Troubleshoot NTP on Unified Communications Manager

Contents

Introduction

This document describes how to troubleshoot Network Time Protocol (NTP) issues on Cisco Unified Communications (UC) products.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Unified Communications Manager (CUCM) requires that NTP be configured in order to ensure:

- Time on the CUCM nodes is synchronized.
- Time is correct prior to any time-sensitive configuration change such as certificate regeneration.
- Database replication is synchronized on all nodes in the cluster.

NTP Polling Mechanism in UC Products

CUCM uses the NTP watchdog in order to keep the time synchronized with the NTP server. The NTP Watchdog periodically polls configured external NTP server(s) and restarts NTP if the time is offset by more than three seconds.

The NTP daemon regularly corrects time, but on a millisecond time scale. A restart of NTP involves that you run an NTP one-shot in order to perform a gross time correction and follow with a restart of the NTP daemon for continued regular micro-corrections.

NTP Watchdog polls NTP once a minute on VMware and once every 30 minutes on physical machines. The polling interval is shorter for VMware because the clock in Virtual Machines (VMs) is less stable than on physical machines, and VMware features such as VMotion and Storage Migration adversely affect time.

A primary node that runs on VMware must always be configured in order to synchronize with external NTP servers that run on a physical machine(s) to compensate for the higher degree of time drift or delay in a VM. Secondary nodes are always automatically configured to reference the primary node NTP server in order to ensure that all nodes within the cluster are close in time.

NTP Watchdog keeps track of the rate at which it restarts the NTP daemon for gross time corrections due to VMWare VMotions and Storage Migrations. If this rate exceeds 10 restarts per hour, NTP Watchdog postpones further restarts until the required rate of restarts falls under 10 per hour. The combined rate of VMotions and Storage Migrations cannot exceed 10 per hour, because this rate is considered excessive.

Because of this NTP Watchdog implementation, you do not follow the poll interval, which is seen in utils ntp status. A sniffer capture has revealed 8 NTP polls (sample) every 60 seconds. This is primarily because the NTP implementation uses NTP Watchdog, and how ntpdate polls the NTP server in UC Implementation.

Identify NTP Version Used

> **Note**: CUCM Publisher is configured with an External NTP server, and the subscriber added to the cluster synchronizes to the Publisher.

> **Note**: CUCM Version 9.x and later requires that the NTPv4 server be configured as the preferred NTP server.

Run a sniffer capture in order to identify the NTP version used by the configured NTP server:

<#root>

```
admin:
```

utils network capture port 123

```
Executing command with options:
size=128         count=1000              interface=eth0
src=dest=                   port=123
ip=

16:03:03.689725 IP cucmlab.cisco.local.34063 > linux.local.ntp: NTPv4,Client, length 48

16:03:03.690174 IP linux.local.ntp > cucmlab.cisco.local.34063: NTPv3,Server, length 48
```

CUCM sends an NTPv4 packet and in response, you receive an NTPv3 packet. Although NTPv4 is backward-compatible to NTPv3, CUCM implementation of NTP varies, which results in unsynchronized NTP:

<#root>

```
admin:
```

utils ntp status

```
ntpd (pid 22458) is running...

remote      refid     st t when poll reach   delay   offset jitter
==============================================================
172.28.5.9   .INIT.     2 u   45   64 377   0.374 492.965 18.189


unsynchronised
time server re-starting
polling server every 64 s
```

In order to fix the issue, Cisco recommends you use a Linux-based external NTP server or Cisco IOS® or Cisco IOS® XE NTP server and ensure that NTPv4 is configured.

Here is a description of the NTP terminology in the NTP status output:

- The refid column indicates the remote's time source. LOCAL(0) is the local hardware clock. .INIT. means that initialization has not yet succeeded.
- The st column is the stratum of the remote NTP server. 16 is an invalid stratum value that means, this server is not considered a time provider. The stratum can be invalid for various reasons. The most common of which is that the time provider not synchronized, the configured source does not exist, or the ntp server not running.
- The t column indicates the server type (l: local; u: unicast; m: multicast, or b: broadcast).
- The when column indicates how many seconds ago the remote was queried.
- The poll column indicates the polling interval in seconds. For example, 64 means the remote is polled every 64 seconds. The shortest interval NTP uses is every 64 seconds and the longest is 1,024 seconds. The better an NTP source is rated over time, the longer the interval. (UC Implementation does not follow the interval defined here.)
- The reach column indicates the trend of reachability tests in octal, where each digit, when converted to binary, represents whether a particular poll was successful (binary 1) or unsuccessful (binary 0). For example, 1 means only one poll has been done thus far, and it was successful. 3 (= binary 11) means the last two polls were successful. 7 (= binary 111) means the last three polls were successful. 17 (= binary 1 111) means the last four polls were successful. 15 (= binary 1 101) means the last two polls were successful. The poll prior to that was unsuccessful, and the poll prior to that was successful.
- The delay, offset, and jitter columns are the round-trip delay, dispersion, and jitter in milliseconds.

Diagnose NTP-Related Issues in CUCM

Complete these steps in order to diagnose NTP-related issues:

1. Ensure that CUCM can communicate with the NTP server on Port 123.

2. Obtain the output of utils ntp status.

    - The stratum level can be less than 4 on the publisher for optimal performance.
    - If multiple NTP servers are configured, ensure at least one server is reachable; you can see the (*) symbol against the NTP server used as a reference by CUCM.

3. Review the syslog alarm and take action accordingly. Probable causes of syslog alarms are:

    - The external NTP server is not reachable.
    - NTP stratum is higher than the acceptable limit.
    - The publisher is down, so the Subscriber NTP is unsynchronized.
    - If ntpdate -q related alerts are seen, it is possible that you have NTP version 4.2.6+ with the Kiss of Death (KoD) feature enabled. (By design, the minimum interval between burst and iburst packets sent by any client is two, which does not violate this constraint. Packets sent by other implementations that violate this constraint can be dropped and a KoD packet returned if enabled). It is recommended to disable this feature when you use that version as the NTP server for a UC product.

4. Use this diagnosis module in order to verify the NTP server is configured.
    - **utils diagnose module ntp_reachability**
    - **utils diagnose module ntp_clock_drift**
    - **utils diagnose module ntp_stratum**

5. Enter **utils ntp restart** in order to restart the NTP client/server. This command is useful whenever a gross time correction needs to occur immediately or whenever external servers are still reachable and operational, but synchronization fails. Use the **utils ntp status** command in order to determine the operational status of external NTP servers.

Common Known Issues with NTP Association on CUCM

Cisco bug ID CSCue18813: NTP configuration tos maxdist parameter controlled via CLI

Resolution: Cisco Technical Assistance Center case can be raised in order to manually add the tos maxdist parameter in the ntp.conf file.

Cisco bug ID CSCuq70611: NTP Stratum test does not validate properly with single NTP Server

Fixed Version: 10.5(2.10000.005)

Cisco bug ID CSCui85967: CUCM jump upgrade from 6.1.5 to 9.1.2 fails due to NTP reference missing

Resolution: Jump upgrade documentation has been updated and NTP configuration is listed as on of the pre-upgrade task.

Cisco bug ID CSCtw46611: NTP synch fails due to incorrect file system labelling of capture.txt

Fixed Version: 8.6(2.24900.017)

Cisco bug ID CSCur94973: Time sync issue betn VMHost & VM Instance during M1 migration

Resolution: Disable the VM's NTP sync with the ESXi host with the use of this workaround . An alternate workaround is to configure the ESXi server and CUCM Publisher to point to the same NTP server.