K10240: Verifying NTP peer server communications

Non-Diagnostic

Original Publication Date: May 3, 2016
Update Date: Oct 10, 2018

Topic

You should consider using these procedures under the following conditions:

- You want to verify the Network Time Protocol (NTP) daemon service.
- You want to verify the BIG-IP system NTP configuration.
- You want to verify the communication between the BIG-IP system and the NTP peer server.
- You want to verify the network connectivity to the NTP peer server.

Prerequisites

You must meet the following prerequisites to use these procedures:

- You have root user access to the BIG-IP system.
- You have shell access to the BIG-IP command line and the TMOS Shell (tmsh).

Description

When the BIG-IP system clock is not showing the correct time zone, or the date and time is not synchronized correctly, this could be caused by incorrect NTP configuration or a communication issue with a valid NTP peer server. The procedures in this article show how you may check the NTP daemon process, verify the NTP configuration, query the NTP peer server, and check the network connectivity to the NTP peer server.

When verifying the NTP peer server communication, you can use the `ntpq` utility. The command generates output with the fields that are explained in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix to the</td>
<td>- An asterisk (*) character indicates that the peer has been declared the</td>
</tr>
<tr>
<td>remote field</td>
<td>system peer and lends its variables to the system variables.</td>
</tr>
<tr>
<td></td>
<td>- A plus sign (+) indicates that the peer is a survivor and a candidate for</td>
</tr>
<tr>
<td></td>
<td>the combining algorithm.</td>
</tr>
<tr>
<td></td>
<td>- A space, x, period (.), dash (-), or hash (#) character indicates that</td>
</tr>
<tr>
<td></td>
<td>this peer is not being used for synchronization because it either does not</td>
</tr>
<tr>
<td></td>
<td>meet the requirements, is unreachable, or is not needed.</td>
</tr>
<tr>
<td>remote</td>
<td>The <code>remote</code> field is the address of the remote peer.</td>
</tr>
</tbody>
</table>
The **refid** field is the Reference ID which identifies the server or reference clock with which the remote peer synchronizes, and its interpretation depends on the value of the stratum field (explained in the **st** definition). For stratum 0 (unspecified or invalid), the refid is an ascii value used for debugging. Example: INIT or STEP. For stratum 1 (reference clock), the refid is an ascii value used to specify the type of external clock source. Example: NIST refers to NIST telephone modem. For strata 2 through 15, the refid is the address of the next lower stratum server used for synchronization.

The **st** field is the stratum of the remote peer. Primary servers (servers with an external reference clock such as GPS) are assigned stratum 1. A secondary NTP server which synchronizes with a stratum 1 server is assigned stratum 2. A secondary NTP server which synchronizes with a stratum 2 server is assigned stratum 3. Stratum 16 is referred to as "MAXSTRAT," is customarily mapped to stratum value 0, and therefore indicates being unsynchronized. Strata 17 through 255 are reserved.

The **t** field is the type of peer: local, unicast, multicast, or broadcast.

The **when** field is the time since the last response to a poll was received (in seconds).

The **poll** field is the polling interval (in seconds). This value starts low (example: 64) and over time, as no changes are detected, this polling value increases incrementally to the configured max polling value (example: 1024).

The **reach** field is the reachability register. The octal shift register records results of the last eight poll attempts.

The **delay** field is the current estimated delay; the transit time between these peers in milliseconds.

The **offset** field is the current estimated offset; the time difference between these peers in milliseconds.

The **jitter** field is the current estimated dispersion; the variation in delay between these peers in milliseconds.

**Procedures**

- **Verifying the NTP daemon service**
- **Verifying the BIG-IP system NTP configuration**
- **Verifying the communication between the BIG-IP system and the NTP peer server**
- **Verifying the network connectivity to the NTP peer server**

**Verifying the NTP daemon service**

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to **tmsh** by typing the following command:

   tmsh

2. To show the status of the NTP daemon, type the following command:

   show /sys service ntpd
3. Optional: If the NTP daemon service is not running, and you would like to start it, type the following command:

```
start /sys service ntpd
```

4. Optional: If the NTP daemon requires a restart, type the following command:

```
restart /sys service ntpd
```

5. To exit **tmsh**, type the following command:

```
quit
```

Verifying the BIG-IP system NTP configuration

To verify that the NTP configuration is configured appropriately, refer to the following articles:

- To manage the BIG-IP system NTP configuration using the command line, refer to one of the following articles:
  - K13380: Configuring the BIG-IP system to use an NTP server from the command line (11.x - 13.x)
  - K8442: Configuring the BIG-IP system to use an NTP server from the command line (9.x - 10.x)
- To manage the BIG-IP system NTP configuration using the Configuration utility, refer to [K3122: Using the BIG-IP Configuration utility to add an NTP server](#).

Verifying the communication between the BIG-IP system and the NTP peer server

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the BIG-IP system command line.
2. To verify the NTP peer server communication, type the following command:

```
ntpq -np
```
3. Observe the output with references on the fields presented in the previous table.

**Example of a successful NTP peer server query**

If the local **ntpd** process can communicate, or attempts to communicate with a declared NTP peer server, the output from the **ntpq** command appears similar to the following example:

```
# ntpq -np

remote refid st t when poll reach delay offset jitter
==============================================================================
172.28.4.133 10.10.10.251 4 u 482 1024 377 0.815 -10.010 0.345
```

In the previous example, the remote server information (**refid**, **stratum**, **delay**, **offset**, **jitter**) displays, indicating that the servers are successfully exchanging information. The value of **377** in the **reach**
column indicates that the server was successfully reached during each of the last eight attempts, and the value of 482 in the `when` column indicates that the last response was received from the remote peer 482 seconds ago, which is within the polling interval of 1024 seconds.

**Example of a failed NTP peer server query**

If the local `ntpd` process fails to communicate with an NTP peer server, the output from the `ntpq` command may appear similar to the following example:

```
# ntpq -np remote refid st t when poll reach delay offset jitter
==============================================================================
172.28.4.133 .INIT. 16 u - 64 0 0.000 0.000 0000.00
```

*Note:* An `st` (stratum) of 16 means that the destination NTP server is unreachable or is not considered a viable candidate.

In this example, the remote server information (`refid`, `stratum`, `delay`, `offset`, `jitter`) is not available. The value `.INIT.` in the `refid` column indicates that NTP is initializing, and the server has not yet been reached. The value of 0 (zero) in the `reach` column indicates that the server has not been reached during any of the last eight attempts. The absence of a value in the `when` column indicates that no data has been received from the remote peer since the local `ntpd` process was started. The `poll` value of 64 is still at the MINPOLL value, which indicates that NTP was recently restarted.

NTP has a MINPOLL and MAXPOLL value, which it uses to determine the optimal time between updates with the reference server. If `jitter` is low, and there are no changes in data received, NTP automatically incrementally increases the `poll` value until it reaches MAXPOLL, or 1024 seconds.

*Note:* For an explanation of the inner workings of the octal shift register that displays in the `reach` column, and how to interpret the value contained therein, refer to [Understanding NTP Reachability Statistics](#). This link takes you to a resource outside of AskF5. The third party could remove the document without our knowledge.

**Example of a successful NTP preferred peer server query**

If the local `ntpd` process communicates or attempts to communicate with a declared `preferred` NTP peer server, the output from the `ntpq` command appears similar to the following example:

```
# ntpq -np remote refid st t when poll reach delay offset jitter
==============================================================================
*172.28.4.133 10.10.10.251 4 u 482 1024 377 0.815 -10.010 0.345
+172.28.4.134 10.10.10.252 6 u 482 1024 179 0.215 -1.010 0.545
```

In the previous example, **172.28.4.133** is the preferred server, or current time source, and is designated by the `*` symbol. Any remaining servers available for use are indicated by the `+` symbol.
When initially configured, NTPd can take up to a few minutes to calculate and designate the current preferred time source.

Verifying the network connectivity to the NTP peer server

If the system is unable to establish communication with a valid NTP peer server, you can perform the following actions:

- Troubleshoot the network reachability of the system to the NTP peer server.
- Ensure that no firewall rules prevent access to the NTP peer server.
- Ensure that locally-managed time servers are functioning properly.

Supplemental Information

- Traffic Management Shell (tmsh) Reference Guide

Note: For information about how to locate F5 product guides, refer to K12453464: Finding product documentation on AskF5.

- K7017: The BIG-IP ntpd process is unable to communicate with the NTP server
- K10239: Traffic originating for management purposes may not use the intended management address or management routes

Note: This link takes you to a resource outside of AskF5. The third party could remove the document without our knowledge.

Applies to:

**Product:** BIG-IP, BIG-IP AAM, BIG-IP AFM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP DNS, BIG-IP Edge Gateway, BIG-IP GTM, BIG-IP Link Controller, BIG-IP LTM, BIG-IP PEM, BIG-IP PSM, BIG-IP WebAccelerator, BIG-IP WOM
14.0.0, 13.0.1, 13.0.0, 12.1.3, 12.1.2, 12.1.1, 12.1.0, 12.0.0, 11.6.3, 11.6.2, 11.6.1, 11.6.0, 11.5.7, 11.5.6, 11.5.5, 11.5.4, 11.5.3, 11.5.2, 11.5.1, 11.5.0, 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, 11.0.0, 10.2.4, 10.2.3, 10.2.2, 10.2.1, 10.2.0, 10.1.0, 10.0.1, 10.0.0

**Product:** Enterprise Manager
3.1.1, 3.1.0, 3.0.0