Monitoring the NTP Server

eG Enterprise v6.0

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2003, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Table of Figures

No table of figures entries found.

1

Monitoring the NTP Server

A time server is a server computer that reads the actual time from a reference clock and distributes this information to its clients using a computer network. The protocol most widely-used by time servers for distributing and synchronising time over the Internet is the **Network Time Protocol** (NTP). The term NTP applies to both the protocol and the client/server programs that run on computers. The programs are compiled by the user as an NTP client, NTP server, or both. In basic terms, the NTP client initiates a time request exchange with the NTP server. As a result of this exchange, the client is able to calculate the link delay and its local offset, and adjust its local clock to match the clock at the server's computer.

On the other hand, if for any reason, the client is unable to contact the NTP server, time synchronization will not occur, resulting in serious failures - for instance, scheduled tasks may not run on time on the client, SSL certificate validity checks may go awry, domain controllers may not be able to authenticate the Windows clients, etc.

To avoid such ill effects, administrators must periodically check whether the NTP server is accessible to clients, check the responsiveness of the server to client requests, and if possible, even determine how different the client's time is from the server's time. This way, if a sudden loss of communication occurs between the client and the NTP server or if the time difference between the client and server is abnormally high, administrators can promptly detect the same and rapidly initiate remedial measures.

eG Enterprise offers a specialized **NTP Server** monitoring model to monitor the availability and overall health of the NTP server. This model requires that an **eG external agent** be deployed on any remote host – for example, an NTP client - in the environment. This external agent will run tests on the NTP server non-intrusively to check the network availability and accessibility of the NTP server, report how long the server takes to respond to client requests, and also measure the time difference between the client and the server.

The **Network** layer of this model is mapped to a **Network** test that pings the NTP server at configured intervals to evaluate the health of the network connection between the client and the server. If the network link to the server is of a poor quality and may potentially break, this test will proactively alert administrators to it. Since this test has already been discussed at length in the *Monitoring Unix and Windows Servers* document, let us proceed to the **NTP Server** layer.

1.1 The NTP Server Layer

1.1.1 NTP Time Check Test

The absence of time synchronization between an NTP client and server can have serious repercussions on the performance and operations of the client - for instance, scheduled tasks such as virus scans or backup routines may not run on time on the client, SSL certificate validity checks may go awry, domain controllers may not be able to authenticate Windows clients, etc. If these adversities are to be avoided, administrators should be proactively alerted to a potential non-sync between the client's time and the server's time and should also receive a 'heads-up' on the probable reasons for the same. This is where the **NTP Time Check** test helps! This test periodically checks the accessibility and responsiveness of the NTP server from an external location, and also indicates how different the

client's time is from the server's time. In the process, the test not only points to a time non-sync, but also reveals the probable reasons for the same - is it because the NTP server is down? Is it because the NTP server is slow in processing client requests? Or is it because the gap between the server's time and the client's time is very high?

Purpose	Periodically checks the accessibility and responsiveness of the NTP server from an external location, and also indicates how different the client's time is from the server's time. In the process, the test not only points to a time non-sync, but also reveals the probable reasons for the same - is it because the NTP server is down? Is it because the NTP server is slow in processing client requests? Or is it because the gap between the server's time and the client's time is very high?		
Target of the test	An NTP server		
Agent deploying the test	External agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The host for which the test is to be configured. 3. **PORT** – The port used by the specified **HOST** 4. **REPORT CLOCK OFFSET** – By default, this test reports the time difference between the NTP client and the server (the *Clock offset value* measure) and also indicates whether the client's time is ahead or behind the server's (the *Client time relative to server time* measure). This is why, the **REPORT CLOCK OFFSET** flag is set to **Yes** by default. However, the measures mentioned above are of significance only to an NTP client, which has to sync time with the monitored NTP server – say, a member server of a Windows domain that needs to sync time with its domain controller. On the contrary, for a host that does not seek to sync time with the NTP server, these two measures are meaningless! Such a situation may arise, if, owing to security constraints, an administrator prefers to deploy the external agent (that executes this test) on some remote host that need not sync time with the NTP server that is being monitored. Under such circumstances, the administrator may just want the test to report whether the NTP server is up and running or not, and if running, how responsive it is to requests. In this case, its best to turn off the **REPORT CLOCK OFFSET** flag by setting it to **No**, so that the *Clock offset value* measure and the *Client time relative to server time* measure are no longer reported by the test.		
Outputs of the test	One set of results for the target Server Node being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether/not the NTP server is available.	Percent	If this measure reports the value 100, it indicates that the NTP server is accessible. The value 0 on the other hand indicates that the NTP server cannot be connected to.

	Roundtrip delay: Indicates the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. This time delay therefore consists of the transmission times between the two points of a signal.	Secs	To synchronize its clock with a remote server, the client must compute the round-trip delay time and the offset. The round-trip delay δ is computed as: $$\delta = (t_3 - t_0) - (t_2 - t_1)$$ where t_0 is the client's timestamp of the request packet transmission, 100 t_1 is the server's timestamp of the request packet reception, 150 t_2 is the server's timestamp of the response packet transmission and 160 t_3 is the client's timestamp of the response packet reception. 120 The shorter and more symmetric the round-trip time, the more accurate the estimate of the current time.
	Clock offset of client: Indicates the number of seconds the client must add to its time to synchronize with the server's time.	Secs	The offset θ is given by $$\theta = \frac{(t_1 - t_0) + (t_2 - t_3)}{2}$$ A positive value indicates the server clock is higher. A negative value indicates the client clock is higher. Normally, if the client offset exceeds NTP's default panic threshold of 1000 secs, NTP exits with a message to the system log. You can however, configure NTP to allow the time to be set to any value without restriction; but, this can happen only once. If the panic threshold is exceeded after that, NTP will exit with a message to the system log. You can use the detailed diagnosis of this measure to know the client's time stamp, the server's time stamp, and the offset.

	Client time relative to server time: Indicates whether the client is behind / ahead of the server in terms of time.		If the client's clock is running faster than the server's, this measure will report the value *Ahead***.** If the client's clock is running slower than the server's, this measure will report the value *Behind*. The numeric values that correspond to these measure values are as follows: **Measure Value** / **Numeric Value** Ahead / 1 Behind / 0 **Note:** By default, this measure reports the **Measure Value**s listed above to indicate whether client is ahead or behind the server. In the graph of this measure however, the same represented using the numeric equivalents.

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **NTP Server**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.