

セキュアアクセスXDR統合におけるモジュールのヘルスチェック失敗エラーコードのトラブルシューティング

内容

問題

Cisco Secure AccessとXDRの統合は、ヘルスチェックフェーズでHTTP 431「Request Header Fields Too Large」エラーで失敗します。以前は正常に統合できましたが、Cisco Secure Accessダッシュボードから生成されたAPIキーを使用して接続を確立しようとする、このエラーが表示され、突然失敗し始めました。

特定のエラーメッセージは次のように表示されます。

```
<#root>
```

```
Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access
```

このエラーにより、Secure AccessのデータがXDRに取り込まれなくなり、セキュリティの可視性と監視機能に影響が及びます。

環境

- Cisco Secure Access with Advantageライセンス
- Cisco XDRサブスクリプション
- Cisco Secure Accessテナント
- Cisco Secure Accessダッシュボードで生成されたキーを使用したAPI統合

- 必須APIスコープ：「調査」>「読取り専用」、「レポート」>「読取り専用」、「配置」>「読取り専用」、「ポリシー」>「読取り/書き込み」

解決方法

この問題は、Cisco Secure AccessでAPIキーとシークレットを再生成することで解決されました。

431エラーを解決するには、次の手順に従います。

手順1：新しいAPIキーの生成

Cisco Secure Accessダッシュボードに移動し、必要なスコープで新しいAPIキーを作成します。

- 調査：読み取り専用
- レポート：読み取り専用
- 展開：読み取り専用
- ポリシー：読み取り/書き込み

ステップ2:XDR統合への新しいキーの適用

XDR Secure Access統合設定の既存のAPIキーを、新しく生成されたキーで置き換えます。

手順3：統合の確認

統合をテストして、接続が正常に行われたことを確認します。APIコールは、431エラーではなくHTTP 200応答を返すようになりました。

予防的な検出と防御

今後、同様の431エラーを特定して防止するには、次の手順を実行します。

1.- Postmanやブラウザコンソールなどのツールを使用してデバッグを行う場合は、サイズ列で要求ヘッダーを確認します。要求ヘッダーが8 KB (8192バイト) を超える場合、APIゲートウェイで431エラーがトリガーされます。jwt.ioなどの外部ツールを使用して、OAuthトークンのサイズを確認できます。

2. - エラーパターンの分析：

- ヘルスチェックの最初のハンドシェイク中に431エラーが即座に発生した場合、スタティッククレデンシャルに問題があることを示しています
- 431エラーが、統合が数分間実行された後にのみ発生した場合は、後続の再試行に対するcookieの累積を示します

ベスト プラクティス

統合クライアント/ブラウザでCookieまたはセッションの永続性を無効にして、ヘッダー・サイズの累積を防止します。

原因

HTTP 431エラーは、Base64が標準のHTTP Authorizationヘッダー用にエンコードした際に、特定のAPIキーと秘密のペアが異常に大きいかまたは不正なAuthorizationヘッダーを生成したことが原因です。

初期APIキーの暗号文字列に一連の文字が含まれており、エンコード時にAPIゲートウェイの制限を超えるヘッダーサイズに展開されたため、「Request Header Fields Too Large」が拒否されました。

APIキーが再生成されたとき、新しい暗号文字列によって適切なサイズの認証ヘッダーが生成されました。新しいキーを取り消して生成するプロセスでは、統合マネージャ側のキャッシュされた要求コンテキストもクリアされ、ヘッダーサイズが標準化されました。

関連コンテンツ

- [Cisco Secure Access API認証](#)
- [XDRへのシスコセキュアアクセスの統合](#)
- [XDRコンソールからのHARログの収集](#)
- [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。