# 管理 ISE-PIC



# ISE-PIC ノードの管理

セカンダリードの追加または削除、ノード間のデータの同期、セカンダリノードのプライマリノードへの昇格などを行います。

## Cisco ISE-PIC 展開のセットアップ

『*Cisco Identity Services Engine Hardware Installation Guide*』で説明されているように Cisco ISE-PIC 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（PAN）として定義し、セカンダリノードを PAN に登録する必要があります。

すべての Cisco ISE-PIC システムおよび機能に関連する設定は、PAN でだけ実行する必要があります。PAN で行った設定の変更は、展開内のセカンダリ ノードに複製されます。セカンダリノードからは、セカンダリノードを PAN に昇格させるアクションのみを実行できます。

セカンダリノードを PAN に登録した後は、そ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、PAN のログインクレデンシャルを使用する必要があります。

## プライマリからセカンダリ ISE-PIC 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-PIC 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-PIC 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 2 つの Cisco ISE-PIC 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-PIC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 Cisco ISE-PIC ノードが同期されます。Cisco ISE-PIC 管理者ポータルの展開のページから [ノードステータス（Node Status）] 列で複製のステータスを表示できます。セカンダリ ノードとして Cisco ISE-PIC ノードを登録するか、または PAN との手動同期を実行すると、要求されたアクションが進行中であることを示すオレンジのアイコンがノードステータスに表示されます。これが完了すると、ノード ステータスは、セカンダリ ノードが PAN と同期されたことを示す緑に変わります。

# Cisco ISE-PIC でのノードの変更による影響

Cisco ISE-PIC 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）
- ノードの昇格（セカンダリからプライマリへ）
- 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）

# 展開で 2 つのノードを設定する場合のガイドライン

2つのノードを使用してCisco ISE-PICをセットアップする前に、次の内容をよく読んでください。

- 両方のノードに同じ Network Time Protocol（NTP）サーバを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ中に同じ NTP サーバ名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE-PIC のインストール時に Cisco ISE-PIC の管理者パスワードを設定します。以前の Cisco ISE-PIC 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 サーバでの展開に含まれる両方のCisco ISE-PIC 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 サーバからのハイアベイラビリティ展開の Cisco ISE-PIC ノードの両方に正引きと逆引きの DNS ルックアップを設定します。設定しなかった場合、Cisco ISE-PIC 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。両方のノードに逆引き DNS ルックアップが設定されていない場合は、パフォーマンスが低下する可能性があります。

- （任意）PAN からセカンダリ Cisco ISE-PIC ノードを登録解除して、Cisco ISE-PIC をアンインストールします。
- 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-PIC が実行されていることを確認します。

# 展開内のノードの表示

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

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

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

展開を構成するすべての Cisco ISE ノードが表示されます。

# セカンダリ Cisco ISE-PIC ノードの登録

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。再起動が完了すると、PAN の [展開（Deployment）] ページから行ったすべての設定変更を表示できます。ただし、変更が反映され、[展開（Deployment）] ページに表示されるには 5 分間の遅延が生じます。

**ステップ 1** PAN にログインします。

**ステップ 2** **[管理（Administration）]** > **[展開（Deployment）]** を選択します。
展開にセカンダリノードが登録されていない場合は、ページの下部に [セカンダリノードの追加（Add Secondary Node）] セクションが表示されます。

**ステップ 3** [セカンダリノードの追加（Add Secondary Node ）] セクションで、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。

Cisco ISE-PIC 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、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 サーバでセカンダリ ノードの IP アドレスおよびFQDN を事前に定義しておく必要があります。

**ステップ 4** [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 5** **[保存（Save）]** をクリックします。

Cisco ISE-PIC 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。

セカンダリノードが展開に登録されるとノードが再起動しますが、[展開（Deployment）]ページからセカンダリノードの情報が表示されるまでに最大 5 分かかることがあります。

セカンダリノードが正常に登録されると、[展開（Deployment）] ページの[セカンダリノード（Secondary Node）] セクションにそのノードの詳細が表示されます。

セカンダリ ノードが正常に登録されると、PAN 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 PAN 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。登録およびデータベース同期が正常に完了した後、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するにはプライマリ管理ノードのクレデンシャルを入力します。

（注） 展開の既存のプライマリ ノードに加えて、新しいノードの登録に成功した場合は、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。設定変更アラームは、新しく登録されたノードに対応する情報を反映します。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。

# プライマリおよびセカンダリの Cisco ISE-PIC ノードの同期

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

### 始める前に

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

**ステップ 1** プライマリ PAN にログインします。

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

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

# セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗した場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

### 始める前に

プライマリ PAN に昇格するように設定された 2 番目の Cisco ISE-PIC ノードがあることを確認します。

**ステップ 1** セカンダリ PAN のユーザ インターフェイスにログインします。
**ステップ 2** **[管理（Administration）]** > **[展開（Deployment）]** を選択します。
**ステップ 3** [プライマリに昇格（Promote to Primary）] をクリックします。
**ステップ 4** [保存（Save）] をクリックします。

### 次のタスク

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

# 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-PIC ノードになります。

ノード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。ノードがスタンドアロンノードになった後で、そのノードでエンドポイントデータを保持するには、プライマリ PAN からバックアップを取得し、そのノードでこのデータ バックアップを復元できます。

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

### 始める前に

展開から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。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。

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

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

**ステップ 2** セカンダリ ノードの詳細の隣にある [登録解除（Deregister）] をクリックします。

**ステップ 3** [OK] をクリックします。

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

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

### 始める前に

Cisco ISE-PIC ノードが 2 ノード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-PIC 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-PIC 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-PIC ノードは、2 ノード展開の一部である場合、プライマリ PAN に登録します。

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

# Cisco ISE-PIC アプライアンス ハードウェアの交換

Cisco ISE-PIC 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-PIC ソフトウェアを再インストールできます。

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

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

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

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

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

# ISE-PIC のインストールの管理

パッチのインストール、バックアップの実行、またはシステムの復元の実装を行います。

## ソフトウェアパッチのインストール

**ステップ 1** **[管理（Administration）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択し、[インストール（Install）] をクリックします。

**ステップ 2** [参照（Browse）] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

**ステップ 3** [インストール（Install）] をクリックしてパッチをインストールします。

PAN でのパッチのインストールが完了すると、Cisco ISE-PIC から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

（注） パッチインストールの進行中は、[パッチ管理（Patch Management）]ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

**ステップ 4** **[管理（Administration）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択して、[パッチのインストール（Patch Installation）] ページに戻ります。

**ステップ 5** セカンダリノードにインストールしたパッチの横のオプションボタンをクリックし、[ノードステータスを表示（Show Node Status）] をクリックしてインストールが完了したことを確認します。

### 次のタスク

セカンダリノードでパッチをインストールする必要がある場合は、ノードが動作中であることを確認し、プロセスを繰り返して残りのノードにパッチをインストールします。

## Cisco ISE-PIC ソフトウェアパッチ

Cisco ISE-PIC ソフトウェアパッチは通常累積されます。Cisco ISE-PIC では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

展開内の Cisco ISE-PIC サーバにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUIにリストされている順序で、展開内の他のノードにパッチをインストールします。ノードが更新される順序を制御することはできません。パッチバージョンを手動でインストール、ロールバック、および表示することもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します[管理（Administration）] > [システム（System）] > [メンテナンス（ Maintenance）] > [パッチ管理（Patch Management）]。

CLIからパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。

展開全体をアップグレードする前にいくつかのノードでパッチを検証する場合、CLIを使用すると、選択したノードでパッチをインストールできます。パッチをインストールするには、次の CLI コマンドを使用します。

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

詳細については、『Cisco Identity Services Engine CLI Reference Guide』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「install Patch」の項を参照してください。

必要なパッチバージョンを直接インストールすることができます。たとえば、Cisco ISE 2.x を使用していて、Cisco ISE 2.x パッチ 5 をインストールする場合、以前のパッチ（Cisco ISE 2.x パッチ 1 ～ 4 など）をインストールしなくても、Cisco ISE 2.x パッチ 5 を直接インストールできます。CLI でパッチバージョンを表示するには、次の CLI コマンドを使用します。

```
show version
```

## ソフトウェア パッチ インストールのガイドライン

ISE ノードにパッチをインストールすると、インストールの完了後にノードが再起動されます。再びログインできる状態になるまで、数分かかることがあります。メンテナンスウィンドウ中にパッチをインストールするようにスケジュール設定し、一時的な機能停止を回避することができます。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE-PIC のバージョンに適用されるものであることを確認してください。Cisco ISE-PIC はパッチファイルのバージョンの不一致とあらゆるエラーをレポートします。

（注） Cisco ISE パッチは、ISE-PIC にもインストールできます。

Cisco ISE-PIC に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE-PIC にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE-PIC サーバにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

2 ノード展開の一部であるプライマリ PANからパッチのインストールを実行するときは、Cisco ISE-PIC によってそのパッチが展開内のプライマリノードとセカンダリノードにインストール

されます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE-PIC はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。

# ソフトウェアパッチのロールバック

複数のノードの展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISE-PIC によってそのパッチが展開内のプライマリノードとセカンダリノードにロールバックされます。

**ステップ 1** **[管理（Administration）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します

**ステップ 2** 変更をロールバックするパッチバージョンのオプションボタンをクリックしてから、[ロールバック（Rollback）] をクリックします。

（注） パッチのロールバックの進行中は、[パッチ管理（Patch Management）] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

PAN からのパッチのロールバックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

**ステップ 3** ログイン後に、ページの一番下にある [アラーム（Alarms）] リンクをクリックしてロールバック操作のステータスを表示します。

**ステップ 4** パッチのロールバックの進行状況を表示するには、[パッチ管理（Patch Management）] ページでパッチを選択し、[ノードステータスを表示（Show Node Status）] をクリックします。

**ステップ 5** パッチのオプションボタンをクリックし、セカンダリノード上で [ノードステータスを表示（Show Node Status）] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE-PIC は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

## ソフトウェア パッチ ロールバックのガイドライン

展開の Cisco ISE-PIC ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリノードからパッチがロールバックされます。PAN でロールバックプロセスが失敗した場合は、セカンダリノードからのパッチロールバックは行われません。

Cisco ISE-PIC によるセカンダリノードからのパッチロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリノードは、ロールバック後に再起動されます。

# バックアップと復元データ

（注） シスコ ISE-PIC は、多くの場合、Cisco ISE のバックアップおよび復元の手順と同じように機能します。そのため、Cisco ISE-PIC に関連する操作や機能を示すために Cisco ISE という用語を同義で使用する場合があります。

Cisco ISE-PIC では、プライマリ ノードまたはスタンドアロン ノードからデータをバックアップできます。バックアップは CLI またはユーザ インターフェイスから実行できます。

Cisco ISE-PIC では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。
- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。

## バックアップ/復元リポジトリ

Cisco ISE-PIC では、リポジトリを作成および削除できます。次のタイプのリポジトリを作成できます。

- ディスク（DISK）
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

KVM を使用して作成された仮想 CD-ROM を CD-ROM としてリポジトリ タイプを作成できます。

（注） リポジトリは、各デバイスに対してローカルです。

（注） 小規模な展開（100 個以下のエンドポイント）では、10 GB のリポジトリを、中規模の展開では 100 GB のリポジトリを、大規模な展開では 200 GB のリポジトリを用意することを推奨します。

# リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリは、他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このためアップグレード時に、新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバにエクスポートする必要があります。展開からノードを除去する場合、非管理ノードの GUI でキーを生成し、SFTP サーバにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE-PIC の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュア キーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバにエクスポートします。

### 始める前に

- RSA 公開キー認証を使用する SFTP リポジトリを作成する場合は、次を実行してください。
  - SFTP リポジトリの RSA 公開キー認証を有効にします。
  - **crypto host_key add** コマンドを使用して Cisco ISE CLI から SFTP サーバのホスト キーを入力します。ホスト キー文字列は、リポジトリの設定ページで、[パス（Path）] フィールドに入力したホスト名と一致する必要があります。
  - GUI でキーペアを生成し、ローカル システムに公開キーをエクスポートします。Cisco ISE CLI から **crypto key generate rsa passphrase***test123* コマンドを使用してキー ペアを生成し（この場合パスフレーズは 5 文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。
  - エクスポートした RSA 公開キーを PKI 対応の SFTP サーバにコピーし、「authorized_keys」ファイルに追加します。

**ステップ 1** [管理（Administration）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** [追加（Add）] をクリックして、新しいリポジトリを追加します。

**ステップ 3** 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、リポジトリの設定 （12 ページ）を参照してください。

**ステップ 4** [送信（Submit）] をクリックしてリポジトリを作成します。

**ステップ 5** 左側の [操作（Operations）] ナビゲーション ペインで [リポジトリ（Repository）] をクリックするか、このページ上部の [リポジトリ リスト（Repository List）] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。

### 次のタスク

- 作成したリポジトリが有効であることを確認します。これは、リポジトリのリストページから行います。リポジトリを選択し、[確認（Validate）] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

  **show repository** *repository_name*

  ここで、*repository_name* は作成したリポジトリの名前です。

  （注） リポジトリの作成時に指定したパスが存在しない場合、「%無効なディレクトリです（%Invalid Directory）」というエラーが表示されます。

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

## リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリ リスト（Repository List）] ページのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します**[管理（Administration）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]**。

**表 *1:* リポジトリの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| リポジトリ （Repository） | リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。 |
| プロトコル | 使用する使用可能なプロトコルの 1 つを選択します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ホスト | （TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバのホスト名または IP アドレス（IPv4 または IPv6）を入力します。<br>（注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。 |
| パス | リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。<br>この値は、サーバのルート ディレクトリを示す2つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルート ディレクトリではなく FTP ユーザのホーム ディレクトリを示します。 |

**関連トピック**

バックアップ/復元リポジトリ
リポジトリの作成 （11 ページ）

## SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバでは、各ノードに 2 つの RSA 公開キー（CLI 用と GUI 用にそれぞれ 1 つずつ）が必要です。SFTP リポジトリの RSA 公開キー認証を有効にするには、以下のステップに従います。

**ステップ 1** */Etc/ssh/sshd_config.file* を編集する権限を持つアカウントで SFTP サーバにログインします。

（注） *sshd_config* ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

**ステップ 2** **vi etc/ssh/sshd_config** コマンドを入力します。

Sshd_config ファイルの内容がリストされます。

**ステップ 3** RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- RSAAuthentication yes
- PubkeyAuthentication yes

（注） Public Auth Key が no の場合は yes に変更してください。

- AuthorizedKeysFile ~/.ssh/authorized_keys

## オンデマンドおよびスケジュール バックアップ

プライマリ PAN のオンデマンドバックアップを設定できます。バックアップ データがすぐに必要な場合にオンデマンド バックアップを実行します。

システムレベルのバックアップは、1 回のみ、毎日、毎週、または毎月実行するようにスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできるため中断が発生することはありません。管理者ポータルからバックアップをスケジュールできます。

（注） 内部 CA を使用している場合は、CLI を使用して証明書とキーをエクスポートする必要があります。管理ポータルのバックアップでは、CA チェーンはバックアップされません。

詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Basic Setup」の章にある「Export Cisco ISE CA Certificates and Keys」の項を参照してください。

### オンデマンド バックアップの実行

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE-PIC が復元されます。

**重要** バックアップと復元を行う場合、復元によって、ターゲット システムの信頼できる証明書のリストがソース システムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE-PIC ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  **長所**：ソース システムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  **短所**：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  **長所**：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソース システムによって発行された証明書は引き続き信頼されます。

  **短所**：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

### 始める前に

- この作業を実行する前に、Cisco ISE-PIC のバックアップ データのタイプの基本を理解している必要があります。
- バックアップファイルを格納するリポジトリを作成したことを確認します。
- ローカルリポジトリを使用してバックアップしないでください。

**ステップ 1** **[管理（Administration）] > [メンテナンス（Maintenance）] > [バックアップ/復元（Backup and Restore）]** ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** バックアップのタイプ [設定（Configuration）] または [動作中（Operational）] を選択します。

**ステップ 3** [すぐにバックアップ（Backup Now）] をクリックします。

**ステップ 4** バックアップを実行するために必要な値を入力します。

**ステップ 5** [OK][バックアップ（Backup）]をクリックします。

**ステップ 6** バックアップが正常に完了したことを確認します。

Cisco ISE-PIC はタイムスタンプを持つバックアップ ファイル名を付け、指定されたリポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE-PIC は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

（注） バックアップが実行されているときに、高いCPU使用率が観察されたり、[負荷平均が高い（High Load Average）] アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

## バックアップのスケジュール

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE-PIC が復元されます。

**重要** バックアップと復元を行う場合、復元によって、ターゲットシステムの信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE-PIC ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  **長所**：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

  **短所**：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  **長所**：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

  **短所**：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

### 始める前に

- この作業を実行する前に、Cisco ISE-PIC のバックアップ データのタイプの基本を理解している必要があります。
- リポジトリを設定していることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。

**（注）** バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

## CLI を使用したバックアップ

CLI と GUI の両方からバックアップをスケジュールできますが、GUI から実行することを推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

## バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップ ファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイム スタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元（Backup and Restore）] ページから入手できます。

バックアップが失敗すると、Cisco ISE-PIC がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティング システムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

## バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- NTP 同期またはサービス障害の問題があるかどうかを確認します。Cisco ISE の NTP サービスが動作していない場合、Cisco ISE では、[NTPサービスの障害（NTP Service Failure）] のアラームが発生します。Cisco ISE が、設定されているすべての NTP サーバと同期できない場合、Cisco ISE では、[NTP同期に失敗（NTP Sync Failure）] のアラームが発生します。NTP サービスがダウンしている場合、または同期の問題がある場合は、Cisco ISE のバックアップが失敗する可能性があります。バックアップ操作を再試行する前に、[アラーム（Alarm）] ダッシュレットを確認し、NTP 同期またはサービスの問題を修正してください。
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
  - （操作）バックアップのモニタリングは、モニタリング データがモニタリング データベースに割り当てられたサイズの 75% を超えると失敗します。たとえばノードに 600 GB 割り当てられており、モニタリング データがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。
  - データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。

- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

## Cisco ISE 復元操作

プライマリまたはスタンドアロン ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

（注） Cisco ISE-PIC の新しいバックアップ/復元ユーザ インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE-PIC バックアップ/復元ユーザ インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップ ファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

### データの復元に関するガイドライン

次は、Cisco ISE-PIC バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード（A）からバックアップを取得して、別の ISE ノード（B）に復元することができます。両方のノードは同じホスト名（IP アドレスは異なる）です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE-PIC ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE-PIC ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE-PIC ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。
  - **application reset-config ise**
- システムのタイムゾーンは、最初の Cisco ISE-PIC インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE-PIC ノードまたはプライマリ PAN から取得する

必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。

（注） Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] > [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA certificate chain）]**）。ただし、適切な FQDN でプラチナ データベースを復元する場合は、CA 証明書が自動的に再生成されます。

- Cisco ISE-PIC がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。

- スタンドアロンノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、セカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。

（注） Cisco ISE-PIC では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーションファイルの収集を行い、これらをトラブルシューティングに利用できます。

## CLI からの設定またはモニタリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

**restore** *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

構文の説明

| | |
|---|---|
| **restore** | 設定または操作バックアップからデータを復元するには、このコマンドを入力します。 |

| | |
|---|---|
| *filename* | リポジトリに存在するバックアップ ファイルのファイル名。最大120文字の英数字をサポートします。<br>（注） ファイル名の後に、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。 |
| **repository** | バックアップを含むリポジトリを指定します。 |
| *repository-name* | バックアップを復元するリポジトリの名前。 |
| **encryption-key** | （オプション）バックアップを復元するユーザ定義の暗号キーを指定します。 |
| **hash** | バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された（ハッシュ化された）暗号化キーを指定します。40 文字までで指定します。 |
| **plain** | バックアップを復元するためのプレーン テキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。 |
| *encryption-key name* | 暗号キーを入力します。 |
| **include-adeos** | （オプション、設定バックアップのみに該当）設定バックアップから ADE-OS 設定を復元する場合に、このコマンドオペレータ パラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。 |

### デフォルト

デフォルトの動作や値はありません。

### コマンド モード

EXEC

### 使用上のガイドライン

Cisco ISE-PIC で restore コマンドを使用すると、Cisco ISE-PIC サーバが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

### 例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

### 関連コマンド

| | 説明 |
|---|---|
| **backup** | バックアップ（Cisco ISE-PIC と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。 |
| **backup-logs** | システム ログをバックアップします。 |
| **repository** | バックアップ設定のリポジトリ サブモードを入力します。 |
| **show repository** | 特定のリポジトリにある使用可能なバックアップ ファイルを表示します。 |
| **show backup history** | システムのバックアップ履歴を表示します。 |
| **show backup status** | バックアップ操作のステータスを表示します。 |
| **show restore status** | 復元操作のステータスを表示します。 |

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

### GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。GUIには現在のリリースから取得されたバックアップのみが表示されます。このリリースより前のバックアップを復元するには、CLIから restore コマンドを使用します。

**ステップ 1** **[管理（Administration）] > [メンテナンス（Maintenance）] > [バックアップ/復元（Backup and Restore）]** ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** バックアップの名前を設定バックアップのリストから選択し、[復元（Restore）] をクリックします。

**ステップ 3** バックアップ時に使用した暗号キーを入力します。

**ステップ 4** [復元（Restore）] をクリックします。

#### 次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

### 復元履歴

操作監査レポートからは、すべての復元操作、ログイベント、ステータスに関する情報を取得することができます。

（注） ただし操作監査レポートには、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE-PIC サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

## プライマリ ノードとセカンダリ ノードの同期

PANのバックアップファイルの復元後に、プライマリおよびセカンダリノードのCisco ISE-PICデータベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE-PIC ノードへの完全複製を手動で強制実行できます。強制同期は、PAN からセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE-PIC で

は、同期が完全に完了した後にのみ、他の Cisco ISE-PIC 管理者ポータル ページに移動して設定変更を行うことができます。

**ステップ 1** **[管理（Administration）] > [展開（Deployment）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** 非同期レプリケーション ステータスのセカンダリ 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 3** [同期を更新（Syncup）] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE-PIC 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

## スタンドアロンおよび2 ノード展開での失われたノードの復元

この項では、スタンドアロンおよび2 ノード展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

### 2 ノード展開での既存 IP アドレスとホスト名を使用しての失われたノードの復元

#### シナリオ

2 ノード展開では、自然災害が全ノードの損失につながります。復元後に、既存IPアドレスとホストネームを使用します。

たとえば、2 つのノード、N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

#### 前提

展開内のすべての Cisco ISE-PIC ノードが破壊されました同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

#### 解決手順（Resolution Steps）

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンドアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。
3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしますが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

## 2 ノード展開の新 IP アドレスとホスト名を使用しての失われたノードの復元

### シナリオ

2 ノード展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE-PIC ノード N1（プライマリ ポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ノード）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE-PIC ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

### 前提条件

展開内のすべての Cisco ISE-PIC ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

### 解決手順（Resolution Steps）

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. 古い N2 ノードを削除します。

   新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

## スタンドアロン展開の既存 IP アドレスとホスト名によるノードの復元

### シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノードN1があったとします。N1データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

### 前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

### 解決手順（Resolution Steps）

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE-PIC ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

## スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

### シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

### 前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

### 解決手順（Resolution Steps）

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

## 設定のロール バック

### 問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の設定に戻すことができます。

### 考えられる原因

N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

### ソリューション

誤った設定変更を行う前に取得した N1 ノードのバックアップを入手します。N1 ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

## 2 ノード展開での障害発生時のプライマリ ノードの復元

### シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE-PIC ノード、N1（PAN）と N2（セカンダリ管理ノード）があります。ハードウェアの問題で N1 に障害が発生します。

### 前提条件

2 ノード展開内のプライマリ ノードのみに障害が発生します。

### 解決手順（Resolution Steps）

1. N2 管理者ポータルにログインします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します N2 をプライマリノードとして設定します。

   N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリ ノードとして新しい N1 ノードを登録します。

   これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリ ノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリ ノードに設定します。N2 は、自動的にセカンダリ サーバとなります。データが失われることはありません。

## 2 ノード展開での障害発生時のセカンダリ ノードの復元

### シナリオ

マルチノード展開で、1 台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

### 解決手順（Resolution Steps）

1. セカンダリ ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. プライマリ ノードから管理者ポータルにログインし、セカンダリ ノードを削除します。
3. セカンダリ ノードを再登録します。

   データはプライマリ ノードからセカンダリ ノードに複製されます。復元の必要はありません。

# 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、データベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク領域使用率しきい値（ディスク領域のパーセンテージ）に達したときに使用されます。このオプションでは、各月は 30 日で構成されます。デフォルトの 3 ヵ月は 90 日間です。

## データベースの消去に関するガイドライン

次に、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。

- データベースのディスク使用量がしきい値設定の 80% を超えた場合、データベース サイズが割り当てられたディスク サイズを超過したことを示すクリティカル アラームが生成されます。ディスク使用量が 90% より大きい場合は、別のアラームが生成されます。
- 消去は、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。データベースの使用済みディスク領域がしきい値（デフォルトは80%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、過去7日間のモニタリング データのみを削除します。ディスク領域が 80% 未満になるまで繰り返しプロセスを続行します。消去では、処理の前にデータベースのディスク領域制限が常にチェックされます。

## 運用データの消去

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

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

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

### 関連トピック

古い運用データの消去 （28 ページ）

## 古い運用データの消去

運用データはサーバに一定期間集められています。すぐに削除することも、定期的に削除することもできます。

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

**ステップ 2** 次のいずれかを実行します。

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

  1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。ISE-PIC には RADIUS または TACACS 機能がありませんが、インフラストラクチャの一部が ISE と共有されます。このため、データベースからこのような情報を定期的に消去する必要があります。
  2. [リポジトリ（Repository）] 領域で、[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、データを保存するリポジトリを選択します。詳細については、「リポジトリの作成」の項を参照してください。
  3. [暗号キー（Encryption Key）] テキスト ボックスに必要なパスワードを入力します。
  4. [保存（Save）] をクリックします。

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

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

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

# 完全な ISE インストールへの ISE-PIC のアップグレード

Cisco ISE-PIC は、完全な Cisco ISE GUI に基づくシンプルで直感的な GUI に表示されます。このため、ISE-PIC をインストールすると、ISE へ迅速かつ効率的にアップグレードできます。ISE-PIC から ISE の Base ライセンスにアップグレードすると、ISE では引き続き、アップグレード前に ISE-PIC で使用可能だった機能がすべて提供されます。アップグレードした ISE-PIC ノードをプライマリ PAN として使用している場合は、すでに設定している設定値を設定し直す必要はありません。

（注） アップグレードした既存の ISE-PIC ノードをプライマリ PAN として使用しない場合、アップグレード時にそのノードのデータは消去され、新しく追加したノードから、既存の完全な ISE 展開のデータにアクセスできるようになります。

フル アップグレードを実行するには、まず ISE-PIC アップグレード ライセンスをノードにインストールし、次のいずれかの操作を行います。

- アップグレードした ISE-PIC ノードを既存の ISE 展開に追加する。
- Base ライセンス以上のライセンスをインストールする。

（注） 完全な Cisco ISE 展開にアップグレードすると、以前の Cisco ISE-PICインストール環境にロールバックすることはできません。

ISE へのアップグレードの利点の詳細については、ISE および CDA と ISE-PIC の比較を参照してください。

# ライセンスの登録による ISE へのアップグレード

### 始める前に

シスコ ISE-PIC の永久ライセンスがインストールされていることを確認します。さらに、次のいずれかの方法でノードをアップグレードできます。

- 既存の完全な ISE の展開に ISE-PIC ノードを追加します。アップグレードされた ISE-PIC ノードは、セカンダリノードとして既存の展開に参加します。これを行うには、Cisco ISE-PIC のアップグレードライセンスを使用して、このタスクのステップ 5 までのみを実行します。ISE-PIC ノードをセカンダリノードとして追加すると、既存の ISE 展開内のすべてのデータが保持され、新しく結合（アップグレード）された ISE-PIC ノードに同期されますが、元の ISE-PIC ノードデータは保持されません。このライセンスについては、シスコの担当者にお問い合わせください。
- ISE 展開のプライマリノードまたはスタンドアロンノードとして特定の ISE-PIC ノードをアップグレードします。既存のすべてのデータを保持したまま ISE-PIC ノードをアップグレードします。Cisco ISE-PIC のアップグレードライセンスと Cisco ISE の Base ライセンスについては、シスコの担当者にお問い合わせください。

ライセンスモデルの詳細については、次を参照してください。 Cisco ISE-PIC ライセンス

**ステップ 1** セカンダリノードがインストールされている場合は、Cisco ISE-PIC のプライマリノードのインストールから、**[管理（Administration）] > [展開（Deployment）]**を選択し、セカンダリノードの登録を解除します。次に、両方のノードがプライマリノードになり、いずれかをアップグレードできます。

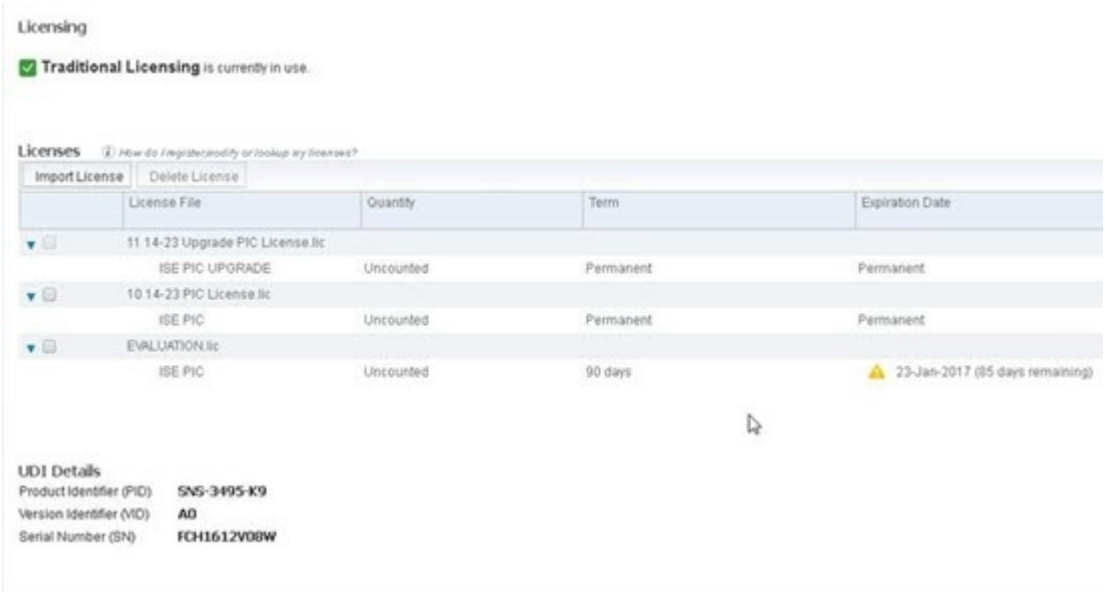
**ステップ 2** **[管理（Administration）] > [ライセンス（Licensing）]** を選択します。

**ステップ 3** [ライセンスのインポート（Import License）] をクリックします。

**ステップ 4** [ファイルの選択（Choose File）] をクリックし、アップグレード ライセンス ファイルを参照して、[OK] をクリックします。

**ステップ 5**　（注）　この ISE-PIC ノードを既存の ISE 展開に追加する場合は、この手順を完了するとアップグレードが完了し、その展開のプライマリノードからノードを登録できるようになります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

[新しいライセンスファイルのインポート（Import New License File）] 画面で、[インポート（Import）] をクリックします。
[ライセンス（License）] テーブルが更新され、アップグレードライセンスが表示されます。




**ステップ 6**　このアップグレードされたノードを完全な ISE 展開のプライマリノードにするには、この時点で Base ライセンスをインポートします。[ライセンスのインポート（Import License）] をもう一度クリックします。

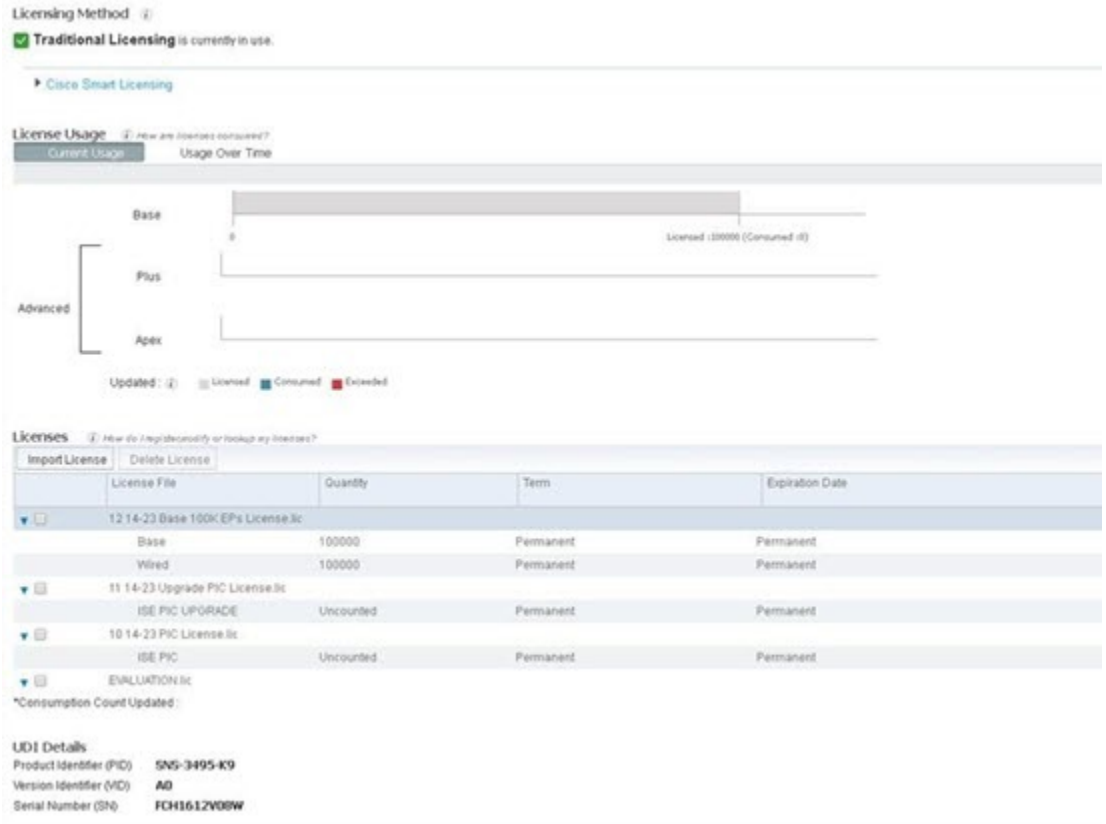
**ステップ 7**　[ファイルの選択（Choose File）] をクリックし、シスコの担当者から受け取った完全な ISE の Base ライセンスを参照して、[OK] をクリックします。

**ステップ 8**　[新しいライセンスファイルのインポート（Import New License File）] 画面で、[インポート（Import）] をクリックします。

**ステップ 9**　**[OK]** をクリックします。
ISE のプライマリノードにするアップグレードが開始され、「このノードはバックグラウンドで ISE にアップグレード中です。数分待ってから、*ISE* にログインしてください（*This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.*）」というメッセージが表示されます。

**ステップ 10**　**[OK]** をクリックします。

[ライセンス（License）] テーブルが更新され、Base ライセンスが表示されます。




数分後にログイン画面が表示されます。再度ログインし、完全な ISE の Base ライセンスのインストールで提供されるすべてのメニューにアクセスします。

アップグレードしたプライマリ ISE-PIC ノードが完全な ISE インストールのプライマリノードになり、以前のセカンダリノードがプライマリであり、ISE-PIC のスタンドアロンインストールの唯一のノードになります。これで、同じ方法で最後の ISE-PIC ノードを個別にアップグレードできるようになりました。

# での設定の管理 ISE-PIC

## ロールベース アクセス コントロール

Cisco ISE-PIC では、管理者に対して特定のシステム動作の権限を許可または拒否するロールベースアクセスコントロール（RBAC）ポリシーを定義することができます。これらの RBAC ポリシーは、個々の管理者の ID、または管理者が属する管理者グループの ID に基づいて定義されます。

さらにセキュリティを強化し、管理者ポータルにアクセスできる者を制御するために、次を実行します。

- リモート クライアントの IP アドレスに基づいて管理アクセスを設定します。
- 管理アカウントの強力なパスワード ポリシーを定義します。
- 管理 GUI セッションのセッション タイムアウトを設定します。

# Cisco ISE-PIC 管理者

管理者は、次の目的で管理者ポータルを使用できます。

- 展開ノードのモニタリングとトラブルシューティングの管理。
- Cisco ISE-PIC のサービス管理者アカウント、およびシステム設定と操作の管理。
- 管理者パスワードおよびユーザ パスワードを変更します。

CLI 管理者は、Cisco ISE アプリケーションの起動と停止、ソフトウェアのパッチとアップグレードの適用、Cisco ISE アプライアンスのリロードとシャットダウン、およびすべてのシステム ログとアプリケーション ログの表示を実行できます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE 展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

セットアップ時に設定したユーザ名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理ユーザ（CLI 管理者）と見なされます。デフォルトでは、CLI 管理ユーザのユーザ名は admin、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザはデフォルトの admin ユーザであり、このユーザアカウントは削除できません。ただし、このアカウントのパスワードを有効化、無効化、または変更するオプションなど、他の管理者によって編集できます。

管理者を作成するか、または既存のユーザを管理者ロールに昇格できます。管理者は、対応する管理者権限を無効にすることで、単純なネットワーク ユーザ ステータスに降格することもできます。

管理者は、Cisco ISE-PIC システムを設定および操作するローカル権限を持つユーザです。

管理者は、1 つ以上の管理者グループに割り当てられます。利便性のため、これらの管理者グループはシステムで事前に定義されています。これについては、次の項で説明します。

**関連トピック**

Cisco ISE-PIC 管理者グループ （33 ページ）

## Cisco ISE-PIC 管理者グループ

管理者グループは、Cisco ISE-PIC のロールベース アクセス コントロール（RBAC）グループです。同じグループに属するすべての管理者は、共通の ID を共有し、同じ権限を持ちます。特定の管理者グループのメンバーとしての管理者の ID は、許可ポリシーの条件として使用できます。管理者は、複数の管理者グループに属することができます。

どのアクセスレベルの管理者アカウントでも、管理者がアクセスできるすべてのウィンドウの、権限を持つオブジェクトを変更または削除できます。

次の表に、Cisco ISE-PIC で事前定義された管理者グループ、およびこれらのグループのメンバーが実行できるタスクを示します。これらの事前定義グループは、システムで管理者ユーザを定義するにのみ使用できます。

表 *2 : Cisco ISE* 管理者グループ、アクセス レベル、権限、および制約事項

| 管理者グループロール | アクセス レベル | 権限 | 制約事項 |
|---|---|---|---|
| スーパー管理者 | すべての Cisco ISE-PIC 管理機能。デフォルトの管理者アカウントは、このグループに属します。 | すべての Cisco ISE-PIC リソースに対する作成、読み取り、更新、削除、および実行（CRUDX）権限。 | |
| 外部 RESTful サービス（ERS）管理者 | GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス | • ERS API 要求の作成、読み取り、更新、および削除 | ロールは、内部ユーザ、ID グループ、およびエンドポイントをサポートする ERS 許可のみを対象としています |

## CLI 管理者と Web ベースの管理者の権限の比較

CLI 管理者は Cisco ISE-PIC アプリケーションの開始と停止、ソフトウェアパッチとアップグレードの適用、Cisco ISE-PIC アプライアンスのリロードとシャットダウン、およびすべてのシステムログとアプリケーションログの表示を行うことができます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE-PIC の展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

## 新しい管理者の作成

Cisco ISE-PIC 管理者は、特定の管理タスクを実行するために、特定のロールが割り当てられたアカウントが必要です。管理者アカウントを作成して、管理者が実行する必要がある管理タスクに基づいて 1 つ以上のロールを割り当てることができます。

[管理者ユーザ（Admin Users）] ウィンドウを使用して、Cisco ISE-PIC 管理者の属性の表示、作成、変更、削除、ステータスの変更、複製、または検索を実行できます。

（注） 管理者ユーザのドメインが CLI と GUI の両方で同じである場合は、CLI で Active Directory アクセスを設定してから GUI に参加することをお勧めします。それ以外の場合は、そのドメインへの認証の失敗を回避するために、GUI からドメインに再参加する必要があります。

**ステップ 1** **[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者ユーザ（Admin Users）] > [追加（Add）] > [管理者ユーザの作成（Create an Admin User）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は次のとおりです：# $ ’ ( ) * + -。/ @ _。

**ステップ 3** [送信（Submit）] をクリックして、新しい管理者を Cisco ISE-PIC 内部データベースに作成します。

**関連トピック**

読み取り専用管理ポリシー
内部読み取り専用管理者の作成
読み取り専用管理者のメニュー アクセスのカスタマイズ
外部グループを読み取り専用管理者グループにマッピング

# Cisco ISE-PIC への管理アクセス

Cisco ISE-PIC 管理者は、自分が属する管理者グループに基づいてさまざまな管理タスクを実行できます。これらの管理タスクは重要です。ネットワーク内の Cisco ISE-PIC の管理が許可されているユーザにのみ、管理アクセス権を付与します。

Cisco ISE-PIC では、次のオプションによって Web インターフェイスへの管理アクセスを制御することができます。

（注） Cisco ISE サーバがネットワークに追加された場合、その Web インターフェイスが起動すると実行状態になるようにマークされます。ただし、ポスチャサービスなどの一部のアドバンスドサービスが使用可能になるまでに時間がかかる場合があるため、すべてのサービスが完全に動作するまでに時間がかかることがあります。

### 管理アクセスの方法

Cisco ISE サーバには、いくつかの方法で接続することができます。管理者ポータルは PAN によって運用されます。ログインには管理者パスワードが必要です。CLI を実行できる SSH またはコンソールを使用すると、他の ISE ペルソナサーバにアクセスできます。ここでは、各接続タイプで利用可能なプロセスとパスワードのオプションについて説明します。

- [管理者パスワード（Admin password）]：インストール時に作成した Cisco ISE 管理者ユーザのタイムアウトは、デフォルトで 45 日間です。**[管理（Administration）] > [システム（System）] > [管理者設定（Admin Settings）]** でパスワードの有効期間をオフにすると、これを回避することができます。[パスワードポリシー（Password Policy）] タブをクリックし、[パスワードの有効期間（Password Lifetime）] で [管理パスワードの有効期限（Administrative passwords expire）] をオフにします。

この操作を行わないと、パスワードの有効期限が切れます。管理者パスワードは CLI で **application reset-passwd** コマンドを実行してリセットできます。CLI にアクセスするコンソールに接続するか、またはブートオプションメニューにアクセスする ISE イメージファイルを再起動することにより、管理者パスワードをリセットできます。

- [CLI パスワード（CLI password）]：CLI パスワードはインストール時に指定する必要があります。無効なパスワードが原因で CLI へのログインに問題がある場合は、CLI パスワードをリセットできます。コンソールに接続し、**password** CLI コマンドを実行して、パスワードをリセットします。詳細については、「*ISE CLI* リファレンス」を参照してください。
-

# 管理者アクセスの設定

Cisco ISE-PIC では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE-PIC の [管理者アカウントの設定（Administrator Account Settings）] で定義するパスワード ポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE-PIC では、管理者パスワードに UTF-8 文字は使用できません。

## 同時管理セッションとログイン バナーの最大数の設定

同時管理 GUI または CLI（SSH）セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログイン バナーは無効になっています。

**ステップ 1** **[管理（Administration）]** > **[管理者アクセス（Admin Access）]** > **[アクセス設定（Access Settings）]** > **[セッション（Session）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。

**ステップ 3** Cisco ISE-PIC で管理者がログインする前にメッセージを表示する場合は、[プリログインバナー（Pre-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

**ステップ 4** Cisco ISE-PIC で管理者がログインした後にメッセージを表示する場合は、[ポストログインバナー（Post-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

**ステップ 5** [保存（Save）] をクリックします。

## IP アドレスの選択からの Cisco ISE-PIC への管理アクセスの許可

Cisco ISE-PIC では、管理者が Cisco ISE-PIC 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

**ステップ 1** **[管理（Administration）] > [管理者アクセス（Admin Access）] > [アクセス設定（Access Settings）] > [IP アクセス（IP Access）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** [リストにある IP アドレスだけに接続を許可（Allow only listed IP addresses to connect）] を選択します。

（注） 管理アクセスにはポート 161（SNMP）の接続を使用します。ただし、IP アクセス制限が設定されている場合は、実行元のノードで管理アクセスが設定されていないと snmpwalk が失敗します。

**ステップ 3** [アクセス制限の IP リストの設定（Configure IP List for Access Restriction）] 領域で、[追加（Add）] をクリックします。

**ステップ 4** [IP アドレス（IP Address）] フィールドに IP アドレスをクラスレス ドメイン間ルーティング（CIDR）形式で入力します。

（注） この IP アドレスの範囲は IPv4 から IPv6 です。ISE ノードに複数の IPv6 アドレスを設定できるようになりました。

**ステップ 5** [CIDR 形式のネットマスク（Netmask in CIDR format）] フィールドにサブネット マスクを入力します。

**ステップ 6** [OK] をクリックします。このプロセスを繰り返して、他の IP アドレス範囲をこのリストに追加します。

**ステップ 7** [保存（Save）] をクリックして、変更内容を保存します。

**ステップ 8** [IPアクセス（IP Access）] ページを更新するには、[リセット（Reset）] をクリックします。

## 管理者アカウントのパスワード ポリシーの設定

Cisco ISE-PIC では、セキュリティ向上のために管理者アカウントにパスワード ポリシーを作成することもできます。ここで定義したパスワード ポリシーは、Cisco ISE-PIC のすべての管理者アカウントに適用されます。

（注）

- 内部管理者ユーザの電子メール通知は root@host に送信されます。電子メール アドレスは設定できません。多くの SMTP サーバがこの電子メールを拒否します。

  未解決の不具合 CSCui5583 を確認できます。これは、電子メール アドレスの変更を許可する拡張機能です。

- Cisco ISE-PIC では、管理者パスワードに UTF-8 文字は使用できません。

**ステップ 1** **[管理（Administration）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** [パスワード ポリシー（Password Policy）] タブをクリックし、値を入力します。

**ステップ 3** [保存（Save）] をクリックして、管理者パスワード ポリシーを保存します。

（注） 外部IDストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワード ポリシーにこの設定値が設定されている場合でも、外部 ID ストアが依然として管理者のユーザ名とパスワードを認証することに留意してください。

## 管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE-PIC では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

**ステップ 1** [管理（Administration）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [アカウント無効化ポリシー（Account Disable Policy）] の順に選択します。

**ステップ 2** [非アクティブになってから n 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。

このオプションでは、管理者アカウントが連続する日数非アクティブだった場合に管理者アカウントを無効にすることができます。

**ステップ 3** [保存（Save）] をクリックして、管理者のグローバル アカウント無効化ポリシーを設定します。

## 管理者のセッション タイムアウトの設定

Cisco ISE-PIC を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE-PIC は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE-PIC 管理者ポータルにアクセスするには再びログインする必要があります。

**ステップ 1** **[管理（Administration）] > [管理者アクセス（Admin Access）] > [セッションの設定（Session Settings）] > [セッションタイムアウト（Session Timeout）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** 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-PIC 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。

**ステップ 3** [保存（Save）] をクリックします。

## アクティブな管理セッションの終了

Cisco ISE-PIC では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

**ステップ 1** **[管理（Administration）] > [管理者アクセス（Admin Access）] > [セッションの設定（Session Settings）] > [セッション情報（Session Info）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** 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。

# 管理者ポータルで使用されるポート

管理者ポータルは HTTP ポート 80 および HTTPS ポート 443 を使用するように設定され、これらの設定は変更できません。Cisco ISE-PIC はまた、あらゆるエンドユーザ ポータルが同じポートを使用することを禁止して、管理者ポータルへのリスクを減らすようになっています。

# 通知をサポートするための SMTP サーバの設定

アラーム前に実行するアクションを受信したりできるようにするには、Simple Mail Transfer Protocol（SMTP）サーバを設定します。

電子メールを送信する ISE ノード

次のリストは、電子メールを送信する分散 ISE 環境のノードを示しています。

| 電子メールの目的 | 電子メールを送信するノード |
|---|---|
| ゲストの有効期限 | プライマリ PAN |
| アラーム | アクティブな MnT |
| ゲストとスポンサーのポータルからのスポンサーとゲストの通知 | PSN |
| パスワードの有効期限 | プライマリ PAN |

**ステップ 1** **[設定（Settings）] > [SMTP サーバ（SMTP Server）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** [SMTPサーバ（SMTP Server）] フィールドにアウトバウンド SMTP サーバのホスト名を入力します。この SMTP ホスト サーバは Cisco ISE-PIC サーバからアクセス可能である必要があります。このフィールドの最大長は 60 文字です。

**ステップ 3** [保存（Save）] をクリックします。

アラーム通知の受信者は、[電子メールにシステムアラームを含む（Include system alarms in emails）] オプションが有効になっている内部管理者ユーザです。アラーム通知を送信する送信者の電子メール アドレスは、ise@<hostname> としてハード コードされています。

# GUI からの外部 RESTful サービス API の有効化：ERS 設定

### 始める前に

Cisco ISE REST API 用に開発されたアプリケーションから Cisco ISE にアクセスできるようにするには、Cisco ISE REST API をイネーブルにする必要があります。Cisco REST API は HTTPS ポート 9060 を使用します。このポートはデフォルトでは閉じられています。Cisco ISE REST API が Cisco ISE 管理用サーバでイネーブルになっていない場合、クライアント アプリケーションは、サーバから Guest REST API 要求に対するタイムアウト エラーを受信します。

すべてのタイプの外部 RESTful サービス要求はプライマリ ISE ノードに限り有効です。セカンダリ ノードは読み取りアクセス（GET 要求）に対応します。

**ステップ 1** **[設定（Settings）]** > **[ERS 設定（ERS Settings）]**ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。

**ステップ 2** [読み取り/書き込み用に ERS を有効化（Enable ERS for Read/Write）] を選択し、[保存（Save）] をクリックします。

### 次のタスク

API コールと ISE-PIC の詳細については、『ISE API Reference Guide』を参照してください。