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、モニターリング、トラブルシューティングなど、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、モニターリング、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、またはモニター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。展開の各ノードは、管理、ポリシーサービス、およびモニター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、ネットワークで次の組み合わせのノードを使用できます。

- 高可用性を実現するプライマリポリシー管理ノード（プライマリ PAN）およびセカンダリポリシー管理ノード（セカンダリ PAN）
- 高可用性を実現するプライマリモニターリングノード（プライマリ MnT ノード）およびセカンダリモニターリングノード（セカンダリ MnT ノード）
- プライマリ 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）

環境のダウンロードが成功し、実行中の Cisco ISE ノードのみが結果に表示されます。

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、およびモニターリング 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。

実稼働環境の Cisco ISE で設定済みのホスト名とドメイン名は、変更しないことを推奨します。変更が必要な場合は、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）]** の順に選択します。

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。

プライマリポリシー管理ノード（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。

最初は [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

Cisco ISE ノードを複数ノード展開形式でプライマリ PANに登録できます。展開内のプライマリ PAN 以外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ーが再起動します。データが完全になった後でプライマリ PANで行われた追加の設定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、[信頼できる証明書（Trusted Certificates）] ウィンドウで 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 （68 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）]** の順に選択します。

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 [ユーザー名（Username）] フィールドと [パスワード（Password）] フィールドに、セカンダリ ノードの GUI ベースの管理者ログイン情報を入力します。

ステップ 6 [次へ（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、Cisco ISE の GUI ダッシュボードの [アラーム（Alarms）] ダッシュレットで確認できます。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

- ゲストユーザーのアクセスと許可、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 サービスを使用している場合は、プライマリ PAN から Cisco ISE CA 証明書と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（別名高可用性または冗長）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、モニターリング、ポリシーサービスペルソナで展開できます。各ペルソナは、ネットワークポリシー管理トポロジ全体で異なる重要な部分を実行します。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 の分散型展開では、管理とモニターリングのアクティビティは一元化されており、処理は PSN 間で分配されます。パフォーマンスのニーズに応じて、展開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、およびモニター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* ハードウェア設置ガイド』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ーリング ペルソナを有効にする必要があります。必要に応じて、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 システムと機能に関連する設定は、プライマリ PAN でのみ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。

分散展開には 1 つ以上の MnT が必要です。プライマリ PAN の設定時に、モニターリング ペルソナを有効にする必要があります。展開内の MnT 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、モニターリング 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 ノードで使用可能な設定データの整合性を確保できます。

通常、最初に Cisco 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（Deployment）] ウィンドウの [ノード 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。同期が完了すると、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（Deployment）] ウィンドウ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。

（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。

- Cisco ISE サーバーのノードタイプを選択します。管理、ポリシー、サービス、およびモニターリング機能には Cisco 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）サーバーを選択します。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 サーバー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 管理者パスワードを設定します。以前の Cisco ISE 管理者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ー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。

- DNS サーバーを設定します。DNS サーバーに、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 サーバーの分散展開のすべての Cisco ISE ノードの正引きおよび逆引き 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。
- （オプション）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 MnT をバックアップし、新しいセカンダリ MnT にデータを復元します。これにより、新しい変更が複製されるときに、プライマリ MnT の履歴が新しい MnT と同期されます。
- 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。
- 展開に別のノードを追加する前に、Cisco ISE プライマリ PAN で内部 CA 設定を有効にして、Cisco ISE 証明書サービスが期待どおりに機能することを確認します。内部 CA 設定を有効にするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [内部 CA 設定（Internal CA Settings）]** の順に選択します。Cisco ISE CA サービスを参照してください。
- 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。
- TrustSec をサポートするように Cisco ISE を設定する場合、または Cisco ISE が Cisco DNA Center と統合されている場合は、PSN を SXP 専用として設定しないでください。SXP は、Cisco TrustSec デバイスと Cisco TrustSec 以外のデバイス間のインターフェイスです。SXP は、Cisco TrustSec 対応ネットワークデバイスと通信しません。

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ー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ー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プライマリロールのモニター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、PSN およびプライマリ MnT 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、それぞれのペルソナを担当する 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 サーバー設定の表示および設定。 • サーバー証明書のインストールと証明書署名要求の管理。すべてのサーバー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、サーバー証明書の操作を実行できます。 （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。
プライマリポリシー管理ノード（プライマリ PAN）	すべてのメニューおよびサブメニュー。
プライマリ モニターリング ノード（プライマリ MnT ノード）	• モニターリングデータへのアクセスを提供。 （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）]** メニューはモニターリングノードに表示されません。
PSN（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を使用できます。各 PSN 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 PSN 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
セカンダリポリシー管理ノード（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 のログイン情報を使用する必要があります。

展開とノードの設定

[展開ノード（Deployment Nodes）] ウィンドウを使用すると、Cisco ISE（PAN、PSN、および MnT）ノードを設定して、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

表 *2:* 展開ノードリスト

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。 • Cisco ISE（PAN、PSN、MnT）ノード
ペルソナ（**Personas**）	（ノードタイプが Cisco ISE の場合のみ表示されます）Cisco ISE ノードが想定しているペルソナ（管理、ポリシーサービス、モニターリング、pxGrid など）が表示されます。 例えば、[管理（Administration）]、[ポリシーサービス（Policy Service）]、[モニターリング（Monitoring）]、または [pxGrid] などです。

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ーリング 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。 • [PRI(A)]：プライマリ PAN を意味します。 • [SEC(A)]：セカンダリ PAN を意味します。 • [PRI(M)]：プライマリ MnT を意味します。 • [SEC(M)]：セカンダリ MnT を意味します。
サービス（**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。 • **ID マッピング** • **セッション** • **プロファイリング** • **すべて**

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Cisco ISE ノードのステータスを示します。 • [緑（接続済み）（Green（Connected））]：すでに展開に登録されているCisco 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。 • [赤（切断）（Red（Disconnected））]：Cisco ISE ノードに到達できないか、またはダウンしているか、あるい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。 • [オレンジ（進行中）（Orange（In Progress））]：Cisco ISE ノードがプライマリ PAN に新規に登録されているか、または 手動同期操作を実行したか、あるいは Cisco 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。 詳細については、[ノードステータス（Node Status）] 列で各 Cisco 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 （2 ページ）
Cisco ISE ノードの設定 （3 ページ）
セカンダリ Cisco ISE ノードの登録 （4 ページ）

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。このウィンドウへのナビゲーションパスは、次のとおりです。**[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）]**の順に選択します。

表 *3:* 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（例：ise1.cisco.com）。
IP アドレス（IP Address）	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。 [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。ペルソナは[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。 [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。このウィンドウ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（Standalone）] ロールがある場合は、横に [プライマリにする（Make Primary）] ボタンが表示されます。ノードに [セカンダリ（Secondary）] ロールがある場合は、横に [プライマリに昇格（Promote to Primary）] ボタンが表示されます。ノードに [プライマリ（Primary）] ロールがあり、他のノードが登録されていない場合は、横に[スタンドアロンにする（Make Standalone）] ボタンが表示されます。[スタンドアロンにする（Make Standalone）] 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
モニターリング（**Monitoring**）	

フィールド名	使用上のガイドライン
	Cisco ISE ノードにモニター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ーリング 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、モニター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 モニターリング 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、モニターリングペルソナを無効にしたりできます。 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。 モニターリング 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。展開にモニターリング 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 つのモニター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ー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。 • [プライマリ（Primary）]：現在のノードをプライマリ モニターリング ノードにする場合。 • [セカンダリ（Secondary）]：現在のノードをセカンダリ モニターリング ノードにする場合。 • [なし（None）]：モニター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。 モニターリング 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、もう一方のモニターリング ノードが自動的にそれぞれ

フィールド名	使用上のガイドライン
	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 モニターリング ノードおよびセカンダリ モニターリング 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つのモニターリングノードのロールを [なし（None）] に変更すると、もう 1 つのモニターリングノードのロールも [なし（None）]になるため、ノードをモニターリングノードに指定した後はハイアベイラビリティペアが取り消されます。このノードは、[リモートロギングターゲット（Remote Logging Targets）] ウィンドウ（**[管理（System）]**>**[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）]**）に syslog ターゲットとしてリストされます

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
	次のサービスのいずれか 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。 • [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所属するグループを、[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。認証局（CA）サービスと Enrollment over Secure Transport（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。 [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。 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 サーバー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 サーバーとしても設定できます。 多数の ISE ノード（RADIUS サーバーや動的許可クライアントとして）を持つ単一の NAD は設定できますが、すべてのノードが同じノードグループに所属して

フィールド名	使用上のガイドライン
	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 （68 ページ）」セクションを参照してください。 • [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、[プロファイリング設定（Profiling Configuration）] 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 サーバー 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 サーバー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。 • [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ーのアクセス 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。 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。 • [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。 • [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で認証されるユーザーをモニターすることができます。Cisco ISEがユーザー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ドメインコントローラからユーザー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 適応型セキュリティアプライアンス（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、ISE関連以外の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 （35 ページ）
ポリシー サービス ノード （44 ページ）
モニターリング ノード （47 ページ）
Cisco pxGridノード （56 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 （66 ページ）
ポリシー サービス ノード グループの作成 （68 ページ）
Cisco pxGrid ノードの展開 （60 ページ）
ノード ペルソナとサービスの変更 （67 ページ）
自動フェールオーバー用の MnT ノードの設定 （55 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）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、次のとおりです。**[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）]**の順に選択します。

表 *4:* 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 パケットを受信するためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに NetFlow 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。次のオプションに必要な値を入力します。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。 • [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 ヘルパーからの 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ていた Cisco ISE ノードごとに DHCP 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。次のオプションに必要な値を入力します。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。 • [ポート（Port）]：DHCP サーバーの 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ていた Cisco ISE ノードごとに DHCP SPAN 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。 • [インターフェイス（Interface）]：Cisco 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パケットを受信し、解析するためにポリシーサービスペルソナを担当していた 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。 • [インターフェイス（Interface）]：Cisco ISEノード上のインターフェイスを選択します。
RADIUS	Cisco IOS センサー対応デバイスからの RADIUS セッション属性およびシスコサービスペルソナ（CDP）属性と Link Layer Discovery Protocol（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ていたISEノードごとに RADIUS 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。
ネットワーク スキャン（NMAP）（Network Scan (NMAP)）	NMAP ノードを有効にするには、このチェックボックスをオンにします。
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ていた Cisco ISE ノードごとに DNS 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。[タイムアウト（Timeout）] の時間を秒単位で入力します。 （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、これら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	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ていたCisco ISEノードごとにSNMPクエリを有効にするには、このチェックボックスをオンにします。[再試行回数（Retries）]、[タイムアウト（Timeout）]、[イベントタイムアウト（Event Timeout）]（必須）、および[説明（Description）]（任意）に値を入力します。 （注） SNMP クエリ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上でCDPとLLDPがグローバルに有効になっ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、およびMACの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ていたCisco ISE ノードごとに SNMP トラッププローブを有効にするには、このチェックボックスをオンにします。次の情報を入力または有効にします。 • [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。 • [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。 • [インターフェイス（Interface）]：Cisco ISE ノードのインターフェイスを選択します。 • [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 サーバーをスキャンして Windows ユーザーに関する情報を探すには、このチェックボックスをオンにします。 • [再スキャン前の日数（Days before rescan）]：スキャンを再度実行するまでの日数を選択します。
pxGrid	Cisco ISE が pxGrid を介してエンドポイント属性を収集（プロファイル）できるようにするには、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 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

以降の項では、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、およびこれらの外部ログターゲットにログメッセージを送信するための Cisco ISE の有効化の方法について説明します。

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 サーバー）を作成してロギングメッセージを保存するために使用する [リモートロギングターゲット（Remote Logging Targets）] 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。[追加（Add）] をクリックします。

表 *5:* リモート ロギング ターゲットの設定

フィールド名	使用上のガイドライン
名前（Name）	新しい syslog ターゲットの名前を入力します。
ターゲット タイプ（Target Type）	ドロップダウンリストから、該当するターゲットタイプを選択します。デフォルト値は [UDP Syslog] です。
説明（Description）	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。Cisco ISE は、ロギング用に IPv4 形式と 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必要がある syslog ファシリティコードをドロップダウンリストから選択します。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。有効な値は 200 ～ 1024 バイトです。

フィールド名	使用上のガイドライン
サーバー ダウン時のバッファ メッセージ（**Buffer Message When Server Down**）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [TCP Syslog] または [セキュアな syslog（Secure Syslog）] を選択すると表示されます。TCP syslog ターゲットまたはセキュアな syslog ターゲットが使用できないときに syslog メッセージを Cisco ISE がバッファできるようにするには、このチェックボックスをオンにします。Cisco ISE は、ターゲットへの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。接続が再開されると、メッセージは最も古いものから順に送信されます。バッファされたメッセージは、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。
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)**）	サーバーがダウンした場合に TCP とセキュアな syslog を破棄するまで保存する期間を設定する期間を秒単位で入力します。
CA 証明書の選択（**Select CA Certificate**）	このドロップダウンリストは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。ドロップダウンリストからクライアント証明書を選択します。
サーバー証明書有効性を無視（**Ignore Server Certificate validation**）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。サーバー証明書の認証を無視し、syslog サーバーを許可するには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

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
- 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、ロギングカテゴリを設定するために使用可能なフィールドについて説明します。ログの重大度レベルを設定し、ロギングカテゴリのログにロギングターゲットを選択します。このウィンドウ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。

表示するロギングカテゴリの横のオプションボタンをクリックし、[編集（Edit）] をクリックします。次の表では、ロギングカテゴリの編集ウィンドウに表示されるフィールドについて説明します。

表 *6*: ロギング カテゴリの設定

フィールド名	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。

フィールド名	使用上のガイドライン
ログの重大度レベル（**Log Severity Level**）	一部のロギングカテゴリでは、この値はデフォルトで設定されており、編集できません。一部のロギングカテゴリでは、次の重大度レベルのいずれかをドロップダウンリストから選択できます。 • [重大（FATAL）]：緊急事態レベル。このレベルは、Cisco ISE を使用できず、必要なアクションをただちに実行する必要があることを意味します。 • [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。 • [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。これは、多くのロギングカテゴリに設定されるデフォルトのレベルです。 • [情報（INFO）]：このレベルは情報メッセージを示します。 • [デバッグ（DEBUG）]：このレベルは、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（**Targets**）	この領域では、左右の矢印アイコンを使用し、[使用可能（Available）] 領域と [選択済み（Selected）] 領域間でターゲットを移動して、ロギングカテゴリのターゲットを選択できます。[使用可能（Available）] 領域には、ローカル（事前定義済み）と外部（ユーザー定義）の両方の既存のロギングターゲットが含まれています。[選択済み（Selected）] 領域（最初は空）には、カテゴリに選択されたターゲットが表示されます。

関連トピック

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

これらのセクションで、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

次の表では、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[パスワードポリシー（Password Policy）]ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、次のとおりです**[管理（Administration）]**>**[システム（System）]**>**[管理者アクセス（Admin Access）]**>**[認証（Authentication）]**>**[パスワードポリシー（Password Policy）]**の順に選択します。

表 *7:* 管理者パスワード ポリシーの設定

フィールド名	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）を指定します。デフォルトは 6 文字です。

フィールド名	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（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザー名またはその文字の逆順でのパスワードとしての使用を制限します。
	[Ciscoまたはその文字の逆順（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パスワードとしての使用を制限します。
	[この単語またはその文字の逆順（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パスワードとしての使用を制限します。
	[4 回以上連続する繰り返し文字の使用（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パスワードとしての使用を制限します。

フィールド名	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（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、または単語の文字の置き換えでのパスワードとしての使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」などに置き換えることはできません。たとえば、「Pa $$ w0rd」は許可されません。 • [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。 このオプションは、デフォルトで選択されます。 • [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。
パスワードには選択したタイプの文字がそれぞれ 1 文字以上含まれている必要があります（Password must contain at least one character of each of the selected types）	管理者のパスワードに含める必要がある文字のタイプのチェックボックスをオンにします。次の 1 つまたは複数のオプションを選択します。 • **英文字の小文字** • **英文字の大文字** • **数字** • **英数字以外の文字**

フィールド名	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。[パスワードは以前の *n* バージョンとは異なる必要があります（Password must be different from the previous n versions）] チェックボックスをオンにし、対応するフィールドに数字を入力します。 ユーザーがパスワードを再使用できない日数を入力します。[パスワードを *n* 日以内に再利用することはできません（Cannot reuse password within n days）] をオンにし、対応するフィールドに数字を入力します。
パスワードライフタイム（**Password Lifetime**）	次のオプションのチェックボックスをオンにして、指定した期間後にパスワードを変更するようユーザーに強制します。 • [管理者パスワードは作成後または最終変更後 *n* 日で有効期限が切れます（Administrator passwords expire n days after creation or last change）]：パスワードを変更しない場合に管理者アカウントが無効になるまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。 • [パスワードの有効期限の *n* 日前に管理者に電子メールリマインダを送信します（Send an email reminder to administrators n days prior to password expiration）]：パスワードが期限切れになることを管理者に通知するまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。
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ー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をオンにします。

フィールド名	使用上のガイドライン
[パスワードを *n* 分間キャッシュします（Password cached for n Minutes）]	管理者ユーザー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。管理ユーザーはこの間、ネットワークデバイスの機密データを表示するの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）]ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、次のとおりです。**[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）]** の順に選択します。

表 *8*: セッション タイムアウトおよびセッション情報の設定

フィールド名	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、プライマリポリシー管理ノード（PAN）がアクティブな状態です。セカンダリ 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、Cisco 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 の自動昇格が開始されます。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 がダウンするか、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 の昇格を開始して、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、3 つ以上のノードが必要です。このうちの 2 つが管理ペルソナとなり、1 つ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、PSN、MnT、pxGrid ノード、あるいはそれらの組み合わせにできます。プライマリ PAN とセカンダリ 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。

機能名	プライマリ PAN がダウンしている場合に使用できますか。（可/不可）
既存の内部ユーザーの RADIUS 認証	可
既存または新しい AD ユーザーの 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

機能名	プライマリ PAN がダウンしている場合に使用できますか。（可/不可）
既存のゲスト：ローカル Web 認証（LWA）	可
既存のゲスト：中央 Web 認証（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	可
内部 CA による BYOD	不可
登録済みの既存のデバイス	可
MDM オンボーディング	不可
pxGrid サービス	不可
セカンダリノードの GUI へのログイン	可（ログインプロセスは、PAN へのコールのブロックが最後のログイン詳細を更新しようとしたときに遅延します。ログインは、このコールタイムアウト後に続行されます）

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、昇格後に、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 への昇格後に追加された 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、モニターリングノード、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。

（注） 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 モニターです。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、受動的にモニターリングを行います。

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有効になると、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構成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。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 に対して行われます。

ヘルス ノードの変更

ヘルス チェックに使用している Cisco 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 H1 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 Cisco ISE を設定できます。この設定は、[展開（Deployment）] ウィンドウのプライマリポリシー管理ノード（プライマリ PAN）で実行できます。このウィンドウ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 PAN 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。
- セカンダリ 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例を示します（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確認されます。

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。

- 昇格要求を受信するノードがセカンダリノードではない。
- セカンダリ PAN が受信した昇格要求にプライマリ PAN の正しい情報がない。
- 不正なヘルス チェックノードから昇格要求を受信した。
- 昇格要求は受信したが、プライマリ PAN は起動していて良好な状態である。

- 昇格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有効になっている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	
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。 PAN の自動フェールオーバー機能は、以前のバージョンの Cisco ISE からリリース 1.4 にアップグレードした後に設定で使用できるようになります。デフォルトでは、この機能は無効になっています。 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、PSN、MnT、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ーインターフェイスがブロックされます。 PAN の自動フェールオーバーの設定が復元前に有効だった場合は、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	GUI による以下のノードペルソナの変更はブロックされます。 • プライマリ PAN とセカンダリ PAN の両方の管理ペルソナ • PAN のペルソナ • PAN の自動フェールオーバー機能を有効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。 • パッチのインストールおよびロールバック • DNS サーバーの変更 • 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 • タイムゾーンが変更されました
他の管理ポータル操作	GUIによる次の管理操作がブロックされます。 • 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とその逆）。
すでに最大数のデバイスに接続しているユーザーは接続できません。	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無効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設定が有効になっている場合は、CLI を介した次の管理操作で警告メッセージが表示されます。サービスまたはシステムがフェールオーバーのウィンドウ内に再起動されない場合は、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。 • Cisco ISE サービスの手動停止 • 管理CLIを使用したCisco ISEのソフトリロード（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、PSN、MnT、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 GUI 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。

（注） 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。PSN、MnT、または pxGrid ノード、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 の正常性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 PAN 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。有効な値の範囲は 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、PAN のステータスに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 GUI にログインします。

ステップ 2

ステップ 3 [ノードの編集（Edit Node）] ウィンドウで、[プライマリに昇格（Promote to Primary）] をクリックします。

（注） 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ーリングペルソナ、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、自動的にレベルが下げられ、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）] ウィンドウでは、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 Cisco ISE 展開での既存の Cisco ISE 展開のノードのプライマリ PAN としての再利用

既存の Cisco ISE 展開のノードを新しい Cisco 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 Cisco 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、Cisco 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 *Cisco ISE* インストールガイドの説明のとおりに、Cisco ISE の新規インストールを実行します。

ステップ 3 プライマリポリシー管理ノード（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ポリシー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有効にするには、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 PAN がダウンした場合は、セカンダリ PAN の自動昇格が開始されます。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。プライマリ PAN について受信したヘルス チェック応答がデバイスのダウンや到達不能などで良好でない場合、ヘルス チェック ノードは設定したしきい値まで待機した後にプライマリ ロールを引き継ぐようにセカンダリ PAN の昇格を開始します。セカンダリ PAN の自動フェールオーバー後、いくつかの機能は使用できなくなります。Cisco ISE は、元のプライマリ 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」セクション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 つの分散型の展開に複数の PSN が存在します。

同じ高速ローカルエリアネットワーク（LAN）か、またはロードバランサの背後に存在するすべての PSN をまとめてグループ化し、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 PSN 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 サーバー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 サーバーとしても設定できます。

（注） 多数の ISE ノード（RADIUS サーバーや動的許可クライアントとして）を持つ単一の NAD は設定できますが、すべてのノードが同じノードグループに所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 （68 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 PSN がある場合は、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。PSN をロードバランサの背後に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

ノードグループ内の PSN はセッション情報を共有します。ノードはハートビートメッセージを交換して、ノードの障害を検出します。ノードに障害が発生した場合、障害が発生した PSN のセッションをノードグループのピアの 1 つが認識し、それらのセッションの接続を解除するための CoA を発行します。ほとんどのクライアントが自動的に再接続し、新しいセッションを確立します。

一部のクライアントは自動的に再接続しません。たとえば、クライアントが VPN 経由で接続する場合、そのクライアントは CoA を認識しない可能性があります。IP Phone、マルチホスト 802.1X ポート、または仮想マシンであるクライアントも、CoA を認識しないか、または CoA に応答できない場合があります。URL リダイレクトクライアント（Web 認証）も自動的に接続できません。これらのクライアントは手動で再接続する必要があります。

タイミングの問題も再接続を妨げる可能性があります。たとえば、PSN フェールオーバー時にポスチャ状態が保留中の場合です。

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大きくなると、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 PSN 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 PSN の数にはハード制限はありません。

ライト セッション ディレクトリ

ライト セッション ディレクトリを使用すると、ユーザー 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、ユーザー 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 セッション ディレクトリには、CoA に必要なセッション属性のみが保存されます。

この機能を有効にするには、[管理（Administration）] > [設定（Settings）] > [ライトセッションディレクトリ（Light Session Directory）] を選択し、[ライトセッションディレクトリの有効化（Enable Light Session Directory）] チェックボックスをオンにします。このオプションを有効にすると、各 PSN のライト セッション ディレクトリ インスタンスは、セッション レコードの一貫性を維持するために、他の PSN とセッションキャッシュから、正常に認証、アカウンティング開始、アカウンティング停止などのセッション更新を受信します。[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。

モニターリング ノード

モニター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 PAN と PSN 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 MnT ノードとセカンダリ MnT ノードの両方がログメッセージを収集します。プライマリ MnT がダウンした場合、プライマリ PAN がモニター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。その場合は、「MnT ロールの手動変更」で説明されている手順に従って行う必要があります。

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、モニター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、および最適なパフォーマンスが得られるように、ノードは監視専用にすることをお勧めします。

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

（注）

pxGrid を有効にした場合は、pxGrid ノードの新しい証明書を作成する必要があります。デジタル署名を使用して証明書テンプレートを作成し、新しい PxGrid 証明書を生成します。

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 GUI にログインします。

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

ステップ 3 ノードのリストで、ロールを変更するMnTノードの横にあるチェックボックスをオンにします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [モニターリング（Monitoring）] セクションで、[プライマリ（Primary）] または[セカンダリ（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、MnT 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 メッセージングサービスを介した syslog

Cisco ISE リリース 2.6 は、デフォルトで組み込みの 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。この存続可能性は、[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（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ログ設定（Log Settings）]**）によって有効になります。このオプションを有効にすると、UDP syslog が Transport Layer Security（TLS）によって保護されます。

[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）] オプションは、Cisco ISE リリース 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 以降のリリースではデフォルトで有効になっています。

UDP syslog に Cisco 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 Cisco ISE ノードから各 Cisco 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）も Cisco ISE メッセージングサービスを使用しています。

（注） 展開環境で Cisco ISE 展開に TCP または Secure syslog を使用する場合、機能は以前のリリースと同じままになります。

キューリンクアラーム

Cisco 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。Cisco ISE GUI ダッシュボードの [アラーム（Alarms）] ダッシュレットに `queue-link alarm` が表示される場合があります。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 Cisco ISE メッセージングサービスが機能している。
- Cisco 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 Cisco 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、アップグレードプロセスによって queue-link アラームがトリガーされることがあります。

queue-link アラームを解決するには、Cisco ISE ルート CA チェーンを再生成します。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。
- [証明書署名要求の作成（Generate Certificate Signing Request）] をクリックし、[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）] を選択します。

[キューリンクエラー（Queue Link Error）] アラームは、次のシナリオで生成される可能性があります。

- タイムアウト：Cisco ISE 展開内の 2 つノード間でネットワークの問題がある場合は、[タイムアウト（Timeout）] が原因で [キューリンクエラー（Queue Link Error）] アラームが発生します。このエラーをトラブルシューティングするには、ポート 8671 の接続を確認します。
- 不明な CA：[システム証明書（System Certificates）] ウィンドウ内（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書**

（**System Certificates**）]）に破損した Cisco ISE メッセージング証明書が存在する場合、[不明なCA（Unknown CA）] が原因で [キューリンクエラー（Queue Link Error）] アラームが発生します。この問題は、**[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）]** を選択し、Cisco ISE GUI から [証明書署名要求（CSR）の生成（Generate Certificate Signing Request (CSR)）] をクリックして、Cisco ISE メッセージング証明書を再生成することで解決できます。Cisco ISE ルート CA 証明書チェーンをすでに置き換えている場合は、再生成は必要ありません。

Cisco ISE ルート CA チェーンを置き換えると、Cisco ISE メッセージングサービス証明書も置き換えられます。その後、Cisco ISE メッセージングサービスが約 2 分のダウンタイムで再起動されます。このダウンタイム中に syslog が失われます。ダウンタイム中に syslog が失われるのを防ぐために、Cisco ISE メッセージングサービスを短期間無効化できます。

MnT に UDP Syslog を伝送するために Cisco 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、次の手順を実行します。

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

ステップ 2 [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）] チェックボックスをオンまたはオフにして、Cisco ISE メッセージングサービスの使用を有効または無効にします。

ステップ 3 [保存（Save）] をクリックします。

MnT ノードでの自動フェールオーバー

MnT ノードはハイアベイラビリティを実装しませんが、アクティブスタンバイを提供します。PSN は、プライマリとセカンダリの両方の MnT ノード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 MnT ノードがダウンした場合は、セカンダリ MnT ノードがすべてのモニターリング情報とトラブルシューティング情報を引き継ぎます。

セカンダリノードをプライマリノードに手動で変換するには、「MnT ロールの手動変更」を参照してください。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 MnT 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。

MnT 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

Cisco ISE ネットワークでは 2 つの MnT 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 MnT ノードをバックアップし、新しいセカンダリ MnT 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 MnR 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 MnT 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、モニター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 からのモニターリング情報は、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 ノードでモニターリング情報が利用できます。
- MnT 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。プライマリとセカンダリの両方の MnT ノード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。

MnT ノードのフェールオーバーシナリオ

次のシナリオは、MnT 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。

- MnT ノードのアクティブ/スタンバイ構成では、プライマリ PAN は、常にプライマリ MnT ノードに接続してモニターリングデータを収集します。プライマリ MnT ノードに障害が発生した後に、PAN はスタンバイ MnT ノードに接続します。プライマリノードからスタンバイノードへのフェールオーバーは、プライマリ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、セカンダリ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、PAN ノードは再開されたプライマリノードからのモニターリングデータの収集を再び開始します。
- プライマリ MnT ノードがダウンしたときにスタンバイ MnT ノードをアクティブステータスに昇格する場合は、MnT ロールの手動変更か、既存のプライマリ MnT ノードの登録を解除して、スタンバイ MnT 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 MnT ノードの登録を解除すると、スタンバイノードがプライマリ MnT 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 MnT ノードの登録を解除するか、またはセカンダリ MnT ノードがダウンした場合は、既存のプライマリ MnT 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MnT 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 MnT ノードとして機能し、PAN にモニターリングデータを提供します。ただし、新しい MnT 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 MnT ノードが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 MnT ノードに接続し、モニターリングデータを収集します。

モニターリング データベース

モニターリング機能によって利用されるデータレートとデータ量には、これらを目的とした専用のノード上に別のデータベースが必要です。

PSN のように、MnT ノードにはこの項で説明するトピックなどのメンテナンスタスクの実行に必要な専用のデータベースが備わっています。

モニターリングデータベースのバックアップと復元

モニター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、MnT 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 MnT ノードを登録する場合は、最初にプライマリ MnT ノードをバックアップしてから、新しいセカンダリ MnT 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 MnT 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。

モニターリング 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、モニター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、消去用のディスク容量使用率しきい値（合計ディスク容量の80%）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。

モニターリング データベースの消去に関するガイドライン

次に、モニター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%（すなわち合計ディスク容量の60%）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の最大値を超過しそうであることを示すクリティカルアラームが生成されます。ディスク使用量がしきい値設定の90%（すなわち合計ディスク容量の70%）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の最大値を超過したことを示す、別のクリティカル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、[データ消去の監査（Data Purging Audit）] ウィンドウで確認できます。このウィンドウへのナビゲーションパスは、次のとおりです。**[操作（Operations）]**>**[レポート（Reports）]**>**[レポート（Reports）]** > **[監査（Audit）]** > **[データ消去の監査（Data Purging Audit）]**の順に選択します。消去の完了後に情報（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容量がしきい値（デフォルトは合計ディスク容量の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、最も古い7日間のモニター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、処理の前にモニターリング 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

Cisco ISE モニターリング運用データベースには、Cisco ISE レポートとして生成された情報が含まれています。最近のCisco ISEのリリースには、モニターリング運用データを消去し、Cisco ISE の管理者 **application configure ise** を実行した後にモニターリングデータベースをリセットするためのオプションが備わっています。CLI コマンドを入力します。

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、データベースを指定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、再起動するまではCisco 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）] ウィンドウには、[データベース使用率（Database Utilization）] および [データを今すぐ消去（Purge Data Now）] 領域があります。このウィンドウへのナビゲーションパスは、**[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）]** の順に選択します。[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）] 領域に指定します。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、リポジトリを選択して作成し、[暗号キー（Encryption Key）] を指定します。

[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 （54 ページ）

古い運用データの消去

運用データはサーバー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（Data Purging Audit）]** 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 ）]** エリア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）]** エリアで、**[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。
3. [暗号キー（Encryption Key）] フィールド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、データはこのウィンドウで設定した値（3 日）に従って消去されます。

- **[データを今すぐ消去（Purge Data Now）]** エリアで、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 MnT ノードの設定

展開に 2 つの MnT 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 モニター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 MnT ノードが自動的にモニター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 MnT ノードを設定するには、MnT 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ーリング 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 MnT ノードとセカンダリ MnT 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 MnT ノードでバックアップおよび消去に 2 つのリポジトリが使用されている場合、セカンダリノードに同じリポジトリを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 MnT 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ー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、MnT 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 MnT 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）]** の順に選択します。

ステップ 2 **[展開ノード（Deployment Nodes）]** ウィンドウで、プライマリとして指定する MnT ノードの横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。

MnT ノードをプライマリとして選択すると、他の MnT ノードが自動的にセカンダリになります。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。プライマリ ノードとセカンダリ ノードの両方が再起動します。

Cisco 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、Cisco ISE エコシステムのパートナーシステムなどの余暇のネットワークシステムやシスコの他のプラットフォームと共有できます。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や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ます。また、その他の情報交換にも使用できます。Cisco pxGrid によって、サードパーティ製のシステムは適応型のネットワーク制御アクション（EPS）を呼び出し、ネットワークまたはセキュリティイベントに応じてユーザーまたは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、Cisco TrustSec のトピックを通して Cisco ISE から他のネットワークに渡すことができます。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 トピックを通じて 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。

Cisco pxGrid 経由で SXP バインディング（IP-SGT マッピング）を公開および登録できます。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 サーバーは、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、Cisco pxGrid サーバーは、クライアントの登録とサブスクリプション処理を停止します。Cisco pxGrid サーバーの 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。[Cisco pxGrid サービス（Cisco pxGrid Services）] ウィンドウ（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）を調べ、Cisco 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。

pxGrid ペルソナがあるアクティブなシスコノードでは、これらのプロセスは [実行中（Running）] と表示されます。スタンバイの Cisco pxGrid ノードでは、[スタンバイ（Standby）] と表示されます。アクティブな pxGrid ノードがダウンすると、スタンバイ pxGrid ノードがこれを検出し、4 つの pxGrid プロセスを開始します。これらのプロセスは、数分以内に [実行中（Running）] と表示され、スタンバイ ノードがアクティブ ノードになります。CLI コマンド **show logging**

application pxgrid/pxgrid.state を実行すると、Cisco pxGrid がそのノードでスタンバイ状態であるかどうかを確認できます。

Extensible Messaging and Presence Protocol クライアントの場合、Cisco pxGrid ノードはアクティブ/スタンバイのハイアベイラビリティモードで動作します。つまり、Cisco 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。

（注） ハイアベイラビリティ Cisco ISE 展開では、アクティブ/スタンバイ設定で動作する pxGrid ペルソナノードは、pxGrid サービスがアクティブノードでは [実行中（running）] の状態で、スタンバイノードでは [スタンバイ（standby）] 状態であることを示します。

Cisco ISE ノード上の pxGrid サービスのステータスを確認するには、次の CLI コマンドを使用します。

```
show logging application pxgrid/pxgrid.state
```

セカンダリ Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco pxGrid ノードがダウンすると、セカンダリ Cisco 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 Cisco 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。

Cisco pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更の通知。
- pxgrid-cm.log：パブリッシャまたはサブスクライバ、あるいはその両方、およびクライアントとサーバー間で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。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログを表示します。
- 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すべての情報を表示します。

（注） ノードで Cisco 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、ポート 8910 （Web クライアントで使用）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 Cisco pxGrid を有効にできますが、Cisco 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 Cisco 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 ワークセンターで使用するには Cisco 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。

Cisco pxGrid クライアントと機能の管理

Cisco ISE に接続するクライアントは、Cisco 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。Cisco pxGrid クライアントは、クライアントになるために Cisco pxGrid SDK で使用可能な Cisco 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 Cisco 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 Cisco pxGrid サーバーのホスト名または IP アドレスに接続できます。

Cisco pxGrid の機能は、クライアントの Cisco 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（ANC）、セキュリティ グループ アクセス（SGA） などの機能のみがサポートされています。クライアントが新しい機能を作成すると、[機能別に表示（View by Capabilities）] ウィンドウに表示されます。このウィンドウへのナビゲーションパスは、次のとおりです。**[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]**の順に選択します。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。

Web クライアントパブリッシャが REST API または WebSocket プロトコルを使用する場合、Web クライアントパブリッシャに追加されたトピックは、Cisco ISE の **[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [Web クライアント（Web Clients）]** タブにすぐには表示されません。このような Web クライアントトピックは、最初のインスタンスが公開されて初めて [Web クライアント（Web Clients）] タブに表示されます。

（注） Cisco pxGrid セッショングループが EPS グループの一部であるため、エンドポイント保護サービス（EPS）ユーザーグループに割り当てられたユーザーはセッショングループでアクションを実行できます。ユーザーが EPS グループに割り当てられると、そのユーザーは Cisco pxGrid クライアントのセッションのグループに登録できます。

関連トピック

Cisco pxGrid 証明書の生成 （61 ページ）

pxGrid サービスの有効化

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。

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。
ステップ 4 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 5 [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 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。また、アップグレードライセンスを最近インストールした場合は、Base インストールで特定の拡張 pxGrid サービスを使用できる可能性があります。
- すべてのノードは、Cisco pxGrid サービス用に CA 証明書を使用します。アップグレード前に Cisco pxGrid サービスにデフォルトの証明書を使用した場合、アップグレードによってその証明書が内部 CA 証明書に置き換えられます。
- Websocket（pxGrid 2.0）の場合はポート 8910 を、XMPP（pxGrid V1.0）の場合はポート 5222 を開く必要があります。ノードで Cisco 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、ポート 8910 は機能し、引き続き要求に応答します。

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

ステップ 2 **[展開ノード（Deployment Nodes）]** ウィンドウで、Cisco pxGrid サービスを有効にするノードの横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]** トグルボタンを有効にします。**[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）] ウィンドウには、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。

このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブログ（Live Log）]** です。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。

Cisco 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）]** の順に選択します。

ステップ 2 要件に基づき、次のいずれかのチェックボックスをオンにします。

- [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をオンにすると、新しい Cisco 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をオンにすると、Cisco pxGrid クライアントのユーザー名または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、Cisco pxGrid クライアントを自動的に承認することはできません。

ステップ 3 [保存（Save）] をクリックします。

Cisco pxGrid の [設定（Settings）] ウィンドウで [テスト（Test）] オプションを使用して、Cisco pxGrid ノードでヘルスチェックを実行します。pxgrid ファイルまたは pxgrid-test.log ファイルの詳細を表示します。

Cisco pxGrid 証明書の生成

始める前に

- Cisco ISE の一部のバージョンには NetscapeCertType を使用する Cisco pxGrid の証明書があります。新しい証明書を生成することを推奨します。
- 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。
- Cisco 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。
- デジタル署名を使用して証明書テンプレートを作成し、新しい Cisco pxGrid 証明書を生成します。

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [証明書（Certificates）]** 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した場合は、共通名（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した場合は、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。

ステップ 3 [共通名（CN）（Common Name (CN)）]：（[単一の証明書の生成（証明そ署名要求なし）（Generate a single certificate (without a certificate signing request)）] を選択した場合に必要。）pxGrid クライアントの FQDN を入力します。

ステップ 4 [証明書署名要求の詳細（Certificate Signing Request Details）]：（[単一の証明書の生成（証明そ署名要求なし）（Generate a single certificate (without a certificate signing request)）] を選択した場合に必要。）完全な証明書署名要求の詳細を入力します。

ステップ 5 [説明（Description）]：（オプション）この証明書の説明を入力します。

ステップ 6 [証明書テンプレート（Certificate Template）]：**pxGrig_Certificate_Template** のリンクをクリックして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します。

ステップ 7 [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）]：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 Cisco pxGrid クライアントの IP アドレスを入力します。
- [FQDN]：pxGrid クライアントの FQDN 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 8 [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）（Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)）]：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）（PKCS12 format (including certificate chain; one file for both the certificate chain and key)）]：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 9 [証明書パスワード（Certificate Password）]：証明書のパスワードを入力し、次のフィールドにもう一度入力してパスワードを確認します。

ステップ 10 [作成（Create）] をクリックします。

作成した証明書は、Cisco ISE の [発行された証明書（Issued Certificates）] ウィンドウに表示されます。

ステップ 11 このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行した証明書（Issued Certificates）]** です

ステップ 12 このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**

（注） Cisco ISE 2.4 パッチ 13 以降、pxGrid サービスの証明書要件がより厳格になりました。pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、Cisco ISE 2.4 パッチ 13 以降の適用後に証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバーとして指定された Netscape Cert Type 拡張があるためです。クライアント証明書も必要になっているため、これは失敗するようになりました。

非準拠の証明書を持つクライアントは、Cisco ISE と統合できません。内部 CA によって発行された証明書を使用するか、適切な使用拡張を指定して新しい証明書を生成します。

- 証明書の [キーの使用方法（Key Usage）] の拡張には、[デジタル署名（Digital Signature）] フィールドと [キー暗号化（Key Encipherment）] フィールドが含まれている必要があります。
- 証明書の [拡張キーの使用方法（Extended Key Usage）] の拡張には、[クライアント承認（Client Authentication）] フィールドと [サーバー承認（Server Authentication）] フィールドが含まれている必要があります。
- 証明書に [Netscape 証明書タイプ（Nestscape Certificate Type）] の拡張は必要ありません。その拡張を含める場合は、[SSL クライアント（SSL Client）] と [SSL サーバー（SSL Server）] の両方を拡張に追加する必要があります。
- 自己署名証明書を使用している場合は、[基本制約CA（Basic Constraints CA）] フィールドを **TRUE** にし、[キーの使用方法（Key Usage）] の拡張に [キー証明書署名（Key Cert Sign）] フィールドを含める必要があります。

。証明書は、ブラウザのダウンロードディレクトリにもダウンロードされます。

Cisco pxGrid クライアントの権限の制御

Cisco 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、Cisco 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、Cisco 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）] > [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>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**：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。

事前に定義されたグループ（EPS や ANC など）と手動で追加し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。

（注） ポリシーに含まれるグループに属するクライアントのみが、そのポリシーで指定されたサービスに登録できます。たとえば、com.cisco.ise.pubsub サービスの pxGrid ポリシーを定義し、このポリシーに ANC グループを割り当てた場合、ANC グループに属するクライアントのみが com.cisco.ise.pubsub サービスに登録できます。

展開内のノードの表示

[展開ノード（Deployment Nodes）] ウィンドウで、展開を構成するプライマリとセカンダリのすべての Cisco ISE 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）]** の順に選択します。

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。

MnT 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

MnT 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）が使用可能です。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 統計情報をダウンロードするには、Cisco ISE（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* リファレンスガイド』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。
- 『Cisco Identity Services Engine CLI Reference Guide』の説明に従って、小規模な展開またはその他の理由により、セカンダリ PAN 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 が破損している場合は、『Cisco Identity Services Engine CLI Reference Guide』の説明に従って、登録解除、設定のリセット、および登録を行います。
- スタンドアロンデバイスの場合は、『Cisco Identity Services Engine CLI Reference Guide』の説明に従って最新のバックアップを復元します。

（注） 最新の構成変更が失われないようにするために、スタンドアロンデバイスからバックアップを定期的に取得します。

モニターリングのためのデバイス設定

MnT ノードは、ネットワーク上のデバイスからのデータを受信し、使用して、ダッシュボードに表示されます。MnT 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 の構成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。

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）]** の順に選択します。

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

- PSN で実行されるサービスを有効または無効にしたり、PSN 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 サーバー 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構成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）]** の順に選択します。

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 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）

（注） セカンダリ管理ノードをプライマリ PAN の位置に昇格させると、プライマリ ノードがセカンダリロールになります。これにより、プライマリ ノードとセカンダリ ノードの両方が再起動し、遅延が発生します。

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。

ノード グループは、URL リダイレクト（ポスチャ サービス、ゲスト サービス、および MDM）が適用されるセッションの PSN フェールオーバーに使用されます。

（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、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）] ウィンドウで、PSN 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）]** の順に選択します。

ステップ 2 左側のナビゲーションウィンドウの上部にある [設定（Settings）] アイコンをクリックします。

ステップ 3 [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 4 ノード グループに付ける一意の名前を入力します。

（注） ノード登録で望ましくない問題が発生する可能性があるため、**None** という名前でノードグループを設定することは推奨されません。

ステップ 5 （任意）ノード グループの説明を入力します。

ステップ 6 （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] ウィンドウで MAR が有効になっていることを確認します。

ステップ 7 [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ウィンドウ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するか、またはノードを編集するには、[ポリシーサービス（Policy Service）] 領域の [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、およびモニター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。MnT 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（Deployment）] ウィンドウ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）] ウィンドウ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）] ウィンドウに表示されるには 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ように 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）]** の順に選択します。

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、セカンダリノードの登録が正常に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 からの登録の解除が失敗した場合は、このアラームは生成されません。

Cisco ISE ノードのシャットダウン

Cisco ISE CLI から **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** コマンドを発行すると、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 `Yes` と入力した場合は、次の質問に応答する必要があります。

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

既存の Cisco ISE 構成を保存するために `Yes` と入力すると、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、Cisco 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 リファレンス ガイド』を参照してください。

ノードを再登録する必要があるシナリオの例

次の表は、ノードが破損した場合にノードを再登録する必要があるシナリオの一部をまとめたものです。

シナリオ	必要な作業
プライマリ PAN 以外のノードのいずれかが破損している場合	**1.** 障害が発生したノードを展開から登録解除します。 **2.** 障害が発生したノードに Cisco ISE を再インストールします。 **3.** 既存の展開にノードを再登録します。 （注） 登録の前または後に、古い証明書をノードにインポートする必要があります。
プライマリ PAN が破損している場合	たとえば、N1（プライマリ PAN）と N2（セカンダリ PAN）の 2 つのノードがある場合 **1.** セカンダリ PAN（N2）をプライマリ PAN に昇格させます。 **2.** 障害が発生したノード（N1）を展開から削除します。 **3.** 障害が発生したノード（N1）に Cisco ISE を再インストールします。 **4.** 展開するセカンダリ PAN としてノード（N1）を登録します。 **5.** 登録が完了したら、古い証明書をノード（N1）にインポートします。 **6.** ノード（N1）をプライマリ PAN に再昇格させ、以前と同様の展開にします。

シナリオ	必要な作業
プライマリ PAN とセカンダリ PAN の両方が破損している場合	たとえば、N1（プライマリ PAN）と N2（セカンダリ PAN）の 2 つのノードがある場合 **1.** プライマリ PAN ノード（N1）とセカンダリ PAN ノード（N2）に Cisco ISE を再インストールします。 **2.** プライマリ PAN ノード（N1）で設定のバックアップを復元します。 **3.** プライマリ PAN ノード（N1）で古い証明書をインポートします。 **4.** 他のノード（N2）をセカンダリ PAN として展開に登録します。 **5.** 他のノードで reset-config を実行し、展開にノードを登録します。 **6.** すべてのノードに証明書をインポートします。 （注） プライマリ PAN とセカンダリ PAN が VM の場合、Cisco ISE を再インストールすると UDI が変更される可能性があるため、新しい UDI でライセンスを再インストールする必要があります。

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。ただし、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はプライマリ 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 サーバーに、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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。