Loss of Network Time Impacts PKI

Contents

Introduction

This document describes the error message that is commonly displayed when the device has lost connectivity with the Network Time Protocol (NTP) source.

Loss of Network Time Impacts PKI

ICSeverity

0 - Emergency

Impact

Loss of services dependent upon PKI.

Description

This error message is commonly displayed when the device has lost connectivity with the Network Time Protocol (NTP) source. The system clock is currently not valid, which is critical for Public Key Infrastructure (PKI) operations. Public Key Infrastructure relies heavily on accurate timekeeping to determine the validity of certificates. If the system clock is not synchronized with an authoritative time source, PKI functions do not operate correctly. This can lead to PKI certificates being considered invalid or expired due to time mismatches with the PKI server.

To resolve this issue, the system clock on the device must be configured or updated. This typically involves re-establishing connectivity with a reliable NTP source to ensure that the system clock is accurate and trustworthy. Once the clock is synchronized with an authoritative time source, PKI functions can be initialized, and certificate validation can proceed as expected.

SyslogMessage

PKI-2-NON_AUTHORITATIVE_CLOCK

MessageSample

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

ProductFamily

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco 4000 Series Integrated Services Routers

Regex

N/A

Recommendation

This error is commonly seen when there is a connectivity issue with the NTP server.

Please follow the steps listed to try to remediate the issue:

1. This message can be seen during bootup and it would be expected. When device is booting, it needs time to reach out to the NTP Server and synch. Once this is done, check for the messages.

2. If seen during normal operations, then follow the next actions:

a. Verify if the **NTP status** is showing as unsynchronized with the command **show ntp status**: 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 (00:00:00.000 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. Try to ping ntp source/server to confirm there is no issue with reachability with the use of the command **Router#ping**

c. Verify whether the **ntp source/server** is up and running, and if it is reachable from another device.

d. Check if there is any issue or flap with dynamic routing protocol if configured with the use of the commands **Router#show logging** and **Router#show ip route**.

e. Verify if **port UDP/123** is opened and not blocked at the firewall level or through a local ACL (Access List).

f. Try to remove and re-add the command **ntp server**.

Commands

#show version

#show ip interface

#show platform

#show logging

#show ip route

#show ntp status

#show clock

#show logging

#show ip route