pxGrid

pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッション ディレクトリからの状況依存情報を、ISE エコ システムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。また、pxGrid フレームワークは、Cisco ISE とサード パーティのベンダー間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用でき、その他の情報交換にも使用できます。また、pxGrid では、サードパーティ システムが適応型ネットワーク制御アクション（EPS）を起動して、ネットワーク イベントまたはセキュリティ イベントに応答してユーザ/デバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイント プロファイルは、エンドポイント プロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング（IP-SGT マッピング）を発行および受信登録できます。SXP バインディングの詳細については、セキュリティ グループ タグの交換プロトコルを参照してください。

ハイ アベイラビリティ設定で、Cisco pxGrid サーバは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバの PAN をアクティブにするには、手動で昇格する必要があります。[pxGrid サービス（pxGrid Services）] ページ（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）を調べ、pxGrid ノードが現在アクティブであるか、スタンバイ状態であるかを確認できます。

XMPP（Extensible Messaging and Presence Protocol）クライアントの場合、pxGrid ノードはアクティブ/スタンバイの高可用性モードで動作します。つまり、pxGrid サービスはアクティブ ノード上では「実行中」状態で、スタンバイ ノードでは「無効」状態です。

セカンダリ pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ pxGrid ノードがネットワークに戻された場合、元のプライマリ pxGrid ノードは引き続きセカンダリ

ロールを持ち、現在のプライマリ ノードがダウンしない限り、プライマリ ロールに昇格されません。

（注） 時々、元のプライマリ pxGrid ノードがプライマリ ロールに自動的に昇格されることがあります。

ハイ アベイラビリティ展開では、プライマリ pxGrid ノードがダウンすると、セカンダリ pxGrid ノードに切り替えるのに約 3 ～ 5 分かかることがあります。プライマリ pxGrid ノードに障害が発生した場合は、キャッシュ データを消去する前に、クライアントはスイッチオーバーが完了するまで待機することを推奨します。

pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更通知。
- pxgrid-cm.log：パブリッシャ/サブスクライバおよびクライアントとサーバ間のデータ交換アクティビティの更新。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログ。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関する情報。

（注） ノードで pxGrid サービスが無効になっている場合、ポート 5222 はダウンしますが、（Web クライアントで使用される）ポート 8910 は機能し、引き続き要求に応答します。

（注） Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、 のアップグレード ライセンスを最近インストールしている場合には、Base インストールで特定の拡張 pxGrid サービスが使用可能である可能性があります。

（注） パッシブ ID ワーク センターを使用するには pxGrid を定義する必要があります。詳細については、PassiveID ワークセンターを参照してください。

pxGrid クライアントおよび機能の管理

Cisco ISE に接続するクライアントは、pxGrid サービスを使用する前に、アカウントを登録し、承認を受ける必要があります。pxGrid クライアントは、クライアントになるために pxGrid SDK を介してシスコから利用可能な 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 pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された pxGrid サーバのホスト名または IP アドレスに接続できます。

pxGrid の「機能」は、クライアントの 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、SGA などの機能のみがサポートされます。クライアントが新しい機能を作成すると、その機能は **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]** に表示されます。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャから入手してください。

（注） pxGrid セッション グループが EPS グループの一部であるため、EPS ユーザ グループに割り当てられたユーザはセッション グループで操作を実行できます。ユーザが EPS グループに割り当てられると、ユーザは pxGrid クライアントのセッションのグループに加入できます。

関連トピック

pxGrid 証明書の生成

pxGrid クライアントの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。**[管理（Administration）] > [展開（Deployment）]** を選択し、必要なノードにチェックマークを付け、[編集（Edit）] をクリックします。設定画面で [パッシブ ID サービスを有効にする（Enable Passive Identity Service）] をオンにします。

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。

ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

pxGrid 機能の有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。

• pxGrid クライアントをイネーブルにします。

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。
ステップ 2 右上の [機能別に表示（View by Capabilities）] をクリックします。
ステップ 3 有効にする機能を選択し、[有効（Enable）] をクリックします。
ステップ 4 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ISE pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。
- Cisco pxGrid サービスは、Cisco ISE SNS 3415/3495 アプライアンス上または VMware で実行されます。
- すべてのノードは、pxGrid 用に CA 証明書を使用するように設定されています。アップグレード前にデフォルトの証明書を pxGrid に使用する場合、アップグレード後にこの証明書は内部 CA 証明書に置き換えられます。
- 分散展開を使用しているか、または Cisco ISE 1.2 からアップグレードする場合は、証明書で [pxGrid 使用（pxGrid Usage）] オプションを有効にする必要があります。[pxGrid 使用（pxGrid Usage）] オプションを有効にするには、**[管理（Administration）] > [証明書（Certificates）] > [システム証明書（Certificates）]** に移動します。展開に使用される証明書を選択し、[編集（Edit）] をクリックします。pxGrid を確認します。[pxGrid コントローラ（pxGrid Controller）] チェックボックスの証明書を使用します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。
ステップ 2 [展開ノード（Deployment Nodes）] ページで、pxGrid サービスを有効にするノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブをクリックし、[pxGrid] チェックボックスをオンにします。
ステップ 4 [保存（Save）] をクリックします。

以前のバージョンからアップグレードするとき、[保存（Save）] オプションが無効になる場合があります。このことは、ブラウザ キャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存（Save）] オプションを有効にするには、ブラウザ キャッシュを消去します。

pxGrid の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認（Automatically Approve New Accounts）：このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可（Allow Password Based Account Creation）：このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存（Save）] をクリックします。

[pxGrid の設定（pxGrid Settings ）] ページで [テスト（Test）] オプションを使用して、pxGrid ノードでヘルス チェックを実行します。pxgrid/pxgrid-test.log ファイルで詳細を確認できます。

pxGrid 証明書の生成

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- PxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] の順に選択します。

ステップ 2 [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム（CN）を入力する必要があります。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。

- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- ルート証明書チェーンのダウンロード（Download root certificate chain）：ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

[証明書テンプレート（Certificate Templates）] リンクから証明書テンプレートをダウンロードし、必要に応じて、テンプレートを編集できます。

ステップ 3 （[単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] オプションを選択した場合は必須）pxGrid クライアントの FQDN を入力します。

ステップ 4 （オプション）この証明書の説明を入力できます。

ステップ 5 サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- IP アドレス（IP address）：この証明書に関連付ける pxGrid クライアントの IP アドレスを入力します。
- FQDN：pxGrid の完全修飾ドメイン名を入力します。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンド エンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

作成した証明書は、ISE の **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** に表示され、ブラウザのダウンロード ディレクトリにダウンロードされます。

pxGrid クライアントの権限の制御

pxGrid クライアントの権限を制御するために、pxGrid 許可ルールを作成できます。これらのルールを使用して、pxGrid クライアントに提供されるサービスを制御します。

さまざまな種類のグループを作成し、pxGrid クライアントに提供されるサービスをこれらのグループにマッピングできます。[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して、新しいグループを追加します。[権限（Permissions）] ウィンドウで、事前定義されたグループ（EPS や ANC など）を使用する事前定義された許可ルールを表示できます。事前定義されたルールでは [操作（Operations）] フィールドだけを更新できることに注意してください。

pxGrid クライアントの許可ルールを作成するには、以下の手順を実行します。

ステップ 1 [管理（Administration）] タブから、[pxGridサービス（pxGrid Services）] > [権限（Permissions）] を選択します。

ステップ 2 [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

ステップ 3 [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **<ANY>**
- **パブリッシュ**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

（注） このオプションを選択すると、カスタム操作を指定できます。

ステップ 4 [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

（EPS や ANC などの）事前定義されたグループ、および（[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して）手動で追加されたグループが、このドロップダウン リストに表示されます。

Cisco pxGrid ライブ ログ

[ライブ ログ（Live Logs）] ページには、すべての pxGrid 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベント タイプとタイムスタンプが含まれています。

[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブ ログ（Live Log）] の順に移動して、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。