



分散環境での Cisco ISE の設定

- [Cisco ISE 展開の用語](#) (1 ページ)
- [分散 Cisco ISE 展開のペルソナ](#) (2 ページ)
- [Cisco ISE 分散展開](#) (2 ページ)
- [Cisco ISE ノードの設定](#) (6 ページ)
- [管理ノード](#) (9 ページ)
- [ポリシー サービス ノード](#) (18 ページ)
- [モニタリング ノード](#) (19 ページ)
- [pxGrid ノード](#) (22 ページ)
- [展開内のノードの表示](#) (28 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](#) (29 ページ)
- [ノード ペルソナとサービスの変更](#) (29 ページ)
- [Cisco ISE でのノードの変更による影響](#) (30 ページ)
- [ポリシー サービス ノード グループの作成](#) (30 ページ)
- [ISE pxGrid ノードの展開](#) (31 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](#) (32 ページ)
- [展開からのノードの削除](#) (33 ページ)
- [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](#) (34 ページ)
- [Cisco ISE アプライアンス ハードウェアの交換](#) (35 ページ)

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。分散展開では、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
- 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

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ン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 管理者ポータルで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、管理者ポータルで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。

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	<ul style="list-style-type: none"> システム時刻と NTP サーバ設定の表示および設定。 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。 <p>(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。</p>
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	<ul style="list-style-type: none"> ホームおよび操作メニュー。 プライマリモニタリングノードおよびアクティブモニタリングノードの両方からモニタリングデータにアクセスできることで、冗長アクセスが提供されます。
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。 (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ヤルを使用する必要があります。

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 [全般設定 (General Settings)] タブでデータを入力します。

ステップ 5 [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。

関連トピック

[管理ノード \(9 ページ\)](#)

[Cisco ISE 分散展開 \(2 ページ\)](#)

[分散展開を設定する場合のガイドライン \(4 ページ\)](#)

[管理ノードのハイ アベイラビリティ \(9 ページ\)](#)

[セカンダリ PAN のプライマリへの手動昇格 \(17 ページ\)](#)

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、ポストチャなど) 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。同じノードグループに属するノードはセッション情報を共有するため、高い可用性とフェイルオーバー機能が提供されます。

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 [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。

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、スタンダロン、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 (はい/いいえ)
既存の内部ユーザの RADIUS 認証	○
既存または新しい AD ユーザの RADIUS 認証	○

機能	プライマリ PAN のダウン時に使用できるかどうか（はい/いいえ）
プロファイル変更がない既存のエンドポイント	○
プロファイル変更がある既存のエンドポイント	なし
プロファイリングで学習した新しいエンドポイント。	なし
既存のゲスト：LWA	○
既存のゲスト：CWA	はい（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	なし
ゲスト：AUP	なし
ゲスト：ログイン失敗の最大回数の適用	なし
新しいゲスト（Sponsored-Guest またはアカウント登録）	なし
ポスチャ（Posture）	○
内部 CA による BYOD	なし
登録済みの既存のデバイス	○
MDM オンボーディング	なし
pxGrid サービス	なし

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。

関連トピック

[自動フェールオーバー用のモニタリング ノードの設定](#)（32 ページ）

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

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リング回数 (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を受信された。
- 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リング回数 (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

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。

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	<p>CLI によるアップグレードがブロックされます。</p> <p>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。</p> <p>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。</p>
バックアップの復元	<p>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。</p> <p>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。</p>
ノード ペルソナの変更	<p>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。</p> <ul style="list-style-type: none"> • 両方の管理ノード内の管理ペルソナ。 • PAN のペルソナ。 • 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	<p>CLIによる次の管理操作がブロックされます。</p> <ul style="list-style-type: none"> • パッチのインストールおよびロールバック • DNS サーバの変更 • eth1、eth2、およびeth3 インターフェイスの IP アドレスの変更 • 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 • タイムゾーンの変更
他の管理ポータル操作	<p>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。</p> <ul style="list-style-type: none"> • パッチのインストールおよびロールバック • HTTPS 証明書の変更。 • 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。	<p>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ため、PSN によってこれを更新できません。</p>
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	<p>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。</p> <ul style="list-style-type: none"> • 手動による ISE サービスの停止 • 管理 CLI を使用したソフトリロード（リブート）

関連トピック

[ノード ペルソナとサービスの変更](#) (29 ページ)

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リング数 (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リング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。

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。

ポリシー サービス ノード

ポリシー サービス ペルソナの Cisco ISE ノードは、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 サービスを提供します。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。複数のノードがこのペルソナを担当できます。通常、1つの分散展開に複数のポリシー 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。

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。

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 \(30 ページ\)](#) の項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。

分散展開のポリシー サービス ノードは、マシンアクセス制限 (MAR) キャッシュを相互に共有しません。Cisco ISE で MAR 機能を有効にしている、クライアント マシンが障害が発生したポリシー サービス ノードによって認証される場合は、展開内の別のポリシー サービス ノードがユーザ認証を処理します。ただし、2 番目のポリシー サービス ノードでは、その MAR キャッシュにホスト認証情報がないため、ユーザ認証が失敗します。

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、許可されたがポスト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。

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は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

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。

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では真の意味でハイ アベイラビリティがサポートされていないため、自動フェールオーバーという用語が使用されます。モニタリングノードの場合、操作監査データはポリシーサービスノードによって複製されます。ポリシーサービスノードは、コピーをプライマリ 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送信します。



- (注) モニタリングは、プライマリ (アクティブ) モニタリングノードで行われます。アクティブノードがダウンした場合、モニタリングデータは、セカンダリ (スタンバイ) モニタリングノードからのみ提供されます。セカンダリ モニタリングノードは読み取り専用です。

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。セカンダリノードは、読み取り専用機能を提供します。

既存のセカンダリノードをアクティブなプライマリノードに変換するには、管理者は初めに手動でセカンダリノードをプライマリロールに昇格する必要があります。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、復旧後にその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、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/スタンバイペアを作成できます。セカンダリモニタリングノードを登録する場合は、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。アクティブ-スタンバイペアを定義すると、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で行う必要があります。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ー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せん。プライマリノードがダウンすると、セカンダリノードから情報が提供されます。
- 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、常にアクティブ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。アクティブな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。アクティブな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、アクティブな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、アクティブノードに障害が発生した後に、スタンバイノードはアクティブノードになりません。アクティブノードが復旧すると、管理ノードは再開されたアクティブ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。
- アクティブなモニタリングノードがダウンしている間に、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、既存のアクティブモニタリングノードを登録解除する必要があります。既存のアクティブ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アクティブなモニタリングノードになり、PANは新しく昇格されたアクティブノードに自動的に接続を開始します。
- アクティブ/スタンバイペアでは、展開からスタンバイモニタリングノードの登録解除を選択するか、スタンバイモニタリングノードがダウンすると、既存のアクティブモニタリングノードは、アクティブノードの状態を保持します。PANは、既存のアクティブノードに接続してデータを収集します。
- 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PANにモニタリングデータを提供するアクティブモニタリングノードとして機能します。ただし、新

しいモニタリングノードを登録して展開内でアクティブノードにすると、既存のアクティブ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、新しく登録されたアクティブモニタリングノードへの接続を開始し、モニタリングデータを収集します。

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/サブスクリ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リ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。

関連トピック

[pxGrid クライアントおよび機能の管理](#) (23 ページ)

[pxGrid クライアントの有効化](#) (24 ページ)

[ISE pxGrid ノードの展開](#) (31 ページ)

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には登録が必要です。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使用可能な pxGrid クライアント ライブラリを採用する必要があります。Cisco pxGrid クライアントには、pxGrid サービスに参加するための承認済みアカウントが必要です。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。

公開および登録するためにクライアントの pxGrid で作成される、情報トピックまたはチャンネル機能があります。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ー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 クライアントの有効化 \(24 ページ\)](#)
- [pxGrid 証明書の生成 \(26 ページ\)](#)

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。

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。

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。

関連トピック

[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](#) (3 ページ)

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。管理者ポータルでの [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 および TCP/7802 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 [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。

関連トピック

[ポリシー サービス ノード \(18 ページ\)](#)

[ポリシー サービス ノードのハイアベイラビリティ \(18 ページ\)](#)

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。
- Cisco ISE 1.2 で FIPS モードを有効にしていた場合、1.4 にアップグレードすると、証明書 (自己署名証明書または CA 署名証明書を含む) の生成時または編集時に pxGrid オプションが無効になります。pxGrid オプションは、FIPS 対応の Cisco ISE アプライアンスでは有効にできません。これは、pxGrid と Cisco ISE の統合に使用される XCP サーバが FIPS に準拠していないためです。FIPS モードが Cisco ISE 1.2 で有効でなかった場合は、1.4 にアップグレードした後、pxGrid オプションが証明書に対して有効になります。

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

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。

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、[編集 (Edit)] **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 [保存 (Save)] **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。

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、管理者ポータルを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。
-

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**、**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 アプライアンス ハードウェアの交換

Cisco ISE アプライアンス ハードウェアは、ハードウェアに問題がある場合にのみ交換する必要があります。ソフトウェアに問題がある場合は、アプリケーションのイメージを再作成し、Cisco ISE ソフトウェアを再インストールできます。

ステップ 1 新しいノードで Cisco ISE ソフトウェアを再インストールするか、またはイメージを再作成します。

ステップ 2 プライマリおよびセカンダリ PAN の UDI を使用してライセンスを取得し、プライマリ PAN にインストールします。

ステップ 3 置き換えられたプライマリ PAN でバックアップを復元します。

復元スクリプトはセカンダリ PAN でデータの同期を試行しますが、現在セカンダリ PAN はスタンドアロンノードであり、同期は失敗します。データは、プライマリ PAN でバックアップが実行された時刻に設定されます。

ステップ 4 新しいノードをセカンダリ サーバとしてプライマリ PAN に登録します。
