセカンダリ ノードに複製されます。何らかの理由でこの複製が正しく実行されない場合は、プライマリ PAN に手動でセカンダリ PAN を同期できます。

### 始める前に

[同期ステータス（Sync Status）] が [同期していない（Out of Sync）] に設定されている場合や [複製ステータス（Replication Status）] が [失敗（Failed）] または [無効（Disabled）] の場合は、[同期を更新（Syncup）] ボタンをクリックして完全複製を強制的に実行する必要があります。

**ステップ 1** プライマリ PAN にログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** プライマリ PAN と同期させるノードの横にあるチェックボックスをオンにし、[同期を更新（Syncup）] をクリックして完全データベース複製を強制的に実行します。

# ノード ペルソナとサービスの変更

Cisco ISE ノードの設定を編集して、そのノードで実行されているペルソナおよびサービスを変更できます。

### 始める前に

- ポリシーサービス ノードで実行されるサービスを有効または無効にしたり、ポリシーサービス ノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。

- このサービスの再起動の遅延により、自動フェールオーバーが開始される場合があります（展開内で有効になっている場合）。これを回避するには、自動フェールオーバー設定がオフになっていることを確認します。

**ステップ 1** プライマリ PAN にログインします。

**ステップ 2** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 3** ペルソナまたはサービスを変更するノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

**ステップ 4** 必要なサービスおよびペルソナを選択します。

**ステップ 5** [保存（Save）] をクリックします。

**ステップ 6** プライマリ PAN でアラームの受信を確認して、ペルソナまたはサービスの変更を確認します。ペルソナまたはサービスの変更が正常に保存されなかった場合、アラームは生成されません。

# Cisco ISE でのノードの変更による影響

Cisco ISE ISE で次のいずれかの変更を行うと、そのノードが再起動するため、遅延が発生します。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）
- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- 管理ノードの昇格（セカンダリからプライマリへ）
- ペルソナの変更（ノードからポリシー サービスまたは監視ペルソナを割り当てたり、削除したりする場合）
- ポリシー サービス ノードでのサービスの変更（セッションとプロファイラ サービスを有効または無効にします）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）

# ポリシー サービス ノード グループの作成

2つ以上のポリシー サービス ノード（PSN）が同じ高速ローカル エリア ネットワーク（LAN）に接続されている場合は、同じノード グループに配置することを推奨します。この設計は、グループにローカルの重要度が低い属性を保持し、ネットワークのリモート ノードに複製される情報を減らすことによって、エンドポイント プロファイリング データのレプリケーションを

最適化します。ノード グループ メンバーは、ピア グループ メンバーの可用性もチェックします。グループがメンバーに障害が発生したことを検出すると、障害が発生したノードの URL にリダイレクトされたすべてのセッションをリセットし、回復することを試行します。

（注） すべての PSN を同じノード グループの同じローカル ネットワークの部分に置くことを推奨します。PSN は、同じノード グループに参加するために負荷分散クラスタの一部である必要はありません。ただし、負荷分散クラスタの各ローカル PSN は通常同じノード グループに属している必要があります。

ノード グループにメンバーとして PSN を追加する前に、最初にノード グループを作成する必要があります。管理者ポータルの [展開（Deployment）] ページで、ポリシー サービス ノード グループを作成、編集、および削除できます。

### 始める前に

ノード グループ メンバーは TCP/7800 を使用して通信できます。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 2** [アクション（action）] アイコンをクリックし、[ノード グループの作成（Create Node Group）] をクリックします。

**ステップ 3** ノード グループに付ける一意の名前を入力します。

**ステップ 4** （任意）ノード グループの説明を入力します。

**ステップ 5** （任意）[MAR キャッシュ分散の有効化（Enable MAR Cache Distribution）] チェックボックスをオンにし、その他のオプションを入力します。このオプションを有効にする前に、[Active Directory] ページで MAR が有効になっていることを確認してください。

**ステップ 6** [送信（Submit）] をクリックして、ノード グループを保存します。

ノードグループを保存すると、左側のナビゲーション ペインにそのグループが表示されます。左側のペインにノードグループが表示されていない場合、そのグループは非表示になっている可能性があります。非表示オブジェクトを表示するには、ナビゲーション ペインで [展開（Expand）] ボタンをクリックします。

### 次のタスク

ノード グループにノードを追加します。ノードを編集するには、[ノード グループのメンバー（Member of Node Group）] ドロップダウン リストからノード グループを選択します。

# 展開からのノードの削除

展開からノードを削除するには、ノードの登録を解除する必要があります。登録解除されたノードは、スタンドアロン Cisco ISE ノードになります。

これはプライマリ PAN から受信した最後の設定を保持し、管理、ポリシー サービス、およびモニタリングであるスタンドアロン ノードのデフォルトのペルソナを担当します。モニタリング ノードを登録解除した場合、このノードは syslog ターゲットではなくなります。

プライマリ PSN の登録が取り消されると、エンドポイント データは失われます。スタンドアロン ノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンドアロン ノードになったときに、このデータ バックアップを復元します。
- PSN のペルソナを管理者（セカンダリ PAN）に変更し、管理者ポータルの展開ページからデータを同期してから、ノードを登録解除します。この時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ PAN を追加できます。

プライマリ PAN の [展開（Deployment）] ページからこれらの変更を表示できます。ただし、変更が反映され、[展開（Deployment）] ページに表示されるには 5 分間の遅延が生じます。

### 始める前に

展開からセカンダリ ノードを削除する前に、必要に応じて後で復元できる Cisco ISE 設定のバックアップを実行します。

**ステップ 1** **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

**ステップ 2** 削除するセカンダリ ノードの隣のチェックボックスをオンにして、[登録解除（Deregister）] をクリックします。

**ステップ 3** [OK] をクリックします。

**ステップ 4** プライマリ PAN のアラームの受信を確認し、セカンダリ ノードが正常に登録解除されたことを確認します。セカンダリ ノードのプライマリ PAN からの登録解除が失敗した場合は、このアラームは生成されません。

# ISE ノードのシャットダウン

halt コマンドを実行する前に、Cisco ISE アプリケーション サービスを停止し、バックアップ、復元、インストール、アップグレード、または削除操作を実行中でないことを確認します。Cisco ISE がこれらのいずれかの操作を行っている間に halt コマンドを実行すると、次のいずれかの警告メッセージが表示されます。

```
WARNING: A backup or restore is currently in progress! Continue with halt?

WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

halt コマンドの使用時に他のプロセスが実行されていない場合、または表示される警告メッセージに応じて [はい（Yes）] をクリックした場合は、次の質問に応答する必要があります。

```
Do you want to save the current configuration?
```

[はい（Yes）] をクリックして既存の Cisco ISE 設定を保存すると、次のメッセージが表示されます。

```
Saved the running configuration to startup successfully.
```

（注） アプライアンスを再起動する前に、アプリケーション プロセスを停止することをお勧めします。

これは、ISE の再起動にも適用されます。詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

# スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更

スタンドアロン Cisco ISE ノードのホスト名、IP アドレス、またはドメイン名を変更できます。ノードのホスト名として「localhost」を使用することはできません。

### 始める前に

Cisco ISE ノードが分散展開の一部である場合、展開から削除し、スタンドアロン ノードであることを確認する必要があります。

**ステップ 1** Cisco ISE CLI から **hostname**、**ip address**、、または **ip domain-name** の各コマンドを使用して Cisco ISE ノードのホスト名または IP アドレスを変更します。

**ステップ 2** すべてのサービスを再起動するために、Cisco ISE CLI から **application stop ise** コマンドを使用して Cisco ISE アプリケーション設定をリセットします。

**ステップ 3** Cisco ISE ノードは、分散 展開の一部である場合、プライマリ PAN に登録します。

（注） Cisco ISE ノードの登録時にホスト名を使用する場合、登録するスタンドアロン ノードの完全修飾ドメイン名（FQDN）（たとえば、*abc.xyz.com*）は、プライマリ PAN から DNS を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバに、分散展開の一部である Cisco ISE ノードの IP アドレスと FQDN を入力する必要があります。

セカンダリ ノードとして Cisco ISE ノードを登録した後、プライマリ PAN は IP アドレス、ホスト名、またはドメイン名への変更を展開内の他の Cisco ISE ノードに複製します。

# Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。アップグレード前およびアップグレード後のタスクのリストについては、『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

[アップグレードの概要（Upgrade Overview）]ページには、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス（ノードがアクティブか非アクティブか）がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

## さまざまなタイプの展開

- スタンドアロン ノード：管理、ポリシー サービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。分散展開をアップグレードする手順については、次の参照先で説明しています。

ISE コミュニティ リソース

ネットワークが ISE 展開への準備ができているかどうかを評価する方法については、ISE Deployment Assistant（IDA）を参照してください。

## 分散展開のアップグレード

リリース 2.0 以降の管理者ポータルを使用して Cisco ISE 展開環境のすべてのノードをアップグレードすることもできます。また、Cisco ISE 2.0 以降の限定的な可用性リリースを一般的な可用性リリースにアップグレードすることもできます。

### 始める前に

アップグレードする前に、次の作業が完了していることを確認します。

- ISE の設定および運用データのバックアップを取得します。
- システム ログのバックアップを取得します。
- スケジュールしたバックアップを無効にします。展開のアップグレードが完了したら、バックアップ スケジュールを再設定します。
- 証明書および秘密キーをエクスポートします。
- リポジトリを設定します。アップグレードバンドルをダウンロードし、このリポジトリに格納します。

- Active Directory の参加クレデンシャルと RSA SecurID ノード秘密のメモを取ります（該当する場合）。この情報は、アップグレード後に Active Directory または RSA SecurID サーバに接続するために必要です。
- アップグレードのパフォーマンスを向上させるために、運用データを消去します。
- リポジトリとのインターネット接続が良好であることを確認します。

（注） リポジトリからノードにアップグレードバンドルをダウンロードする場合、ダウンロードが完了するまでに 35 分以上かかるとダウンロードがタイムアウトします。この問題は、インターネットの帯域幅が不十分なために発生します。

**ステップ 1** 管理者ポータルの [アップグレード（Upgrade）] タブをクリックします。

**ステップ 2** [続行（Proceed）] をクリックします。

[レビューチェックリスト（Review Checklist）] ウィンドウが表示されます。表示された手順を確認してください。

**ステップ 3** [チェックリストを確認済み（I have reviewed the checklist）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

[バンドルのノードへのダウンロード（Download Bundle to Nodes）] ウィンドウが表示されます。

**ステップ 4** リポジトリからノードにアップグレード バンドルをダウンロードします。

a) アップグレード バンドルをダウンロードするノードの隣のチェックボックスをオンにします。
b) [ダウンロード（Download）] をクリックします。

[リポジトリおよびバンドルの選択（Select Repository and Bundle）] ウィンドウが表示されます。

c) リポジトリを選択します。

異なるノードで同じリポジトリまたは異なるリポジトリを選択できますが、すべてのノードで同じアップグレード バンドルを選択する必要があります。

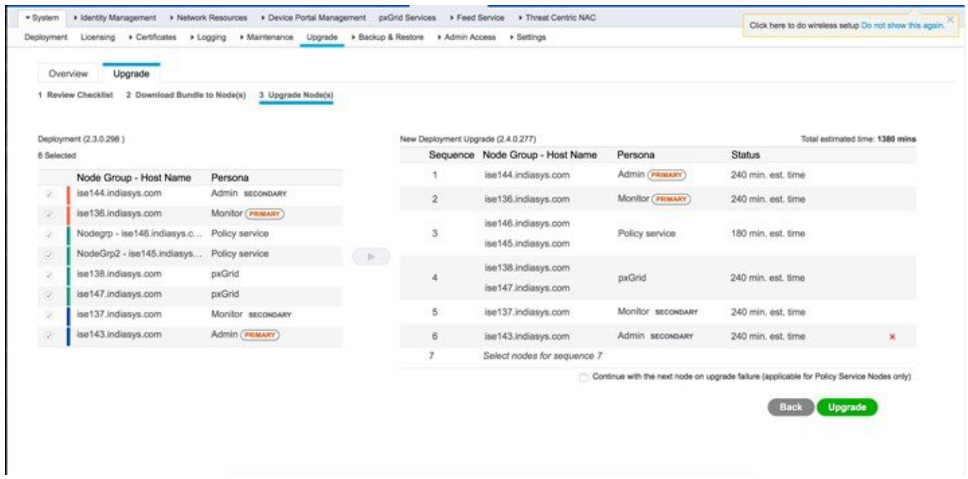
d) アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。
e) [確認（Confirm）] をクリックします。

バンドルがノードにダウンロードされると、ノード ステータスが [アップグレードの準備が整いました（Ready for Upgrade）] に変わります。

**ステップ 5** [続行（Continue）] をクリックします。

[ノードのアップグレード（Upgrade Nodes）] ウィンドウが表示されます。

図 *1* : 現在の展開と新しい展開を表示するアップグレード ウィンドウ




**ステップ 6** アップグレード順序を選択します。

ノードを新しい展開に移動すると、アップグレードの推定所要時間が [ノードのアップグレード（Upgrade Nodes）] ウィンドウに表示されます。この情報を使用して、アップグレードを計画し、ダウンタイムを最小化できます。管理ノードとモニタリング ノードのペアおよび複数のポリシー サービス ノードがある場合は、以下の手順に従います。

a) デフォルトでは、セカンダリ管理ノードは、アップグレード順序の最初にリストされています。アップグレード後に、このノードは新しい展開でプライマリ管理ノードになります。
b) プライマリ モニタリング ノードは、次に新しい展開にアップグレードされるノードです。
c) ポリシー サービス ノードを選択し、新しい展開に移動します。ポリシー サービス ノードをアップグレードする順序を変更できます。

   ポリシーサービスノードは、順番にまたは並行してアップグレードできます。ポリシーサービスノードのセットを選択し、並行してアップグレードできます。

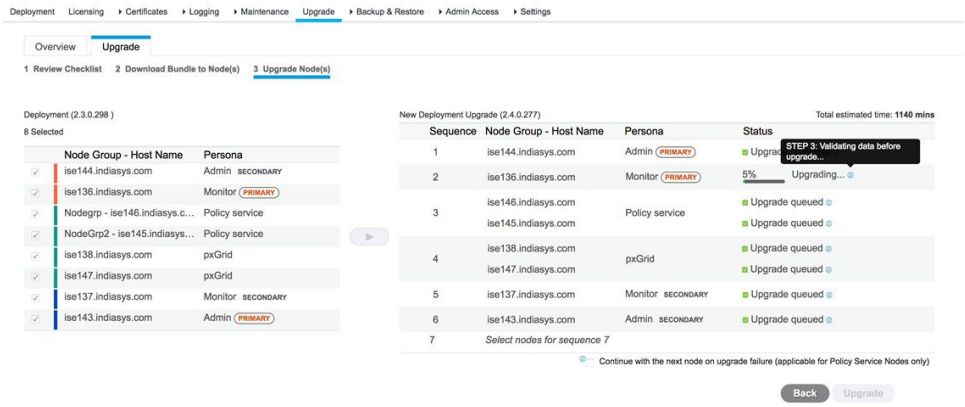
d) セカンダリ モニタリング ノードを選択し、新しい展開に移動します。
e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

**ステップ 7** アップグレードがアップグレード順序のいずれかのポリシーサービス ノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する（Continue with upgrade on failure）] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリ モニタリング ノードには適用されません。これらのノードのいずれかに障害が発生すると、アップグレード プロセスはロールバックされます。ポリシーサービス ノードのいずれかが失敗すると、セカンダリ モニタリング ノードおよびプライマリ管理ノードはアップグレードされず、古い展開内に残ります。

**ステップ 8** [アップグレード（Upgrade）] をクリックして、展開のアップグレードを開始します。

図 *2:* アップグレードの進行状況を表示する *[*アップグレード（***Upgrade***）*]* ウィンドウ




各ノードのアップグレードの進行状況が表示されます。正常に完了すると、ノードのステータスが[アップグレード完了（Upgrade Complete）] に変わります。

（注） 管理者ポータルからノードをアップグレードするときに、ステータスが長時間変化しない場合（80% のままの場合）は、CLI からアップグレードログをチェックするか、コンソールからアップグレードのステータスをチェックできます。アップグレードの進行状況を表示するには、CLI にログインするか、Cisco ISE ノードのコンソールを表示します。**show logging application** コマンドを使用すると、*upgrade-uibackend-cliconsole.log* および *upgrade-postosupgrade-yyyymmdd-xxxxxx.log* を表示できます。

show logging application コマンドを使用すると、CLI から次のアップグレードログを表示できます。

- DB データのアップグレードログ
- DB スキーマログ
- Post OS アップグレードログ

警告メッセージ「**The node has been reverted back to its pre-upgrade state**」が表示された場合は、**[アップグレード（Upgrade）]**ウィンドウに移動し、**[詳細（Details）]** リンクをクリックします。[アップグレードの失敗の詳細（Upgrade Failure Details）] ウィンドウに記載されている問題を解決します。すべての問題を解決した後、[アップグレード（Upgrade）] をクリックして、アップグレードを再起動します。

（注） 新しい展開のプライマリ管理ノードでポスチャデータの更新処理が実行している場合、プライマリ管理ノードにノードを登録できません。ポスチャ更新プロセスが終了するまで待つか（約 20 分かかることがあります）、またはアップグレードまたはノードの新しい展開への登録中に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページから、ポスチャの自動更新機能を無効にすることができます。

（注） Cisco ISE リリース 2.2 以降からリリース 2.7 にアップグレードする場合、MAC SPW バンドルは [ポリシー（Policy）]> [結果（Results）]> [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）] に表示されません。*mac-spw-dmg-2.7.0.1-isebundle* を cisco.com からダウンロードし、リソースにアップロードして Mac OS X 10.15 リリースをプロビジョニングします。