Cisco pxGrid

Cisco pxGridノード

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

Cisco pxGrid 経由で SXP バインディング（IP-SGT マッピング）を公開および登録できます。SXP バインディングの詳細については、e を参照してください。

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

pxGridペルソナがあるアクティブなシスコノードでは、これらのプロセスは[実行中（Running）] と表示されます。スタンバイの Cisco pxGrid ノードでは、[スタンバイ（Standby）] と表示されます。アクティブな pxGrid ノードがダウンすると、スタンバイ pxGrid ノードがこれを検出し、4つのpxGridプロセスを開始します。これらのプロセスは、数分以内に[実行中（Running）] と表示され、スタンバイノードがアクティブノードになります。CLI コマンド **show logging application pxgrid/pxgrid.state** を実行すると、Cisco pxGrid がそのノードでスタンバイ状態であるかどうかを確認できます。

Extensible Messaging and Presence Protocol クライアントの場合、Cisco pxGrid ノードはアクティブ/スタンバイのハイアベイラビリティモードで動作します。つまり、Cisco pxGrid サービスはアクティブノード上では「**実行中**」状態で、スタンバイノードでは「**無効**」状態です。

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

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

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

セカンダリ Cisco pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ Cisco pxGrid ノードがネットワークに戻された場合、元のプライマリ Cisco pxGrid ノードは引き続きセカンダリロールを持ち、現在のプライマリノードがダウンしない限り、プライマリロールに昇格されません。

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

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

Cisco pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更を通知します。
- pxgrid-cm.log：パブリッシャまたはサブスクライバ、あるいはその両方、およびクライアントとサーバー間でのデータ交換アクティビティの更新について表示します。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログを表示します。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関するすべての情報を表示します。

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

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

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

Cisco pxGrid クライアントと機能の管理

Cisco ISE に接続するクライアントは、Cisco pxGrid サービスを使用する前に、アカウントを登録し、承認を受ける必要があります。Cisco pxGrid クライアントは、クライアントになるために Cisco pxGrid SDK で使用可能な Cisco pxGrid クライアントライブラリを使用します。Cisco ISE は、自動および手動承認の両方をサポートします。クライアントは、一意の名前と証明書ベースの相互認証を使用して Cisco pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された Cisco pxGrid サーバーのホスト名または IP アドレスに接続できます。

Cisco pxGrid の機能は、クライアントの Cisco pxGrid 上の情報トピックまたはチャネルであり、これらは公開および登録されます。Cisco ISE では、ID、適応型ネットワーク制御（ANC）、セキュリティ グループ アクセス（SGA） などの機能のみがサポートされています。クライアントが新しい機能を作成すると、[機能別に表示（View by Capabilities）] ウィンドウに表示されます。このウィンドウへのナビゲーションパスは、次のとおりです。**[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]**。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャから入手してください。

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

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

関連トピック

Cisco pxGrid 証明書の生成

pxGrid サービスの有効化

始める前に

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

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。
ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。
ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。
ステップ 4 有効にする機能を選択し、[有効（Enable）] をクリックします。
ステップ 5 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

pxGrid 機能の有効化

始める前に

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

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

Cisco pxGrid ノードの展開

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

始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、アップグレードライセンスを最近インストールした場合は、Base インストールで特定の拡張 pxGrid サービスを使用できる可能性があります。
- すべてのノードは、Cisco pxGrid サービス用に CA 証明書を使用します。アップグレード前に Cisco pxGrid サービスにデフォルトの証明書を使用した場合、アップグレードによってその証明書が内部 CA 証明書に置き換えられます。
- Websocket（pxGrid 2.0）の場合はポート 8910 を、XMPP（pxGrid V1.0）の場合はポート 5222 を開く必要があります。ノードで Cisco pxGrid サービスが無効になっている場合、ポート 5222 はダウンしますが、ポート 8910 は機能し、引き続き要求に応答します。

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

ステップ 2 **[展開ノード（Deployment Nodes）]** ウィンドウで、Cisco pxGrid サービスを有効にするノードの横にあるチェックボックスをオンにし、**[編集（Edit）]** をクリックします。

ステップ 3 **[全般設定（General Settings）]** タブをクリックし、**[pxGrid]** トグルボタンを有効にします。**[pxGrid]** チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

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

Cisco pxGrid 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 要件に基づき、次のいずれかのチェックボックスをオンにします。

- [新しいアカウントの自動承認（Automatically Approve New Accounts）]：このチェックボックスをオンにすると、新しい Cisco pxGrid クライアントからの接続要求が自動的に承認されます。
- [パスワードベースのアカウント作成の許可（Allow password--based account creation）]：このチェックボックスをオンにすると、Cisco pxGrid クライアントのユーザー名またはパスワードベースの認証が有効になります。このオプションを有効にした場合、Cisco pxGrid クライアントを自動的に承認することはできません。

ステップ 3 [保存（Save）] をクリックします。

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

https://<ISE-Admin-Node>:9060/ers/sdk

Cisco pxGrid 証明書の生成

始める前に

- Cisco ISE pxGrid サーバーと pxGrid クライアントに同じ証明書を使用しないでください。pxGrid クライアントにはクライアント証明書を使用する必要があります。クライアント証明書を生成するには、[Administration] > [System] > [Certificates] を選択します。
- Cisco ISE の一部のバージョンには NetscapeCertType を使用する Cisco pxGrid の証明書があります。新しい証明書を生成することを推奨します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- Cisco pxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。
- デジタル署名を使用して証明書テンプレートを作成し、新しい Cisco pxGrid 証明書を生成します。

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

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、次のオプションのいずれかを選択します。

- [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）]：このオプションを選択した場合は、共通名（CN）を入力する必要があります。
- [単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with a certificate signing request)）]：このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。
- [一括証明書の生成（Generate bulk certificates）]：必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード（Download Root Certificate Chain）]：ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

ステップ 3 （オプション）この証明書の説明を入力します。

ステップ 4 [pxGrig_Certificate_Template] のリンクをクリックして証明書テンプレートをダウンロードし、必要に応じて編集します。

ステップ 5 [サブジェクト代替名（SAN）（Subject Alternative Name (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 Cisco pxGrid クライアントの IP アドレスを入力します。
- [FQDN]：pxGrid クライアントの FQDN を入力します。

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

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

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

作成した証明書は、[発行された証明書（Issued Certificates）] ウィンドウに表示されます。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）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[発行された証明書（Issued Certificates）]**。

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

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

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

Cisco pxGrid クライアントの権限の制御

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

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

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

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

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

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

- **com.cisco.ise.mdm**

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

- **<ANY>**
- **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>**：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。

ANC、および手動で追加したグループがこのドロップダウンリストに表示されます。

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

Cisco pxGrid ライブ ログ

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

このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブログ（Live Log）]** です。ログを消去して、リストを再同期またはリフレッシュすることもできます。

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