Cisco Secure Network Analytics

v7.4.2 ISE および ISE-PIC コンフィギュレーション ガイド

目次

はじめに **4**
概要 4
技術的な詳細 4
証明書の要件 4
設定のテスト 5
証明書の導入 **6**
オプション 1：ISE 内部認証局を使用した証明書の導入（推奨） 6
Secure Network Analytics pxGrid クライアント証明書の作成 6
集中管理インターフェイスでクライアント証明書の CSR を生成する 6
ISE の内部 CA を使用した証明書の CSR の作成 6
集中管理インターフェイスへのクライアント アイデンティティ証明書の追加 7
Secure Network Analytics 信頼ストアへの ISE サブ CA 証明書の追加 8
オプション 2 – 外部認証局（CA）サーバーを使用した証明書の導入 8
Secure Network Analytics pxGrid クライアント証明書の生成 8
Secure Network Analytics pxGrid クライアント証明書の CSR の生成 8
外部 CA を使用した Secure Network Analytics pxGrid クライアント証明書の作成 9
マネージャへの Secure Network Analytics pxGrid クライアント証明書の追加 9
マネージャ信頼ストアへの CA ルート証明書のインポート 9
ISE サーバー pxGrid 証明書の生成 10
ISE サーバー pxGrid 証明書の CSR の生成 10
外部 CA を使用した ISE サーバー pxGrid 証明書の作成 10
ISE 信頼ストアへの CA ルート証明書のインポート 11
証明書署名要求（CSR）への ISE 証明書のバインド 11
ISE 設定の追加 **12**
ISE の設定ページを開きます。 12
設定 12
統合オプション 13
その他のパラメータ 13
ノード ステータス インジケータ 13
更新アイコン 14
ISE または ISE-PIC での pxGrid の承認 14
ISE の設定ページを更新します。 14
ISE の設定ページを確認します。 14

保存した ISE クラスタの編集または削除 15
ISE の統合フェールオーバーの設定 16
拡張された ISE 環境に対応するための Secure Network Analytics 設定の調整 17
サポートへの問い合わせ 18
変更履歴 19

はじめに

概要

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch）と Cisco ISE（Identity Services Engine）を導入しているシスコのエンジニアとお客様を対象に Secure Network Analytics vv7.4.2 を ISE pxGrid に接続するために必要な設定ワークフローの変更点について説明します。

技術的な詳細

Secure Network Analytics と ISE を接続するには、2 つのシステム間で信頼性の高い通信を確立できるように、証明書を正しく導入する必要があります。証明書の導入では、さまざまな製品やアプリケーションのインターフェイス（Web アプリケーション、集中管理インターフェイス、ISE サーバー管理ポータル）を使用する必要があります。開始する前に導入の流れを確認し、要件と手順をしっかりと理解してください。

証明書の要件

Secure Network Analytics では、ISE pxGrid ノードを接続するためのクライアント証明書がインポートされます。クライアント アイデンティティ証明書については、次のガイドラインに従ってください。

- **集中管理インターフェイスで証明書署名要求（CSR）を生成**：集中管理インターフェイスで CSR を生成する場合、記載された要件で（*）が付けられた項目が CSR に含まれます（「**集中管理インターフェイスで CSR を生成**」の列を参照）。
- **集中管理インターフェイスで CSR を生成しない**：集中管理インターフェイス以外で CSR を生成する場合、生成した CSR がこの表に記載された要件を満たしていることを確認してください（「**集中管理インターフェイスで CSR を生成しない**」の列を参照）。
- **証明書要件の確認**：集中管理インターフェイスで CSR を生成するか、CSR 生成をスキップするかにかかわらず、証明書を Manager に追加する前に、この表の要件を満たしていることを確認してください。

要件	集中管理インターフェイスで CSR を生成	集中管理インターフェイスで CSR を生成しない
ファイル形式 *	PEM（.cer、.crt、.pem）または PKCS#12（.p12、.pfx、.pks）	PKCS#12（p12、.pfx、pks）
キー *	使用可能な RSA キー長： 2048 ビット（非推奨）、4096 ビット、または 8192 ビット ECDSA カーブ：使用不可	RSA キー長の要件： 2048 ビット（非推奨）以上 または ECDSA キーカーブの要件： NIST P-256、P-384、または P-521
署名者	クライアント アイデンティティ証明書は、自己署名するか、認証局（CA）の署名を受けることができます。	クライアント アイデンティティ証明書は、自己署名するか、認証局（CA）の署名を受けることができます。
認証（拡張キーの使用状況）*	CSR 要求クライアント（clientAuth）の認証。	クライアント アイデンティティ証明書には、クライアント（clientAuth）認証が必要です。
日付の範囲	証明書の日付が最新であり、期限が切れていないことを確認します。	証明書の日付が最新であり、期限が切れていないことを確認します。

** 集中管理インターフェイスで CSR を生成する場合、記載されている要件で（*）が付いている項目が CSR に含まれます。*

設定のテスト

証明書を導入したら、ISE のトラブルシューティングに関する TechNotes 記事（https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217511-troubleshoot-sna-ise-integration-conn.html）[英語] を参照して、ISE と Secure Network Analytics の統合が正しく設定されていることを確認してください。

証明書の導入

オプション 1：ISE 内部認証局を使用した証明書の導入（推奨）

証明書の導入には、ISE 内部認証局（CA）を使用する方法をお勧めします。この方法を実施するには、以下の手順を使用します。

Secure Network Analytics pxGrid クライアント証明書の作成

集中管理インターフェイスでクライアント証明書の CSR を生成する

> 集中管理インターフェイス以外で CSR を生成する場合は、このセクションをスキップして「**ISE の内部 CA を使用した証明書の CSR の作成**」に進みます。手順を開始する前に、CSR が「**証明書の要件**」に示されている要件を満たしていることを確認してください。

1. Manager（旧 Stealthwatch Management Console）にログインします。
2. メインメニューから [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
3. [インベントリ（Inventory page）] ページで、ISE に接続するマネージャの ••• （[省略記号（Ellipsis）]）アイコンes.ISEShortName″ /> をクリックします。
4. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
5. [アプライアンス（Appliance）] タブの [追加の SSL/TLS クライアント アイデンティティ（Additional SSL/TLS Client Identities）] セクションに移動します。
6. [新規追加（Add New）] をクリックします。
7. CSR（証明書署名要求）を生成する必要がある場合は、[はい（Yes）] を選択します。[次へ（Next）] をクリックします。
8. [RSA キー長（RSA Key Length）] を選択し、[CSR の生成（Generate a CSR）] セクションの残りのフィールドを入力します。
9. [Generate CSR] をクリックします。生成プロセスは数分かかることがあります。
10. [CSR のダウンロード（Download CSR）] をクリックし、CSR ファイルをコンピュータに保存します。

ISE の内部 CA を使用した証明書の CSR の作成

1. ISE 管理インターフェイスにログインします。
2. [管理（Administration）] > [pxGridサービス（pxGrid Services）] > [クライアント管理（Client Management）] > [証明書（Certificates）] の順に選択します。[pxGrid 証明書の生成（Generate pxGrid Certificates）] フォームが開きます。

> パスは ISE-PIC とは異なる場合があります。

3. [処理の選択（I want to）] フィールドで、[単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with certificate signing request)）] を選択します。
4. CSR をテキストエディタで開き、[証明書署名要求の詳細（Certificate Signing Request Details）] フィールドにファイルの内容をコピーします。
5. 必要に応じて、説明を入力します。

6. [証明書のダウンロード形式（Certificate Download Format）] フィールドで、[PKCS12形式（証明書チェーンを含む。証明書チェーンとキーの両方で1つのファイル）（PKCS12 format (including certficate chain; one file for both the certificate chain and key)）] を選択します。
7. [証明書パスワード（Certificate Password）] および [パスワードの確認（Confirm password）] フィールドにパスワードを入力します。このパスワードは、[追加のSSL/TLSクライアントID（Additional SSL/TLS Client Identities）] セクションで証明書を集中管理インターフェイスにアップロードするときに要求されます。
8. [作成（Create）] をクリックします。

> 証明書の生成に失敗した場合は、pxGrid_Certificate_Template のキー長が、Secure Network Analytics で作成した CSR のキー長と一致していることを確認してください。PxGrid_Certificate_Template のキー長を編集するには、[Certificate Template] フィールドの横にあるリンクをクリックします。

9. 集中管理インターフェイスで CSR を生成しなかった場合は、PKCS12 ファイルを再パッケージ化して秘密キーを含めます。

集中管理インターフェイスへのクライアント アイデンティティ証明書の追加

1. 上記の項で作成したファイルを解凍して PKCS12 ファイルにアクセスします。

> このファイルをダウンロードするため、ポップアップ メニューをブロック解除することが必要になる場合があります。

2. 集中管理インターフェイスで、マネージャ設定の [追加のSSL/TLSクライアントID（Additional SSL/TLS Client Identities）] セクションに移動します。
3. **集中管理インターフェイスで CSR を生成した場合、**[追加のSSL/TLSクライアントID（Additional SSL/TLS Client Identities）] セクションには、作成したクライアント証明書をインポートするためのフォームが表示されます。

   集中管理インターフェイスで CSR を生成しなかった場合は、[新規追加（Add New）] をクリックします。

   - 「CSRを生成する必要がありますか。（Do you need to generate a CSR?）」のメッセージに対して、[いいえ（No）] を選択します。
   - [次へ（Next）] をクリックします。

4. 証明書のフレンドリ名を指定し、[ファイルの選択（Choose File）] をクリックして証明書ファイルを探します。
5. 前のセクションで入力したパスワードを入力します。
6. [クライアント アイデンティティの追加（Add Client Identity）] をクリックしてシステムに証明書を追加します。
7. [設定を適用（Apply Settings）] をクリックして変更を保存します。

Secure Network Analytics 信頼ストアへの ISE サブ CA 証明書の追加

1. ISE 管理インターフェイスにログインします。
2. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] に移動して、[認証局証明書（Certificate Authority Certificates）] をクリックします。
3. **証明書サービスエンドポイントサブ CA** の証明書を見つけてコンピュータにエクスポートします。

> ISE のサブ CA 証明書が ISE pxGrid ノードで使用される証明書を発行した認証局のものではない場合は、この手順でその CA 証明書を取得する必要があります。

4. マネージャにログインします。
5. メインメニューから [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
6. [インベントリ（Inventory page）] ページで、マネージャの ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
7. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
8. [全般（General）] タブを選択します。
9. [信頼ストア（Trust Store）] セクションに移動し、エクスポート済みの ISE CA 証明書をインポートします。
10. [新規追加（Add New）] をクリックします。
11. 証明書のフレンドリ名を指定して [ファイルの選択（Choose File）] をクリックし、エクスポート済みの ISE CA 証明書を選択します。
12. [証明書の追加（Add Certificate）] をクリックして変更を保存します。

証明書が導入され、2 つのシステム（Secure Network Analytics および ISE）間で相互の信頼性が確立されます。「**ISE 設定の追加**」の章に進み、ISE pxGrid ノードへの接続を設定します。

オプション 2 – 外部認証局（CA）サーバーを使用した証明書の導入

Secure Network Analytics pxGrid クライアント証明書の生成

Secure Network Analytics pxGrid クライアント証明書の CSR の生成

1. マネージャにログインします。
2. メインメニューから [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
3. [インベントリ（Inventory page）] ページで、ISE に接続するマネージャの ••• （[省略記号（Ellipsis）]）アイコンes.ISEShortName″ /> をクリックします。
4. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
5. [アプライアンス（Appliance）] タブの [追加の SSL/TLS クライアント アイデンティティ（Additional SSL/TLS Client Identities）] セクションに移動します。
6. [新規追加（Add New）] をクリックします。

7. CSR(証明書署名要求)を生成する必要がある場合は、[はい(Yes)]を選択します。[次へ(Next)]をクリックします。
8. [RSA キー長(RSA Key Length)]を選択し、[CSR の生成(Generate a CSR)]セクションの残りのフィールドを入力します。
9. [Generate CSR]をクリックします。生成プロセスは数分かかることがあります。
10. [CSR のダウンロード(Download CSR)]をクリックし、CSR ファイルをローカルに保存します。

外部 CA を使用した Secure Network Analytics pxGrid クライアント証明書の作成

> この例では、MS Server 2012 の Microsoft Active Directory 証明書サービスを使用します。別の外部 CA も使用できます。

1. Microsoft Active Directory 証明書サービス(https://server/certsrv/)に移動します。ここで、server は MS サーバの IP または DNS です。
2. [証明書を要求する(Request a certificate)]をクリックします。
3. [高度な証明書要求(Advanced certificate request)]の送信を選択します。
4. 前のセクションで生成した CSR ファイルの内容を[保存された要求(Saved Request)]フィールドにコピーします。
5. [証明書テンプレート(Certificate Template)]で[pxGrid]を選択し、[送信(Submit)]をクリックします。
6. 生成された証明書を **Base-64** 形式でダウンロードし、**pxGrid_client.cer** として保存します。

マネージャへの Secure Network Analytics pxGrid クライアント証明書の追加

1. 集中管理インターフェイスで、マネージャ設定の[追加のSSL/TLSクライアントID(Additional SSL/TLS Client Identities)]セクションに移動します。
2. [追加の SSL/TLS クライアント アイデンティティ(Additional SSL/TLS Client Identities)]セクションには、作成したクライアント証明書をインポートするフォームが含まれています。
3. 証明書のフレンドリ名を指定し、[ファイルの選択(Choose File)]をクリックして証明書ファイルを探します。
4. 前のセクションで入力したパスワードを入力します。
5. [クライアント アイデンティティの追加(Add Client Identity)]をクリックしてシステムに証明書を追加します。
6. [設定を適用(Apply Settings)]をクリックして変更を保存します。

マネージャ信頼ストアへの CA ルート証明書のインポート

1. Microsoft Active Directory 証明書サービスのホームページにアクセスし、[CA 証明書、証明書チェーン、または CRL のダウンロード(Download a CA certificate, certificate chain, or CRL)]を選択します。
2. [Base-64] 形式を選択して[CA 証明書のダウンロード(Download CA certificate)]をクリックします。
3. 証明書を **CA_Root.cer** として保存します。
4. マネージャにログインします。

5. メインメニューから [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
6. [インベントリ(Inventory page)] ページで、マネージャの ••• ([省略記号(Ellipsis)]) アイコンをクリックします。
7. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
8. [全般(General)] タブを選択します。
9. [信頼ストア(Trust Store)] セクションに移動し、エクスポート済みの CA_Root.cer 証明書をインポートします。
10. [新規追加(Add New)] をクリックします。
11. 証明書のフレンドリ名を指定して [ファイルの選択(Choose File)] をクリックし、エクスポート済みの ISE CA 証明書を選択します。
12. [証明書の追加(Add Certificate)] をクリックして変更を保存します。

ISE サーバー pxGrid 証明書の生成

ISE サーバー pxGrid 証明書の CSR の生成

1. ISE 管理インターフェイスを開きます。
2. [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)] に移動します。
3. [証明書署名要求(CSR)の作成(Generate Certificate Signing Request (CSR))] を選択します。
4. [証明書の用途(Certificate(s) will be used for)] フィールドで [pxGrid] を選択します。
5. 証明書を生成する ISE ノードを選択します。
6. 必要に応じて、その他の証明書の詳細を入力します。
7. [生成(Generate)] をクリックします。
8. [エクスポート(Export)] をクリックして、ファイルをローカルに保存します。

外部 CA を使用した ISE サーバー pxGrid 証明書の作成

1. Microsoft Active Directory 証明書サービス(https://server/certsrv/)に移動します。ここで、server は MS サーバの IP または DNS です。
2. [証明書を要求する(Request a certificate)] をクリックします。
3. [高度な証明書要求(Advanced certificate request)] の送信を選択します。
4. 前のセクションで生成した CSR の内容を [保存された要求(Saved Request)] フィールドにコピーします。
5. [証明書テンプレート(Certificate Template)] で [pxGrid] を選択し、[送信(Submit)] をクリックします。
6. 生成された証明書を **Base-64** 形式でダウンロードし、**ISE_pxGrid.cer** として保存します。

ISE 信頼ストアへの CA ルート証明書のインポート

1. Microsoft Active Directory 証明書サービスのホームページにアクセスし、[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。
2. [Base-64] 形式を選択して [CA 証明書のダウンロード（Download CA certificate）] をクリックします。
3. 証明書を **CA_Root.cer** として保存します。
4. ISE 管理インターフェイスにログインします。
5. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼証明書（Trusted Certificates）] の順に選択します。
6. [インポート（Import）] > [証明書ファイル（Certificate file）] の順に選択し、ルート証明書をインポートします。
7. [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必ずオンにします。
8. [送信（Submit）] をクリックします。

証明書署名要求（CSR）への ISE 証明書のバインド

1. ISE 管理インターフェイスにログインします。
2. [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。
3. 前のセクションで生成した CSR を選択し、[証明書のバインド（Bind Certificate）] をクリックします。
4. [CA 署名付き証明書のバインド（Bind CA Signed Certificate）] フォームで、生成済みの **ISE_pxGrid.cer** 証明書を選択します。
5. 証明書のフレンドリ名を指定して [送信（Submit）] をクリックします。
6. 再起動を求められたら [はい（Yes）] をクリックします。
7. 証明書の交換を求められたら [はい（Yes）] をクリックします。
8. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] の順に選択します。
9. 外部 CA によって署名された作成済みの pxGrid 証明書がリストに表示されます。

証明書が導入され、2 つのシステム（Secure Network Analytics および ISE）間で相互の信頼性が確立されます。「**ISE 設定の追加**」の章に進み、ISE pxGrid ノードへの接続を設定します。

ISE 設定の追加

現在のドメインの ISE クラスタを設定するには、次の手順を実行します。

- クラスタが使用される Secure Network Analytics ドメインごとに、ISE クラスタを設定する必要があります。
- 複数の独立した ISE クラスタを Secure Network Analytics のドメインに追加できますが、同じドメイン内のクラスタ間で同じ IP アドレスは使用できません。
- マネージャと ISE がポート TCP/8910 および TCP/443 を介して通信できるように、ファイアウォールを設定する必要があります。

ISE の設定ページを開きます。

1. [設定(Configure)] > [Cisco ISEの統合(INTEGRATIONS Cisco ISE)] の順に選択します。
2. ページの右上隅で、[新しい設定の追加(Add New Configuration)] をクリックします。

設定

次の設定を定義します。

- **[クラスタ名(Cluster Name)]**:この名前は デスクトップ クライアント のエンタープライズツリーならびにマネージャ Web UI の ISE 構成の一覧に表示されます。
- [証明書(Certificate)]:これは、マネージャ設定インターフェイスの [追加のSSL/TLSクライアントID(Additional SSL/TLS Client Identities)] セクションにある [フレンドリ名(Friendly Name)] フィールドに入力した名前と同じです。この証明書により、アプライアンスは ID でクライアントを認証できます(つまりマネージャが ISE に提示するクライアント証明書です)。
- [PxGridノード1(PxGrid Node 1)]:アプライアンスが統合されている ISE クラスタ上のプライマリ pxGrid ノードの IP アドレス、ホスト名、または FQDN です。
- [PxGridノード2(PxGrid Node 2)](オプション):アプライアンスが統合されている ISE クラスタ上のセカンダリ pxGrid ノードの IP アドレス、ホスト名、または FQDN です。このノードは、フェールオーバーのために使用されます。最初のノードへの接続が失敗すると、セカンダリノードが使用されます。
- [PxGridノード3(PxGrid Node 3)](オプション):アプライアンスが統合されている ISE クラスタ上のターシャリ pxGrid ノードの IP アドレス、ホスト名、または FQDN です。このノードは、フェールオーバーのために使用されます。最初のノードとセカンダリノードへの接続が失敗すると、ターシャリノードが使用されます。
- [クライアント名(Client Name)]:この一意の名前は、ISE アプライアンスの ISE クラスタで pxGrid クライアントリストに表示されます。
- [厳密なISEサーバーID検証の有効化(Enable Strict ISE Server Identity Verification)]:Manager が ISE クラスタノードと通信するときにサーバー ID 検証を要求するには、この設定を有効にします。他のセキュリティチェックに加えて、ISE ノード ID 証明書が次のいずれかを満たす場合は、通信が許可されます。
  - これには、証明書の共通名やサブジェクト代替名としてリストされているノード名または ID 情報(FQDN など)が含まれます。
  - Manager の信頼ストア内の証明書と一致します。

- ISE 統合が設定されている v7.4 より前のリリースからアップグレードする場合、[厳密なISEサーバーID検証の有効化(Enable Strict ISE Server Identity Verification)]オプションはデフォルトでオフになっています。このオプションは、v7.4 以降の ISE 統合の設定ではデフォルトでオンになっています。
- 選択した統合オプションを正常に連携および機能させるには、マネージャが ISE サーバー(PAN、Mnt、SXP、pxGrid などの分散環境の場合はすべてのノード)の FQDN(完全修飾ドメイン名)を解決できるように、マネージャの DNS 設定を行います。これらのノードによって提供されるサービスは動的に検出され、ノードの FQDN を使用して参照されます。

統合オプション

統合向けの ISE 製品を選択します。

- [ISE]:すべての統合オプションを有効にできます。
- [Cisco ISE-PIC]:セッション更新のみを有効にできます。

ISE クラスタで有効にする統合オプションを選択します。

- [適応型ネットワーク制御(Adaptive Network Control)]:ISE のエンドポイントに分類(ANC ポリシー)を適用し、ISE に設定されている認証ポリシーに従ってネットワークアクセスを変更できます。
- [静的TrustSec分類(Static TrustSec Classifications)]:認証プロセス以外でエンドポイント IP と静的に関連付けられた TrustSec セキュリティグループタグ(SGT)に関する情報を受信できます。これは、ISE、アクセスレイヤデバイスに手動で設定されたか、または SXP プロセス内で他のシステムから学習した IP-to-SGT バインディングの可能性があります。このデータは、元のフローにエンドポイント IP アドレスが一致する SGT が存在せず、SGT が割り当てられたエンドポイント IP アドレスにセッションが関連付けられていないフローの拡大に使用されます。
- [セッション(Sessions)]:ユーザー名、エンドポイントの MAC アドレス、デバイスプロファイル、および TrustSec セキュリティグループに関する情報を含む、ユーザーセッションの最新情報を受信できます。この情報は、TrustSec セキュリティグループ情報を含むフローを拡大し、マネージャレポートでユーザーとセッションを監視するために使用されます。[マシン認証から導出されたセッションの追跡(Track sessions derived from machine authentications)]を有効にして、ユーザセッションの最新情報と一緒にマシンセッションの最新情報も受信します。

その他のパラメータ

ノード ステータス インジケータ

各 IP アドレスフィールドの横に配置されたノード ステータス インジケータは、追加された各ノードの接続ステータスを示します。これらは、最初のノードの設定と保存後に表示されます。

- ●([緑色ステータス(Green Status)])アイコン は、ノードへの接続が確立されていること、およびシステムが pxGrid に関する必要なすべての情報トピックをサブスクライブしていることを示しています。
- ●([黄色ステータス(Yellow Status)])アイコンは、ノードとの接続が保留中で、ISE の [pxGrid サービス(pxGrid Services)] ページでクライアントが承認されるまで接続が進行中または待機中であることを示しています。

- 🔴([赤色ステータス(Red Status)])アイコン は、ノードへの接続が確立されていないか、pxGrid に関する必要な情報トピックのサブスクライブに失敗したことを示しています。このアイコンをクリックすると、接続が存在しない理由、または失敗したサブスクリプションを示すエラーメッセージを確認できます。

更新アイコン

🔄([更新(Refresh)])アイコンをクリックして、関連付けられたクラスタへの接続を更新します。

ISE または ISE-PIC での pxGrid の承認

1. 次のいずれかを実行します。
    a. ISE を使用している場合は、このアプライアンスにログインし、メインメニューで [管理(Administration)] をクリックします。開いたページで、[pxGrid サービス(pxGrid Services)] タブをクリックします。
    b. ISE-PIC を使用している場合は、このアプライアンスにログインし、メインメニューで [サブスクライバ(Subscribers)] をクリックします。開いたページで、[クライアント(Clients)] タブをクリックします。
2. 表示されたテーブルの [クライアント名(Client Name)] 列で、該当するサブスクライバの名前の横にあるチェックボックスをオンにし、テーブルの上部にあるサブメニューで [承認(Approve)] をクリックします。

ISE の設定ページを更新します。

1. Web アプリケーションで ISE の設定ページに戻り、ページを更新します。
2. 該当する IP アドレスフィールドの横にあるノード ステータス インジケータが、ISE クラスタまたは ISE-PIC クラスタへの接続が確立されていることを示す緑色であることを確認します。

ISE の設定ページを確認します。

ISE のトラブルシューティングに関する TechNotes 記事 (https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217511-troubleshoot-sna-ise-integration-conn.html)[英語] を参照して、ISE と Secure Network Analytics の統合が正しく設定されていることを確認してください。

保存した ISE クラスタの編集または削除

[アクション（Actions）] 列で、省略記号をクリックしてサブメニューを開き、適切なオプションを選択します。

- Secure Network Analytics にまだ存在する ISE クラスタから最後に残ったノードを削除することはできません。
- ライセンス許可されていない機能アラームがISE クラスタでアクティブになっている場合、すべての ISE クラスタを削除できます。それを行ってから数分以内にアラームが非アクティブになります。
- ISE クラスタを削除しても、履歴を示すためにクライアントユーザー名は ISE から削除されません。ユーザー名は引き続き pxGrid ユーザー名リストの ISE ボックスに表示されます。

ISE の統合フェールオーバーの設定

ISE の統合フェールオーバーにより、プライマリおよびセカンダリ マネージャを設定して、ISE セッションの更新情報を受け取ることができます。これにより、プライマリ マネージャで不具合が発生し、セカンダリ マネージャがプライマリロールに切り替わっても、ユーザーに関する情報が引き続きマネージャ レポートに表示されます。

ISE の統合フェールオーバー設定では、次のことを行う必要があります。

- プライマリ マネージャとセカンダリ マネージャの両方で ISE 統合を設定します。
- プライマリ マネージャとセカンダリ マネージャに対して、異なる ISE クライアント証明書を生成します。
- プライマリ マネージャとセカンダリ マネージャの ISE 設定で異なるクライアント名を指定します。

> マネージャのフェールオーバー関係をすでに定義している場合、ISE の統合設定を変更するには、セカンダリ マネージャをプライマリ マネージャに切り替える必要が生じる場合があります。

ISE の統合フェールオーバーを設定するには、次の手順を実行します。

1. 「**ISE 設定の追加**」の手順に従って、プライマリ マネージャを設定します。必ず一意の ISE クライアント証明書を生成し、一意のクライアント名を割り当ててください。
2. セカンダリ マネージャについても、これらの手順を繰り返します。このとき、一意の ISE クライアント証明書を生成し、一意のクライアント名を指定します。

   pxGrid ノードと ISE の統合オプションが、プライマリ マネージャのオプションと一致していることを確認してください。

拡張された ISE 環境に対応するための Secure Network Analytics 設定の調整

デフォルトでは、Secure Network Analytics フローコレクタが処理できる同時アクティブセッション数は、アプライアンスで使用可能なメモリの合計容量によって決まります。

次の仕様を参照してください。

合計 RAM	セッションの総数
16 G ～ 128 G	524,288
128 G 以上	2,097,152

フローコレクタがデフォルトでサポートする数を超える ISE セッションを処理できるようにするには、アプライアンスに追加の設定が必要です。ホスト、ユーザ、セッション、デバイスなどの重要なオブジェクトに関する情報を保持するメモリ内データ構造のサイズを設定することになります。

アプライアンスの設定を調整する場合は、シスコサポートにお問い合わせください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 3 日	最初のバージョン。

著作権情報