ISE 3.4 VPNおよびRADIUS認証障害のトラブルシューティング

内容

お問い合わせ内容

ISE 3.4パッチ4の導入では、セカンダリ管理ノード(SAN)が停止すると認証エラーが発生します。プライマリポリシー管理ノード(PPAN)宛ての認証要求も失敗し、ASA VPN接続とRADIUS認証の中断の原因となります。ISE導入ダッシュボードにSANノードが接続解除として表示され、ログにEAP/TLS関連のエラーとセッション追跡の問題が示されます。

環境

- Cisco Identity Services Engine（ISE）
- ネットワークアクセスデバイス(NAD):Merakiデバイスおよび/またはASAファイアウォールを含む
- トポロジ：SANおよびPPANによるマルチノードISE導入

解決策

1.- Cisco ISE Administrationインターフェイスで、Administration > System > Deploymentの順に選択して、SANノードからすべてのペルソナを削除します。これにより、障害が発生したノードに対する認証の試行が停止し、影響を受けていないノードによる処理の再開が可能になります。

注：ペルソナを削除した後も、SANノードは引き続き接続解除として展開ダッシュボードに表示されます（赤いX）。

2.- SANノードをFAILEDと見なすようにASAファイアウォールに手動で強制し、それ以上の認証の試行が使用不可能なSANに向けられないようにする。このアクションはASA設定で実行され、運用中のISEノードへのフェールオーバーを保証します。

3.- ISE導入で適切な同期を確認し、CPU、メモリ、ディスク使用率などのヘルスメトリックをモニタします。

4. – 新しいDot1x要求とRADIUS要求が影響を受けないISEノードで処理されていることを確認して、認証サービスが動作していることを確認します。

5. – 認証失敗時のDEBUGログとパケットキャプチャを収集して、EAP/TLSネゴシエーションのタイミングとセッションのリセットを分析します。

6.- SANフェールオーバーイベント後も、ISEシステムの健全性メトリックと認証動作のモニタリングを継続します。

7.- Meraki RADIUSフェールオーバーの動作を検証します。ISEがサーバの可用性を検出するための「Status-Server」RADIUSパケットをサポートしていないことに注意してください。

ログメッセージの例

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

原因

根本原因は、ISPリンクの障害によるSANノードの停止であり、サプリカント、NAD、およびISEノード間のセッショントラッキングの不整合やEAP/TLSネゴシエーションエラーの原因となります。さらに、Merakiデバイスはフェールオーバー検出に「ステータスサーバ」RADIUSパケットに依存します。これはCisco ISEがサポートしていないため、失敗したSANノードに対する認証の試行が続行されます。

関連コンテンツ

- MerakiネットワークとISEの統合方法
- ISEでのRADIUS認証とグループポリシーマッピングを使用したリモートアクセスVPNの設定
- 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。