Cisco ISEと統合されたIOS-XEデバイスでの不完全なCTSプロファイルおよびSGACLダウンロードの失敗の解決

内容

問題

CTSサーバリストと環境データが存在する場合でも、ネットワークデバイス上でCisco TrustSec(CTS)プロファイルの一部または不完全が観察されます。ネットワークデバイスがセキュリティグループアクセスコントロールリスト(SGACL)アクセスコントロールエントリ(ACE)のダウンロードに失敗します。

この問題は、Catalyst 9000シリーズスイッチ、ワイヤレスLANコントローラ(WLC)、Identity Services Engine(ISE)を搭載したルータなどのCisco IOS® XEネットワークデバイスを使用する導入に影響を与えます。

ネットワークデバイスログに次のエラーが表示されます。

```
%CTS-2-AUTHZ_POLICY_SGACL_ACE_FAILED: Failed to download ACEs for SGACL '<ACLname>' for SGT='<SGTnumber>
```

環境

- ISE 3.5 パッチ 2
- ISE 3.3 パッチ 8
- ISE 3.2 パッチ 9
- CTS環境
- Cat9k、WLC、ルータなどのIOS XEネットワークデバイス

解決方法

オプションA:ISEのアップグレード（推奨）

この問題を永続的に解決するには、Cisco ISEを、Cisco Bug ID CSCws51319が解決された修正済みリリースにアップグレードします。

- 修正リリース:
  - ISE 3.5 Patch 3以降
  - ISE 3.3パッチ9以降
  - ISE 3.2 Patch 10以降

オプションB：ポリシーの手動更新（回避策）

アップグレードがすぐに可能でない場合は、ISEでポリシーが変更されるたびに、ネットワークデバイスでポリシーの更新を手動でトリガーする必要があります。

1. 該当するネットワークデバイスのCLIにアクセスします。

2. このコマンドを実行して、CTS PACステータスを確認します。

```
show cts pac
```

3. CTS環境データが存在することを確認するには、次のコマンドを実行します。

```
show cts environment data
```

4. 現在のポリシー権限を確認するには、次のコマンドを実行します。

```
show cts role-based permissions
```

5. 次のコマンドを実行して、ポリシーを更新します。

```
cts refresh policy
```

6. ダウンロードが完了するまで数分待ちます。

7. 現在のポリシー条件を確認し、次のコマンドを使用してすべての権限がダウンロードされているかどうかを確認します。

```
show cts role-based permissions
```

原因

この問題は、Cisco Bug ID CSCws51319が原因です。

関連コンテンツ

- Cisco Bug ID CSCws51319
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。