16進数のプレフィクス処理が原因のISE 3.4でのNTP認証失敗の設定

内容

問題

Cisco Identity Services Engine(ISE)3.4.0.608パッチ1は、40文字の長さのSHA1キーを持つ認証済みNTPを使用すると、NTPサーバとの同期に失敗します。CLIではNTP認証キーコマンドがエラーなしで受け入れられますが、認証を有効にしてもNTP同期は行われません。認証を行わないと、NTP同期は正しく動作します。シスコのスイッチを含むその他のネットワークデバイスは、同じキーIDとキー値を使用して同じNTPサーバで正常に認証されます。

トラブルシューティング中、パケットキャプチャの分析により、ISEが適切なキーIDとMAC/オーセンティケータフィールドを使用して認証済みのNTP要求を送信することが明らかになりました。ただし、サーバの応答にはすべて0のキーIDが含まれ、MAC/オーセンティケータは含まれないため、ISEは認証を拒否します。NTPサーバとして動作しているCiscoスイッチのデバッグ出力には、「SHA1-Match: 0」と表示され、認証の失敗を示していました。

環境

- Cisco Identity Services Engine(ISE)バージョン3.4.0.608（パッチ1）
- SHA1アルゴリズムを使用したNTP認証
- 40文字のNTP認証キー
- バージョン17.12.04を実行しているCisco Catalyst 9500スイッチ(C9500-24Y4C)
- 認証されたNTP設定を持つNTPサーバアプライアンス

解決方法

この問題は、Cisco Bug ID CSCwq79772が原因で発生します。この問題の影響を受けるのは、16進数のプレフィックスが必要な場合にISEで長いNTP認証キーを処理する方法です。このバグは、ISE 3.4パッチ8およびISE 3.5パッチ3で修正されました。

根本原因の理解

シスコデバイスでNTP認証キーを設定すると、20文字以上のキーは、プレーンテキストではなく16進数文字列として自動的に処理されます。これには、ISEがキーを設定するときに「HEX:」プレフィックスを使用する必要があります。ただし、このバグが原因で、追加の「HEX:」プレフィクス処理により、ISEは40文字のキーの36文字のみを受け入れ、その結果として認証エラーが発生します。

回避策の即時オプション

ISEソフトウェアを修正を含むバージョンにアップグレードできるまで、次のいずれかの回避策を使用します。

オプション1:36文字のSHA1キーを使用する

NTPサーバとISEの両方に、40文字のキーではなく、36文字のSHA1キーを設定します。

ISEで次を実行します。

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

NTPサーバ（Ciscoスイッチの例）:

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
ntp trusted-key 1
```

オプション2: MD5認証を使用する

SHA1認証からMD5認証に切り替えます。これは同じ長さの制限を示しません。

ISEで次を実行します。

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

NTPサーバ：

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

確認手順

いずれかの回避策を実行した後、NTP同期を確認します。

ISEで次を実行します。

```
show ntp
show clock
```

スイッチ上（スイッチをNTPサーバとして使用している場合）：

```
show ntp associations
show ntp status
```

認証が正常に行われたことを示すインジケータを探し、一方の側で認証が無効になっていて、もう一方の側では有効になっている場合に、NTP同期が失敗することを確認することによって、認証が機能していることを確認します。

永続的な解決策

Cisco Bug ID CSCwq79772の修正を含む次のいずれかのバージョンにISEをアップグレードします。

- ISE 3.4パッチ8（入手可能な場合）
- ISE 3.5 Patch 3以降

アップグレード後は、元の40文字のSHA1キー設定が16進数のプレフィックスで正しく動作します。

原因

この問題は、Cisco Bug ID CSCwq79772（3.4パッチ8および3.5パッチ3より前のISEバージョン）が原因で発生します。NTP認証キーが20文字以上の場合、Ciscoデバイスではこれらを16進数の文字列として扱うので、設定で「HEX:」プレフィクスが必要になります。この不具合により、ISEは16進数のプレフィックスを使用する場合にキー長の計算を誤って処理し、40文字のキーのうち36文字のみを受け入れます。この結果、ISEとNTPサーバ間でキーの不一致が発生し、NTP同期試行時に認証エラーが発生します。

関連コンテンツ

- Cisco Bug CSCwq79772（登録ユーザ専用）
- Ciscoワイヤレスコントローラコマンドリファレンス – NTP認証
- 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。