Limitations Of NTP For Windows On A Domain Controller
Table of Contents

Limitations Of NTP For Windows On A Domain Controller ................................................................. 1
Limitations Of NTP For Windows On A Domain Controller

If the time in a **Windows Active Directory Domain** is to be synchronized then it often is *not* the preferred solution to install the NTP software package on a domain controller, eventually with a hardware reference clock like a GPS receiver or a PCI card.

Usually it is better to set up a different machine as NTP timeserver and then simply configure the domain controller to synchronize to the external NTP server.

Here are some reasons for this:

- If `w32time` runs on a domain controller then it creates an Active Directory entry which marks the domain controller as authoritative time source for the domain, so domain clients can automatically detect this time source, and synchronize to it.

- Depending on the `w32time` version and configuration, the service passes time only to its clients if it is synchronized to an upstream time source.

- If a PCI card plus driver software for the card have been installed, the Windows system time is disciplined by a service that comes with the driver package for the PCI card, but the `w32time` service is not aware that the system time is adjusted by a different service. So it may assume the system time is not synchronized, and try to synchronize to some default NTP server, e.g. `time.windows.com`, and thus work against the PCI card's driver.

- There are some registry settings which should be able to tell `w32time` that the system time is already synchronized by some other service, but it has been found that, depending on the `w32time` version, this may not work reliably. Either the `w32time` service on the domain controller did not pass the time to its clients at all, or it suddenly stopped doing so after a certain period of time, for example exactly after 1 day of operation.

- On the other hand, the NTP service (`ntpd`) can be easily configured not to change the system time but just distribute it on the network, so such a setup worked great if the Windows system time was disciplined e.g. from a built-in GPS PCI card. However, `ntpd` is unable to create the Active Directory entry that marks the domain controller as authoritative time source for the domain, so clients will not automatically identify the domain controller as reliable time source. Instead, `ntpd` may also have to be installed and configured on all the client machines to get the clients' time synchronized.

As a conclusion and best practice you can say the best solution is to install the PCI card plus its driver plus the NTP packet on a different machine than the PDC, then configure the PDC's `w32time` service to use that machine as “internet time server”, and thus synchronize to that machine via NTP.

In a mixed environment the preferred solution is to set up e.g. a Linux machine as NTP server since it can achieve better accuracy than Windows, but in a pure Windows environment any Windows machine can do the job as NTP server. Windows machines running a current Windows version...
Limitations Of NTP For Windows On A Domain Controller

(Windows 10, Server 2016 or newer) should be preferably used as NTP server since those Windows versions support a more precise time adjustment than older Windows versions.

In case of an external NTP server (e.g. a LANTIME device on the local network), `w32time` can be running as usual on the domain controller, has a reliable time source to synchronize to, and the domain clients find their authoritative time source (the domain controller) automatically.

All non-domain members can also synchronize directly to the external NTP server.

— Martin Burnicki martin.burnicki@meinberg.de 2019-12-17