

ネットワーク時間の損失によるPKIへの影響

内容

[はじめに](#)

[ネットワーク時間の損失によるPKIへの影響](#)

[ICSeverity](#)

[影響](#)

[説明](#)

[Syslogメッセージ](#)

[メッセージサンプル](#)

[製品ファミリ](#)

[正規表現](#)

[推奨事項](#)

[コマンド](#)

はじめに

このドキュメントでは、デバイスがNetwork Time Protocol (NTP ; ネットワークタイムプロトコル) ソースとの接続を失ったときに一般的に表示されるエラーメッセージについて説明します。

ネットワーク時間の損失によるPKIへの影響

ICSeverity

0 – 緊急

影響

PKIに依存するサービスの損失。

説明

このエラーメッセージは、通常、デバイスがNetwork Time Protocol (NTP ; ネットワークタイムプロトコル) ソースとの接続を失ったときに表示されます。システムクロックは現在有効ではありません。これは、公開キーインフラストラクチャ(PKI)の運用にとって重要です。Public Key Infrastructure (PKI ; 公開鍵インフラストラクチャ) は、証明書の有効性を判断するために、正確な計時に大きく依存しています。システムクロックが正規の時刻源と同期していない場合、PKI機能は正しく動作しません。これにより、PKIサーバとの時間の不一致により、PKI証明書が無効または期限切れであると見なされる可能性があります。

この問題を解決するには、デバイスのシステムクロックを設定または更新する必要があります。これは通常、システムクロックが正確で信頼できることを保証するために、信頼できるNTPソー

スとの接続の再確立を含みます。クロックが正規の時刻源と同期されると、PKI機能を初期化でき、証明書の検証を期待どおりに進めることができます。

Syslogメッセージ

PKI-2-NON_AUTHORITATIVE_CLOCK

メッセージサンプル

Jan 4 16:40:28 <> %PKI-2-NON_AUTHORITATIVE_CLOCK: PKI functions can not be initialized until an author

製品ファミリ

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ
- Cisco Catalyst 9600 シリーズ スイッチ
- Cisco 4000 シリーズ サービス統合型ルータ

正規表現

N/A

推奨事項

このエラーは、通常、NTPサーバに接続の問題がある場合に発生します。

次の手順に従って、問題の修復を試みてください。

1. このメッセージはブートアップ中に表示される場合があります、予期されています。デバイスのブート時には、NTPサーバにアクセスして同期する時間が必要です。これが完了したら、メッセージを確認します。
2. 通常の動作中に発生した場合は、次の操作を行います。
 - a. コマンド `show ntp status` を使用して、NTPステータスが非同期として表示されるかどうかを確認します。Router#show ntp status Clock is unsynchronized, stratum 16, no reference clock <<< nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10 ntp uptime is 47585900 (1/100 of seconds), resolution is 4000 reference time is 00000000.00000000 000 GMT Mon Jan 1 1900) clock offset is 0.0000 msec, root delay is 0.00 msec root dispersion is 7137.88 msec, peer dispersion is 0.00 msec loopfilter state is 'FSET' (Drift set from file), drift is 0.000000000 s/s

system poll interval is 8, never updated.

b. コマンド Router#ping を使用して、NTP ソース/サーバへの ping を試行し、到達可能性に問題がないことを確認します。

c. ntp ソース/サーバが稼働しているかどうか、および別のデバイスから到達可能かどうかを確認します。

d. コマンド Router#show logging および Router#show ip route を使用してダイナミックルーティングプロトコル(VRRP)が設定されている場合、問題やフラップが発生していないかを確認します。

e. ポート UDP/123(Access List)が開いていて、ファイアウォールレベルでブロックされていないか、またはローカルACL (アクセスリスト) でブロックされていないかを確認します。

f. コマンド ntp server を削除してから再度追加してみてください。

コマンド

#show version

#show ip interface

#show platform

#show logging

#show ip route

#show ntp status

#show clock

#show logging

#show ip route

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。