サプリカントタイムアウトまたは設定ミスが原因でEAPセッションが放棄され、新たに開始された"5440エンドポイントのトラブルシューティング

内容

お問い合わせ内容

ISEがRADIUS Access-Challengeをエンドポイントに送信します。エンドポイントは、Access-Challengeに応答する代わりに、認証プロセスを繰り返し再起動します。Cisco Identity Services Engine(ISE)によるエンドポイント認証が最終的にエラーで失敗します。

```
"5440 – Endpoint abandoned EAP session and started new"
```

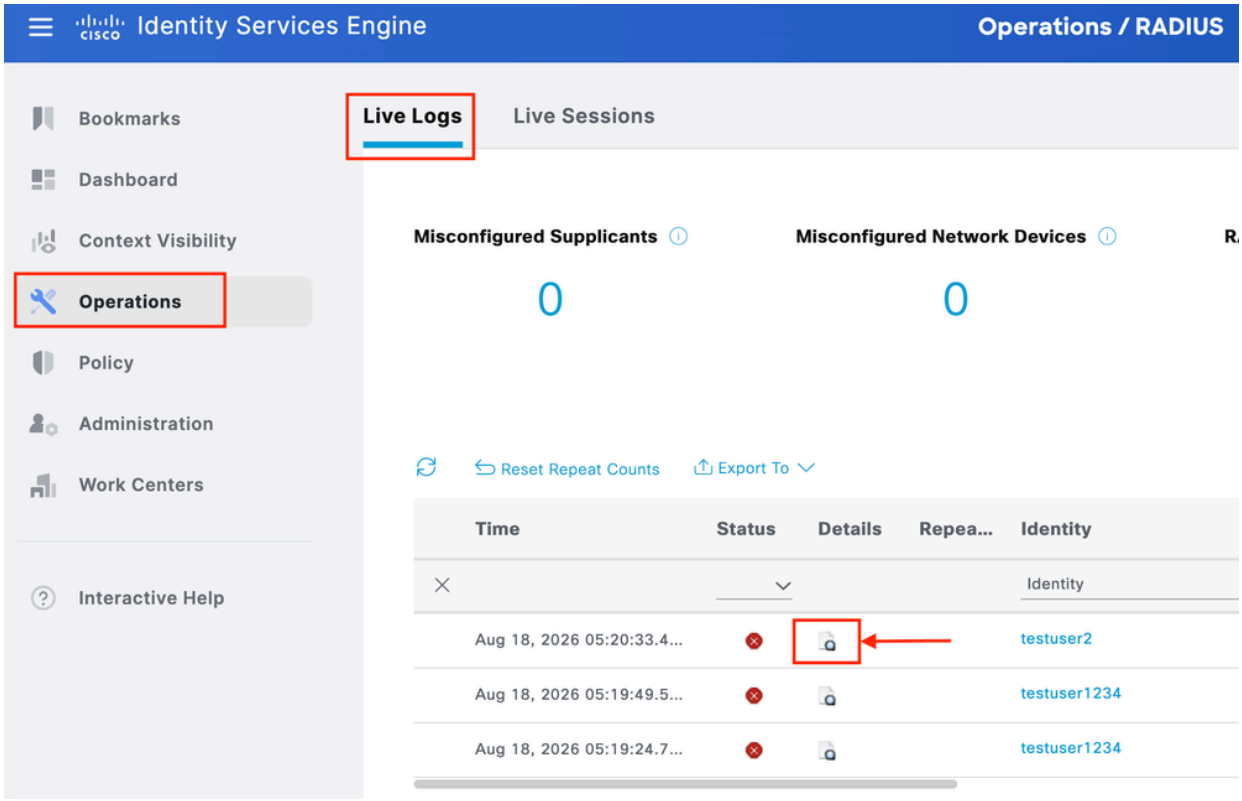
環境

- Cisco ISE
- 802.1X認証
- 有線または無線ネットワーク
- 拡張認証プロトコル(EAP)ベースの認証
- エンドポイントサプリカント

解決策

次の手順でトラブルシュートを行います:

1. ISE認証の詳細を確認します
    1. Operations > RADIUS > Live Logsの順に移動します。
    2. 失敗した認証を開きます。



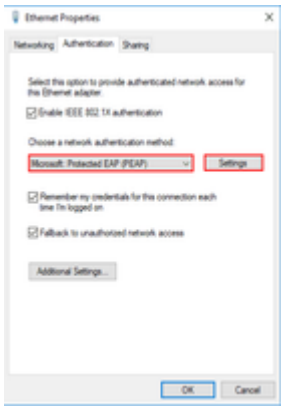
    3. ISEが「Access-Challenge」を送信することを確認します。
    4. エンドポイントがチャレンジに応答する代わりに新しい「Access-Request」を送信することを確認します。
    5. Access-Challengeと新しいAccess-Requestの間の時間をメモします。
    6. この図では、ISEが「Access-Challenge」を送信したが、ISEが応答を受信しなかったことがわかります。

Cisco Identity Services Engine

11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	0
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
5440	Endpoint abandoned EAP session and started new	58134

2. エンドポイントサプリカントの設定を確認します。

- 正しいEAP方式が設定されていることを確認します。
- Machine、User、またはMachine + User認証などの認証モードを確認します。



- サプリカントタイムアウトを確認し、設定をやり直してください。
- エンドポイントが予期される802.1Xプロファイルを使用していることを確認します。
- 設定を動作中のエンドポイントと比較します。

3. エンドポイントログの確認

- オペレーティングシステムとサプリカントの認証ログを確認します。
- サプリカントがEAP要求を受信するかどうかを確認します。
- タイムアウト、認証の再起動、またはEAP関連のエラーを特定します。
- Cisco Secure Clientを使用している場合は、さらに詳しく分析するためにDARTバンドルを収集します。
    - セキュアクライアントのDARTバンドルの収集

4. ネットワークパスを確認する

- エンドポイント(Wireshark)、NAD（SPANキャプチャ）、およびISE(TCPDump)で同時パケットキャプチャを実行
- EAPOLトラフィックがNADに到達することを確認します。

- ISEからのRADIUS応答がNADに到達することを確認します。
- エンドポイント、NAD、およびISE間のパケット損失または遅延を確認します。
- エンドポイントログで再起動の理由が特定されない場合は、パケットキャプチャを使用します。

5. 動作しているエンドポイントと比較する

- 可能な場合は、同じNAD、ISE PSN、および認証ポリシーを使用します。
- EAP方式、サプリカント設定、タイムアウト値、および認証シーケンスを比較します。
- 特定のエンドポイントだけに障害が発生した場合は、エンドポイントの設定またはサプリカントを重点的に調査します。

問題が解決したかどうかを検証するには、新しい認証を実行し、エンドポイントがISE Access-Challengeに応答し、5440を生成せずに認証が正常に完了することを確認します。

原因

設定されたタイムアウト内にエンドポイントサプリカントがEAP認証を完了しないか、または誤った802.1X設定を使用しています。サプリカントタイムアウトが短い、EAP設定が正しくない、またはサプリカントの問題があると、前のセッションが完了する前にエンドポイントが認証を再開する可能性があります。

関連コンテンツ

- EAP-TLSの理解および設定

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。