分散環境での Cisco ISE の設定

Cisco ISE は、スタンドアロン展開と分散展開の両方をサポートする、ハイ アベイラビリティを備えたスケーラブルなアーキテクチャを提供します。分散環境では、プライマリ管理ノードを 1 つ設定して、ネットワークに展開されているセカンダリ ISE ノードを管理します。

Cisco ISE では、中央集中型の構成と管理によるランタイム サービスの分散展開が提供されます。フェールオーバーをサポートするために、複数のノードを同時に分散して展開できます。

この章では、Cisco ISE を構成するペルソナ、ロール、およびサービスと Cisco ISE ノードを設定する方法について説明します。

Cisco ISE の展開シナリオの詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

この章は次のトピックで構成されています。

Cisco ISE 展開の用語

Cisco ISE の展開シナリオについて説明するときに頻繁に使用される用語を次に示します。

- 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：ノードは、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、ノードにより提供され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、インライン ポスチャのペルソナのいずれかを担当することができます。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を担当できます。インライン ポスチャ ペルソナは、専用 Cisco ISE ノードを必要とします。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。
- 導入モデル：導入を、分散、スタンドアロン、または基本的な 2 ノード展開であるスタンドアロンのハイ アビリティのいずれかに決定します。

関連項目

「プライマリおよびセカンダリ ノードで使用可能なメニュー オプション」（P.3-10）

Cisco ISE 分散展開におけるペルソナ

Cisco ISE ノードは、次のペルソナのいずれかを担当することができます。

- 管理ノード
- ポリシー サービス ノード
- モニタリング ノード
- インライン ポスチャ ノード

Cisco ISE ノードは、担当するペルソナに基づいてさまざまなサービスを提供できます。展開の各ノードは、インライン ポスチャ ノードを除き、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 アベイラビリティを実現するプライマリ管理 ISE 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 1 組のモニタリング 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
- ハイ アベイラビリティを実現する 1 組のインライン ポスチャ ノード

管理ノード

管理ペルソナがある Cisco ISE ノードを使用すると、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する、システム関連のすべての設定を処理します。分散環境では、1 つのノードのみ、または最大 2 つのノードで管理ペルソナを実行できます。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。

管理ノードでのハイ 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がアクティブ状態で、すべての設定変更はそのノードに対して行われます。セカンダリ管理ノードはスタンバイ状態であり、プライマリ管理ノードからすべての設定更新を受信します。このため、プライマリ管理ノードの設定の完全なコピーが常に存在することになります。

プライマリ管理ノードがダウンすると、セカンダリ管理ノードのユーザ インターフェイスにログインし、手動でセカンダリ管理ノードを昇格する必要があります。管理ペルソナには自動フェールオーバーがありません。

プライマリ管理ノードがダウンした場合、スポンサー管理者は新しいゲスト ユーザ アカウントを作成できません。その間、ゲストおよびスポンサーのポータルは、それぞれすでに作成されているゲスト ユーザおよびスポンサー ユーザに対する読み取り専用アクセスを提供します。また、プライマリ管理ノードがオフラインになる前にスポンサー ポータルにログインしなかったスポンサー管理者は、セカンダリ管理ノードが格上げされるか、プライマリ管理ノードが使用可能になるまでスポンサー ポータルにログインできません。

分散セットアップでは、少なくとも 1 つのノードが管理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

ポリシー サービス ペルソナがある 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。通常は、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。ロード バランサの背後にあるすべてのポリシー サービス ノードは、1 つのノード グループを形成するようグループ化できます。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に、その他のノードは障害を検出し、保留中のすべての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 ノードでのハイ アベイラビリティ

分散展開では、要求を均等に分散するためにロード バランサの背後に複数のポリシー サービス ノードを配置することがあります。ロード バランサによって、背後の機能ノードに要求が分散されます。また、ノード障害を検出し、障害が発生したノードで保留状態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に障害が発生すると、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のセッションの保留に関する許可変更（CoA）を発行します。

（注） セッションは許可されている場合は保留状態になりますが、ポスチャ評価は完了していません。ノード グループを使用せずに分散展開を設定することは可能ですが、障害が発生したポリシー サービス ノードの保留状態のセッションは自動的にリセットされません。

ノード グループのすべてのノードは、CoA を発行するため、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する必要があります。通常、これらのノードは RADIUS サーバとしても設定します。スイッチでの CoA 関連の設定の詳細については、「RADIUS 許可変更（CoA）の有効化」（P.F-4）を参照してください。

複数の ISE ノードを RADIUS サーバおよび動的許可クライアントとして持つ単一の 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。

同じノード グループ内のすべてのノードは、NAD で、RADIUS サーバおよびクライアントとして設定する必要があります。これは、それらのすべてのノードが、ノード グループ内の任意のノードに対して、その NAD 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。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。ノード グループ内のすべてのノードは、同じマルチキャスト アドレスを共有し、このアドレスを使用してヘルス ステータスをやり取りします。

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

Cisco ISE のハートビート機能によって、ポリシー サービス ノードでのセッション フェールオーバーが処理されます。複数のアクティブ セッションがあるポリシー サービス ノードに障害が発生すると、エンドポイントが中間状態となります。ポスチャ エージェントが通信していたポリシー サービス ノードの障害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 セッションが検知され、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、RADIUS ロード バランシングを使用して、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 ISE ノードにセッションが自動的に移動しませんが、セッションを移動するための CoA が発行されます。

ポリシー サービス ノードでのマシン アクセス制限

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）を相互に共有しません。たとえば、ポリシー サービス ノードの 1 つによってクライアント マシンが認証され、障害が発生した場合、導入の別のポリシー サービス ノードによってユーザ認証が処理されます。ただし、この場合、ユーザ認証は失敗します。これは、2 つめのポリシー サービス ノードの MAR キャッシュにホスト認証情報がないためです。

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、マルチキャスト 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、マルチキャスト 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。

最大で 10 のポリシー サービス ノードをノード グループ クラスタに含めることができます。

ノード グループの数を最小化することによって、管理する必要があるマルチキャスト アドレスの数を削減する場合は、NAD で設定されているすべての RADIUS サーバおよびクライアントを 1 つのノード グループとしてグループ化できます。

マルチキャスト アドレスの管理は問題ないものの、マルチキャスト トラフィックを最小化する必要がある場合は、ノード グループ内のノード数を減らすことができます。

モニタリング ノード

モニタリング ペルソナがある Cisco ISE ノードはログ コレクタとして機能し、ネットワーク内のすべての管理ノードとポリシー サービス ノードからのログ メッセージを格納します。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モニタリング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 ノードの両方は、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 つのノードがモニタリング 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。

[モニタリング（Monitoring）] メニューには、展開のプライマリ管理ノードおよびプライマリ モニタリング ノードからアクセスできます。

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 ノードでは読み取り専用機能が提供されます。

既存のセカンダリ ノードをアクティブ プライマリ ノードに変換するには、管理者は最初にセカンダリ ノードをプライマリ ロールに手動で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 フェールオーバー後にプライマリ ノードが復旧した場合、手動でバックアップおよび復元して、失われたデータが再生されるようにプライマリ ノードを更新する必要があります。

モニタリング ノードのアクティブ-スタンバイ ペア

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ので、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 ノードと同期していることが保証されます。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 ノードで行うことができます。セカンダリ ノードは読み取り専用です。
- プライマリ ノードで行った変更は、セカンダリ ノードに自動的に複製されます。
- プライマリ ノードとセカンダリ ノードは両方とも、他のノードがログを送信するログ コレクタとしてリストされます。
- Cisco ISE ダッシュボードは、モニタリングおよびトラブルシューティングの主要なエントリ ポイントとなります。プライマリ モニタリング ノードからのモニタリング情報は、ダッシュボードに表示されます。プライマリ ノードがダウンすると、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 ノードに対応するアクティブ-スタンバイまたは単一ノード設定に適用されます。

- モニタリング ノードのアクティブ-スタンバイ設定では、管理者 PAP はモニタリング データを収集するために常にアクティブ モニタリング ノードを指します。アクティブ モニタリング ノードに障害が発生したら、管理 PAP はスタンバイ モニタリング ノードを指します。アクティブ 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、1 ～ 10 秒以内に行われます。

  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 ノードが復旧した場合、管理ノードは再開されたアクティブ ノードからモニタリング データを収集し始めます。
- アクティブ 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 ステータスに昇格したい場合は、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 ノードはアクティブ モニタリング ノードになり、管理 PAP は新しく昇格したアクティブ ノードを指すようになります。
- アクティブ-スタンバイ ペアにおいて、導入からスタンバイ モニタリング ノードを登録解除する場合、または、スタンバイ モニタリング ノードがダウンした場合、既存のアクティブ モニタリング ノードは引き続きアクティブ ノードのステータスを保持します。管理 PAP は、データの収集のため既存のアクティブ ノードを指します。
- ISE 導入においてモニタリング ノードが 1 つしかない場合、そのノードはモニタリング データを管理 PAP に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、導入でのアクティブ 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。管理 PAP は、モニタリング データを収集するために、新しく登録されたアクティブ モニタリング ノードを指すようになります。

関連項目

- 「オンデマンド バックアップの実行」（P.12-4）
- 「モニタリング データベースの復元」（P.12-10）

インライン ポスチャ ノード

インライン ポスチャ ノードは、ネットワーク上のワイヤレス LAN コントローラ（WLC）や VPN コンセントレータなどのネットワーク アクセス デバイスの背後にあるゲートキーパー ノードです。インライン ポスチャ ノードにより、ユーザが認証され、アクセス権が与えられた後にアクセス ポリシーが適用され、WLC または VPN が処理できない許可変更（CoA）要求が処理されます。Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担当できるインライン ポスチャ ノードを 2 つ使用してハイ アベイラビリティを実現できます。

インライン ポスチャ ノードは、専用ノードである必要があります。インライン ポスチャ サービス専用である必要があり、他の Cisco ISE サービスを同時に稼働できません。同様に、そのサービスの特性のため、インライン ポスチャ ノードはどのペルソナも担当することができません。たとえば、Cisco ISE ネットワークで、管理サービスを提供する管理ノード、ネットワーク アクセス サービス、ポスチャ サービス、プロファイル サービス、およびゲスト サービスを提供するポリシー サービス ノード、またはモニタリング サービスおよびトラブルシューティング サービスを提供するモニタリング ノードとして稼働することはできません。

インライン ポスチャ ペルソナは、Cisco ISE 3495 プラットフォームではサポートされていません。次のいずれかのプラットフォームにインライン ポスチャ ペルソナをインストールしていることを確認します。Cisco ISE 3315、Cisco ISE 3355、Cisco ISE 3395、または Cisco ISE 3415。

関連項目

第 4 章「インライン ポスチャの設定」

インライン ポスチャ ノードのインストール

Cisco.com からインライン ポスチャ 1.2 ISO イメージをダウンロードし、サポートされているプラットフォームのいずれかにインストールします。次に、コマンドライン インターフェイス（CLI）によって証明書を設定します。その後、管理者ポータルからこのノードを登録できます。

（注） インライン ポスチャのノードの Web ベースのユーザ インターフェイスにアクセスすることはできません。プライマリ管理ノードからのみ設定することができます。

インライン ポスチャ アプリケーションをインストールしてセット アップした後、インライン ポスチャのノードを登録する前に、証明書を設定する必要があります。詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

Cisco ISE の分散展開

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、パフォーマンスを向上させるために、複数の Cisco ISE ノードが分散した展開をセットアップできます。Cisco ISE 分散展開では、管理およびモニタリング アクティビティは集中化され、処理はポリシー サービス ノードにわたって分散されます。パフォーマンス ニーズに応じて、展開の規模を調整できます。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 ペルソナのいずれかを担当することができます。インライン ポスチャ ノードは、その特性のため、他のいずれのペルソナも担当することができません。インライン ポスチャ ノードは、専用ノードである必要があります。

ここでは、次の内容について説明します。

Cisco ISE 展開のセットアップ

『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』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管理ノードとして定義する必要があります。プライマリ管理ノードの定義時に、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、プライマリ管理ノードでポリシー サービス ペルソナを有効にできます。プライマリ管理ノード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管理ノードに登録し、セカンダリ ノードのペルソナを定義できます。

Cisco ISE システムと機能に関連するすべての設定は、プライマリ ISE ノードでのみ行う必要があります。プライマリ管理ノード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。

分散展開に少なくとも 1 つのモニタリング ノードが存在する必要があります。プライマリ管理ノードの設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ管理ノードを編集したり、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 ノードへのデータベース リンクをすぐに作成し、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、プライマリ管理ノード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。複製のステータスは、Cisco ISE 管理者ポータルにある展開ページのノード ステータス カラムで確認できます。Cisco ISE ノードをセカンダリ ノードとして登録するか、または手動でプライマリ管理ノードとの同期を実行すると、ノード ステータスは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色のアイコンを示します。それが完了すると、ノード ステータスは、セカンダリ ノードがプライマリ管理ノードと同期していることを示す緑色に変わります。ノード ステータスが緑色に変わった後、Cisco ISE アプリケーション サーバが再起動して実行され、セカンダリ ISE ノード設定を完了するのに約 5 分かかります。

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。プライマリ管理ノードからセカンダリ 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。

（注）　プライマリ管理ノードの登録は解除できません。

関連項目

第 4 章「インライン ポスチャの設定」

Cisco ISE アプリケーション サーバの自動再起動

次のいずれかの変更を行うと、Cisco ISE ノードのアプリケーション サーバが再起動され、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 サービスまたはモニタリング 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 サービスをイネーブルまたはディセーブルにします）
- 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）

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 タイプを選択します：ISE ノードまたはインライン ポスチャ ノード。管理、ポリシー サービス、およびモニタリングの機能の場合、ISE ノードを選択する必要があります。インライン ポスチャ サービスの場合、インライン ポスチャ 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ネットワーク タイム プロトコル（NTP）サーバを選択します：ノード間のタイムゾーン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。この設定では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。
- 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、分散展開の一部であるすべての 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。
- （任意）セカンダリ Cisco ISE ノードから Cisco ISE をアンインストールするために、プライマリ管理ノードからセカンダリ Cisco ISE ノードを登録解除します。
- 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ので、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 ノードと同期していることが保証されます。

- プライマリ管理ノードと、セカンダリ ノードとして登録するスタンドアロン ノードでは、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 ノードとセカンダリ ノードのデータベース パスワードが同じであることを確認します。ノード インストール中にこれらのパスワードが異なって設定された場合は、次のコマンドを使用してパスワードを変更できます。
  - **application reset-passwd ise internal-database-admin**
  - **application reset-passwd ise internal-database-user**

  Cisco ISE CLI コマンドの使用方法の詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

関連項目

- 「オンデマンド バックアップの実行」（P.12-4）
- 「モニタリング データベースの復元」（P.12-10）

プライマリおよびセカンダリ ノードで使用可能なメニュー オプション

Cisco ISE ノードでは、タスクを実行するために使用できる管理者ポータルが提供されています。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。プライマリ管理ノードによってすべての管理およびモニタリングのアクティビティを実行する必要があります。タスクの中には、セカンダリ ノードを使用する必要があるものがあります。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、異なる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 3-1　Cisco ISE ノードおよび使用可能なメニュー オプション

Cisco ISE ノード	使用可能なメニュー オプション
すべてのノード	• システム時刻と NTP サーバ設定の表示および設定。 • サーバ証明書のインストール、証明書署名要求の管理。 **（注）** サーバ証明書の操作は、各ノードで直接実行する必要があります。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。
プライマリ管理ノード	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	• ホーム メニュー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。

表 3-1　Cisco ISE ノードおよび使用可能なメニュー オプション （続き）

Cisco ISE ノード	使用可能なメニュー オプション
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 ノードがそれぞれ Active Directory ドメインに参加していることを確認します。最初にドメイン情報を定義し、プライマリ管理ノードを 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。
セカンダリ管理ノード	セカンダリ管理ノードをプライマリ管理ノードに昇格するオプション。 **（注）** プライマリ管理ノードにセカンダリ 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、プライマリ管理ノードのログイン クレデンシャ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 Cisco ISE ノードおよびセカンダリ 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。

セカンダリ管理ノードにログインして、このノードをプライマリ管理ノードとして実行する場合は、「セカンダリ管理ノードのプライマリへのプロモート」（P.3-17）を参照してください。

設定済みまたは実稼働の Cisco ISE のホスト名とドメイン名を変更しないことを推奨します。変更する必要がある場合は、最初の展開中にアプライアンスを再作成し、変更を加え、詳細を設定します。

はじめる前に

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」（P.3-9）を読んでおく必要があります。

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

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て、[編集（Edit）] をクリックします。

展開設定で説明されているフィールドのリストを含む [ノード編集（Node Edit）] ページが表示されます。

次の作業

1. 「プライマリ管理ノードの設定」（P.3-12）
2. 「セカンダリ Cisco ISE ノードの登録」（P.3-12）

関連項目

- 「Cisco ISE の分散展開」（P.3-7）
- 「分散展開を設定する場合のガイドライン」（P.3-9）
- 「モニタリング ノードでの自動フェールオーバーの設定」（P.3-18）
- 「スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録」（P.G-7）

プライマリ管理ノードの設定

分散展開を設定するには、Cisco ISE ノードをプライマリ管理ノード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、プライマリ管理ノード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、プライマリ管理ノードを設定します。

ステップ 4　展開設定の説明に従って、[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。

次の作業

1. プロファイラ サービスを有効にし、プローブを設定するには、「Cisco ISE ノードごとのプローブの設定」（P.21-14）を参照します。
2. 展開にセカンダリ ノードを追加するには、「セカンダリ Cisco ISE ノードの登録」（P.3-12）で説明されているようにセカンダリ ノードを正常に登録する必要があります。

関連項目

「スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録」（P.G-7）

セカンダリ Cisco ISE ノードの登録

ノードのタイプ（Cisco ISE またはインライン ポスチャ）は、登録時に決定することを推奨します。後でノード タイプを変更する場合は、ノードを展開から登録解除し、スタンドアロン ノードで Cisco ISE を再起動してから、そのノードを登録する必要があります。

ハイ アベイラビリティを実現するために、2 台の管理ノードを展開する予定の場合は、セカンダリ管理ノードを登録してから、その他のセカンダリ ノードを登録します。ノードがこの順序で登録された場合は、セカンダリ管理ノードをプライマリとして昇格した後にセカンダリ ISE ノードを再起動する必要はありません。

セッション サービスを実行する複数のポリシー サービス ノードを展開し、これらのノード間で相互フェールオーバーが設定される場合は、ノード グループにポリシー サービス ノードを配置します。ノードを登録する前にノード グループを作成する必要があります。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」（P.3-16）を参照してください。

セカンダリ ノードを登録した後、プライマリ ノードのデータベースにセカンダリ ノードの設定が追加され、セカンダリ ノードのアプリケーション サーバが再起動します。再起動が完了した後、セカンダリ ノードでは、そのノードに対して有効にしたペルソナおよびサービスが実行されます。

プライマリ管理ノードの [展開（Deployment）] ページで行ったすべての設定変更を表示できます。ただし、変更が [展開（Deployment）] ページに反映され、表示されるまで 5 分間の遅延が発生します。

はじめる前に

プライマリ ノードの証明書信頼リスト（CTL）に、登録するセカンダリ ノードの HTTPS 証明書を検証する適切な認証局（CA）証明書が含まれていることを確認します。

プライマリ管理ノードの CTL にインポートした証明書は、セカンダリ ノードに複製されます。

また、セカンダリ ノードをプライマリ ノードに登録後、セカンダリ ノードの HTTPS 証明書を変更する場合、適切な CA 証明書をプライマリ ノードの CTL にインポートする必要があります。

ステップ 1　プライマリ管理ノードにログインします。

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）] > [Cisco ISE ノードの登録（Register an Cisco ISE Node）] を選択して、セカンダリ Cisco ISE ノードを登録します。

ステップ 4　セカンダリ Cisco ISE ノードの DNS 解決可能なホスト名を入力します。

（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、プライマリ管理ノードから 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 サーバでセカンダリ ノードの IP アドレスおよび FQDN をあらかじめ定義しておく必要があります。

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、スタンドアロン 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　[次へ（Next）] をクリックします。

Cisco ISE はセカンダリ ノードに接続し、ホスト名、デフォルト ゲートウェイなどの基本情報を取得して、表示します。

セカンダリ Cisco ISE ノードを登録するよう選択している場合は、セカンダリ ノードの設定を編集できます。

セカンダリ インライン ポスチャ ノードを登録するよう選択している場合は、この時点で追加の設定を行う必要はありません。

ステップ 7　[保存（Save）] をクリックします。

結果

セカンダリ ノードが正常に登録されると、プライマリ管理ノードで、ノードの正常な登録を確認するアラームを受信します。セカンダリ ノードのプライマリ管理ノードへの登録が失敗した場合は、このアラームは生成されません。ノートが登録されると、そのノードのアプリケーション サーバが再起動

します。正常な登録およびデータベース同期の後に、プライマリ管理ノードのクレデンシャルを入力してセカンダリ ノードのユーザ インターフェイスにログインし、プライマリおよびセカンダリ ノードで使用可能なメニュー オプションにリストされている任意の操作を実行する必要があります。

（注）　展開内の既存のプライマリ ノードに加えて、新しいノードを正常に登録した場合は、新しく登録されたノードに対応するアラームは表示されません。設定変更アラームには、新しく登録されたノードに対応する情報が反映されます。新しいノードが正常に登録されたことを確認するためにこの情報を使用できます。

次の作業

- 時間プロファイル、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。システム時刻を同期する方法については、「システム時刻と NTP サーバ設定の指定」（P.5-3）を参照してください。
- ハイ アベイラビリティを設定するには、次の項で説明されている作業を完了する必要があります。
  - 「セカンダリ管理ノードのプライマリへのプロモート」（P.3-17）
  - 「モニタリング ノードでの自動フェールオーバーの設定」（P.3-18）
- 展開にインライン ポスチャ ノードを追加するには、「インライン ポスチャの設定」（P.4-1）で説明されている手順を実行します。

関連項目

- 「展開設定」（P.A-1）
- 「Cisco ISE ノード間通信用の CA 証明書のインストール」（P.8-30）

インライン ポスチャ ノードの登録

ノードのタイプ（Cisco ISE またはインライン ポスチャ）は、登録時に決定することを推奨します。後でノード タイプを変更する場合は、ノードを展開から登録解除し、スタンドアロン ノードで Cisco ISE を再起動してから、そのノードを登録する必要があります。

はじめる前に

- プライマリ ノードの証明書信頼リスト（CTL）に、登録するセカンダリ ノードの HTTPS 証明書を検証する適切な認証局（CA）証明書が含まれていることを確認します。
- セカンダリ ノードをプライマリ ノードに登録後、セカンダリ ノードの HTTPS 証明書を変更する場合、適切な CA 証明書をプライマリ ノードの CTL にインポートする必要があります。

ステップ 1　プライマリ管理ノードにログインします。

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。

ステップ 4　[登録（Register）] > [インライン ポスチャ ノードの登録（Register an Inline Posture Node）] を選択して、セカンダリ インライン ポスチャ ノードを登録します。

関連項目

- 「展開設定」（P.A-1）

- 「Cisco ISE ノード間通信用の CA 証明書のインストール」（P.8-30）
- 第 4 章「インライン ポスチャの設定」

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、つまりプライマリ 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　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。

ステップ 4　[展開ノード（Deployment Nodes）] ページのフィールドについては、展開設定を参照してください。

このページでは、次の操作が可能です。

- ノードの編集。このオプションは、単一のノードを選択した場合にのみ有効になります。ノードを選択した後に、[編集（Edit）] ボタンをクリックして、そのノードのペルソナおよびロールを編集します。
- セカンダリ ノードの登録。このオプションは、プライマリ管理ノードを設定した後にのみ有効になります。[登録（Register）] をクリックして、Cisco ISE ノードまたはインライン ポスチャ ノードを登録します。
- プライマリ ノードから選択したセカンダリ ノードへのデータベースの完全複製の開始。
- 1 つ以上のセカンダリ ノードの登録解除。

プライマリ ISE ノードとセカンダリ Cisco ISE ノードの同期

プライマリ管理ノードを介してのみ、Cisco ISE に対する設定変更を行えます。設定変更は、すべてのセカンダリ Cisco ISE に複製されます。何らかの理由で、この複製が正しく行われなかった場合は、手動でセカンダリ管理ノードをプライマリ管理ノードに同期できます。

はじめる前に

[同期ステータス（Sync Status）] が [同期していない（Out of Sync）] の場合や [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　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　プライマリ管理ノードと同期をとるノードの隣にあるチェックボックスをオンにし、[同期を更新（Syncup）] をクリックしてデータベースの完全複製を強制的に実行します。

ポリシー サービス ノード グループの作成

ロード バランシングで要求を均等に分散するために、複数のポリシー サービス ノードを展開できます。ノード障害を検出し、障害が発生したノードで保留状態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 グループにノードを追加するには、ノード グループを作成する必要があります。

Cisco ISE 管理者ポータルの [展開（Deployment）] ページからポリシー 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。

はじめる前に

- ノード グループに属するすべてのノードがレイヤ 2 で隣接している、つまり同じサブネット上にあるか、または IP マルチキャストをサポートするルーテッド LAN ネットワークを介して接続されていることを確認します。
- 同じノード グループに属しているノード間の IP マルチキャストを有効にします。通常、ノード グループ内のすべてのノードは、同じスイッチに接続され、同じ VLAN 内にあります。レイヤ 3 接続を介したマルチキャストもサポートされますが、同じノード グループのメンバーを接続するすべてのスイッチで適切に IP マルチキャストを設定する必要があります。簡単にし、アベイラビリティを向上させるために、ノード グループ内のすべてのノードがレイヤ 2 で隣接していることを推奨します。
- ノード グループのメンバーが UDP/45588、UDP/45590、および TCP/7802 で通信できることを確認します。
- ノード グループに同じマルチキャスト アドレスが設定されていないことを確認します。
- ノード グループに割り当てるマルチキャスト アドレスが、展開内の他のネットワーク プロトコルで使用するために予約されていないことを確認します。Cisco ISE では、入力したマルチキャスト アドレスが許可された有効なマルチキャスト アドレスであるかどうかが確認されます。224.0.0.0 をマルチキャスト アドレスとして使用することは許可されませんが、マルチキャスト アドレスの予約リストは点検されません。使用することができない予約済みマルチキャスト アドレスのリストは、http://www.iana.org/assignments/multicast-addresses/ multicast-addresses.xml 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　[操作（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　一意のマルチキャスト アドレスを入力します。マルチキャスト アドレスは、ノードの健全性のモニタおよびセッション クリーンアップのための、グループ内のノード間での通信に使用されます。マルチキャスト アドレスは 224.0.0.1 と 239.255.255.255 の間である必要があります。

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。

結果

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ない場合は、非表示になっている可能性があります。ナビゲーション ペインで [展開（Expand）] ボタンをクリックして非表示のオブジェクトを表示します。

次の作業

- ノード グループにノードを追加するには、[ノード グループ（Node Group）] ドロップダウン リストのメンバーからノード グループを選択して、ノードを編集する必要があります。
- ノード グループからノードを削除するには、[ノード グループ（Node Group）] ドロップダウン リストのメンバーから [<なし>（<none>）] を選択して、ノードを編集する必要があります。

関連項目

- 「展開設定」（P.A-1）
- 「スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録」（P.G-7）

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。

はじめる前に

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開するまでに遅延が生じます。

ステップ 1　プライマリ管理ノードにログインします。

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　必要なペルソナとサービスを選択します。

ステップ 5　[保存（Save）] をクリックします。

ステップ 6　ペルソナまたはサービスの変更を確認するため、プライマリ管理ノードでアラームの受信を確認します。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。

関連項目

- 「スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録」（P.G-7）
- 「ポリシー サービス ノードを管理ノードに登録した後にモニタリングおよびトラブルシューティング データを消失」（P.G-13）

セカンダリ管理ノードのプライマリへのプロモート

プライマリ管理ノードに障害が発生した場合は、手動でセカンダリ管理ノードを新しいプライマリ ノードに昇格する必要があります。

元はプライマリ管理ノードであったこのノードは、再起動するとセカンダリ管理ノードになります。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のでペルソナまたはサービスを変更することはできません。変更するには、管理者ポータルにログインする必要があります。

はじめる前に

プライマリ管理ノードとして昇格するために管理ペルソナを持つ 2 番めの ISE ノードを設定したことを確認します。

ステップ 1　セカンダリ管理ノードのユーザ 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。

（注）　プライマリ管理ノードに昇格できるのは、セカンダリ管理ノードのみです。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管理ノードに昇格できません。

ステップ 4　[保存（Save）] をクリックします。

ステップ 5　セカンダリ管理ノードを登録する前に元のプライマリ管理ノードに登録されていたセカンダリ Cisco ISE ノードを再起動します。

たとえば、セカンダリ Cisco ISE ポリシー サービスとモニタリング ノードを登録した後にセカンダリ管理ノード（新しいプライマリ）を登録した場合、セカンダリ管理ノードが登録される前に登録されたセカンダリ Cisco ISE ノードを再起動する必要があります。

次の作業

セカンダリ管理ノードをプライマリ管理ノードに昇格した後に、新しく昇格されたプライマリ管理ノードのスケジュール設定された Cisco ISE バックアップを再設定する必要があります。これは、スケジュール バックアップはプライマリ管理ノードからセカンダリ管理ノードに複製されないためです。詳細については、「バックアップのスケジュール作成」（P.12-5）を参照してください。

モニタリング ノードでの自動フェールオーバーの設定

展開内に 2 つのモニタ ノードがある場合、Cisco ISE モニタリング サービスのダウン時間を回避するために、プライマリとセカンダリのペアを自動フェールオーバー用に設定できます。プライマリとセカンダリのペアは、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することを保証します。

はじめる前に

- モニタリング ノードを自動フェールオーバー用に設定するには、これらのノードを Cisco ISE ノードとして登録する必要があります。この手順は「分散展開を設定する場合のガイドライン」（P.3-9）および「Cisco ISE ノードの設定」（P.3-11）で説明します。
- 両方のノードでモニタリング ロールおよびサービスを指定し、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る必要があります。
- 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、それぞれに同じリポジトリを使用する必要があります。これは、バックアップおよび消去機能を正しく動作させるために重要です。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 リポジトリを設定できます。詳細については、「モニタリング データベースのバックアップおよび復元」（P.25-30）および『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

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する必要があります。リポジトリは、2 つのノード間で自動的には同期されません。

はじめる前に

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）] 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）] 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。このノードは、プライマリ管理ノードから受信した最後の設定を保持し、スタンドアロン ノードのデフォルトのペルソナである管理、ポリシー サービス、およびモニタリングを担当します。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 ターゲットでなくなります。

プライマリ管理ノードの [展開（Deployment）] ページでこれらの変更を表示できます。ただし、変更が [展開（Deployment）] ページに反映され、表示されるまで 5 分間の遅延が発生します。

はじめる前に

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）] 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　セカンダリ ノードが正常に登録解除されたことを確認するため、プライマリ管理ノードでアラームの受信を確認します。セカンダリ ノードのプライマリ管理ノード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。

関連項目

「スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録」（P.G-7）

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。

はじめる前に

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** 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 reset-config** 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　分散展開の一部である場合は、Cisco ISE ノードをプライマリ管理ノードに登録します。

（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、プライマリ管理ノードから 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。

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

関連項目

- *『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』*
- 「展開からのノードの削除」（P.3-19）
- 「セカンダリ Cisco ISE ノードの登録」（P.3-12）

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　展開からノードを削除します。

ステップ 2　新しいノードをセカンダリ サーバとしてプライマリ管理ノードに登録します。

ステップ 3　削除されたノードで実行されていたのと同じペルソナおよびサービスを設定します。

関連項目

- 「展開からのノードの削除」（P.3-19）
- 「セカンダリ Cisco ISE ノードの登録」（P.3-12）
- 「Cisco ISE ノードの設定」（P.3-11）