CONFIGURE NTP TIME SYNC USING GROUP POLICY

https://theitbros.com/configure-ntp-time-sync-group-policy/#:~:text=Configure%20Client%20Time%20Sync%20Settings%20Using%20GPO&text=To%20do%20this%2C%20create%20a,policy%20Configure%20Windows%20NTP%20Client.

DO NOT DO THIS ON A VIRTUALIZED DOMAIN CONTROLLER, USE AND EXTERNAL SOURCE FOR VIRTUALIZED VM

Time accuracy between workstations/member servers and Active Directory domain controllers is one of the key requirements for the normal functioning of the Active Directory domain. Kerberos authentication is based on timestamps, and if the time difference between the workstation and DC is more than 5 minutes, your user will not be able to authenticate to AD. In this article, we will look at the basics of time synchronization in Active Directory, how to configure PDC sync with an authoritative time source, and how to configure the NTP time sync in the domain using Group Policies.

In the AD environment, the time synchronization is performed according to a domain hierarchy: domain-joined computers and servers get the time from the nearest domain controller on which they are logged on, all domain controllers synchronize their time with a single DC that holds the PDC (Primary Domain Controller) Emulator FSMO role. By default, the forest root domain PDC emulator gets its time from the BIOS (CMOS) clock. This configuration is not optimal because the time on all computers in the domain depends on the BIOS time setting on the PDC host and may differ from the global time.

You need to configure your PDC Emulator to sync time with an authoritative external time source (NTP provider). The external time source is usually one or more public NTP (Network Time Protocol) servers, like time.windows.com or the NTP server of your provider.

Table of Contents

- How Does Time Sync Works in AD Domain?
- Configure Primary Domain Controller (PDC) to Sync Time with External NTP Source
  - Configure External NTP Source on PDC with GPO

    - Configure Domain Client Time Sync Settings Using GPO
- How to Manually Sync Time with NTP Server on a Windows Client

How Does Time Sync Works in AD Domain?

Windows Time service (W32Time) is used to synchronize the time in the AD organization. A computer can be both a client and an NTP server.

By default, the Windows Time Service in Active Directory is configured as follows:

- After performing a clean Windows installation, an NTP client is launched on the computer, which is synchronized with an external time source (time.windows.com);
- When you join PC to domain, the time sync setting changes. All client computers and member servers in the domain synchronize their time with AD domain controllers;
- When a member server is promoted to a domain controller, it can be used as a time source for domain computers. All domain controllers synchronize their time with a domain controller with the PDC emulator role;
- The PDC emulator in the root domain is the main time source for the entire organization. It synchronizes with an external time source, or with the server's hardware clock in CMOS/BIOS (this method of time synchronization is not recommended);
- The PDC emulator in the child domain synchronizes its time with the domain controller in the parent AD domain;
- This time synchronization scheme (according to the AD DS hierarchy) works properly in most cases and doesn't require admin intervention. However, the structure of the time service in Windows may not follow the domain hierarchy.

The NTP server is enabled on all DCs by default. The following registry setting provides this:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer]: Enabled=1
```

ntp.gpo
Image not found or type unknown

If you are facing a problem when the time on clients and domain controllers is different, most likely your domain has a problem with time synchronization and then this article can be very useful for you.

First of all, it is necessary to select an NTP server you want to use. The NTP time server can be on your local network or you can use an Internet-based (external) NTP source. The list of public NTP atomic clock servers is available at http://ntp.org. In our example, we will use 0.us.pool.ntp.org, 1.us.pool.ntp.org, 2.us.pool.ntp.org, and 3.us.pool.ntp.org.

Configuring domain time synchronization using Group Policy consists of 2 steps:

1. Create a GPO for the domain controller with a PDC role;
2. Create a GPO for Windows client computers in the AD Domain.

Configure Primary Domain Controller (PDC) to Sync Time with External NTP Source

First of all, you need to configure the PDC and enable the NTP service on it. To locate the name of the server with the PDC role in the domain, run the command:

```
netdom /query fsmo
```

ntp group policy

Image not found or type unknown

Connect to the specified DC, open a command prompt, and run:

```
w32tm /query /source
```

group policy time server

Image not found or type unknown

If you see in the output:

- Local CMOS Clock — the time source on this server is its local hardware clock;
- VM IC Time Synchronization Provider — then your domain controller with the PDC role is a virtual machine that synchronizes the time with the host.

Disable time synchronization with the hardware clock on the host via the registry:

- Set the Enabled parameter to 0 in the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\VMICTimeProvider and restart the W32Time service:

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\VMICTimeProvider -Na

Restart-Service "Windows Time"
```

If you are using virtualized domain computers, disable the time sync with the hypervisor host in the VM properties.

The screenshot below shows how to disable the time synchronization of the VM with the Hyper-V host using the Time Synchronization option in the Integration Services section.

gpo ntp
Image not found or type unknown

If you are running a virtualized domain controller on VMware vSphere/ESXi, you can disable time sync in the virtual machine settings (Edit Settings > VM Options > VMware Tools > Time, uncheck the option **Synchronize guest time with host**).

gpo ntp server
Image not found or type unknown

The best approach is to configure the PDC emulator to synchronize the time directly with an external time source.

Check that the external NTP servers you have chosen are accessible from the primary domain controller (outbound port UDP 123 must be open to the PDC host). Get the current time from an external NTP server using the command:

```
w32tm /stripchart /computer:0.us.pool.ntp.org
```

In this example, the specified NTP server is available and you have successfully obtained the current time from it.

gpo time server
Image not found or type unknown

You can manually configure the time synchronization of the PDC host with an external NTP source using the w32tm.exe tool:

```
net stop w32time

w32tm /config /syncfromflags:manual /manualpeerlist:"1.us.pool.ntp.org,0x8 1.us.pool.ntp.org,0x8 2.us.pool.ntp.o

w32tm /config /reliable:yes

w32tm /config /update

net start w32time
```

Check your current configuration:

```
w32tm /query /configuration
```

group policy ntp
Image not found or type unknown

Configure External NTP Source on PDC with GPO

The PDC Emulator role can be transferred between domain controllers, so you need to make sure that GPO is applied only to the current holder of the Primary Domain Controller role. To do this, open the Group Policy Management Console (GPMC.msc). Select the WMI Filters section and create a new WMI filter with the name **Filter PDC Emulator** and the following WMI query in the root\CIMv2 namespace **Select * from Win32_ComputerSystem where DomainRole = 5**.

ntp server gpo
Image not found or type unknown

Create a new GPO and link it to the AD OU named Domain Controllers.

gpo set ntp server
Image not found or type unknown

Select this GPO and switch to the Edit mode. Go to the following section of Group Policy Editor Console: Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers.

Enable the following policy settings:

- Configure Windows NTP Client: Enabled (policy settings are described below);
- Enable Windows NTP Client: Enabled;
- Enable Windows NTP Server: Enabled.

gpo time sync
Image not found or type unknown

Specify the following settings in Configure Windows NTP Client policy:

- NtpServer: us.pool.ntp.org,0x1 1.us.pool.ntp.org,0x1 2.us.pool.ntp.org,0x1 3.us.pool.ntp.org,0x1;
- Type: NTP;
- CrossSiteSyncFlags: 2;
- ResolvePeerBackoffMinutes: 15;
- Resolve Peer BAckoffMaxTimes: 7;
- SpecialPoolInterval: 3600;
- EventLogFlags: 0.

Do not forget to configure your firewall properly and allow your PDC to access the external NTP servers and allow your internal client to connect to the NTP source on PDC. This means that you will need to open UDP port 123 on the domain controller for both inbound and outbound traffic.

You can open the NTP port on Windows Defender Firewall using PowerShell:

```
New-NetFirewallRule -Name 'NTP_Server_123_UDP_In' -DisplayName 'NTP Server In' -Description 'Allow Inbound Co

New-NetFirewallRule -Name 'NTP_Server_123_UDP_Out' -DisplayName 'NTP Server Out' -Description 'Allow Outbou
```

configure windows ntp client gpo

> **Note**. Also open outbound UDP port 123 for your PDC on any perimeter firewall (if used).

Assign a WMI filter “Filter PDC Emulator**“** that you created earlier to the GPO.

ntp server group policy

It remains to update the Group Policy settings on PDC using the command:

```
gpupdate /force
```

Perform a manual time synchronization with your NTP source:

```
w32tm /resync
```

And check the current NTP settings:

```
w32tm /query /status
```

Run the command:

```
w32tm /monitor
```

When running on a domain controller, this command shows how much time is different between other domain controllers and the external time source for which the PDC is configured.

> **Tip**. If something does not work, try to restart the Windows Time service and reset its configuration:
>
> ```
> net stop w32time
>
> w32tm.exe /unregister
>
> w32tm.exe /register
>
> net stop w32tim
> ```

Configure Domain Client Time Sync Settings Using GPO

By default in Active Directory, domain clients synchronize their time with domain controllers (option Nt5DS — synchronize time to domain hierarchy). Typically, this behavior does not need to be reconfigured. However, if there are problems with time sync on your domain clients, you can try to specify the time server directly on clients using GPO.

To do this, create a new GPO and assign it to the OU with computers. In the GPO Editor go to the following section Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers and enable the policy Configure Windows NTP Client.

As an **NTP server** specify the name of your domain (preferred) or IP address/FQDN of the PDC:

```
NTP Server: lon-dc1.adatum.com,0x9

Set Type: NT5DS

CrossSiteSyncFlags: 2

ResolvePeerBackoffMinutes: 15

ResolvePeerBackoffMaxTimes: 7

SpecialPollInterval: 3600

EventLogFlags: 0
```

Possible values for the Type parameter:

- **NoSync** — the NTP server is not synchronized with any external time source. The system clock built into the server's CMOS chip is used;
- **NTP** — the NTP server is synchronized with external time servers, which are specified in the NtpServer registry parameter (this is the default behavior on a stand-alone computer);
- **NT5DS** — the NTP server performs synchronization according to the domain hierarchy (used by default on domain-joined computers);
- **AllSync** — the NTP server uses all available sources for time synchronization.

Update Group Policy settings on the clients and check the received time sync settings as described above.

> **Hint**. By default, domain client systems automatically synchronize their clocks with the NTP server once every hour (3,600 seconds). This is configured through the registry value **SpecialPollInterval** under **HKLM\SYSTEM\ControlSet\Services \W32Time\TimeProviders\NtpClient.**

By default, Windows Server and Windows Client domain member systems synchronize their clocks once per hour (3,600 seconds).

How to Manually Sync Time with NTP Server on a Windows Client

In this section, we will describe how to manually sync time to domain controller on Windows clients. You can use this guide to configure time synchronization on non-domain (workgroup) Windows computers.

First, reset all settings for the time service and remove the service:

```
w32tm /unregister
```

time server gpo

Restart the computer and then re-register the time service:

```
w32tm /register
```

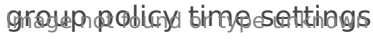
Start the w32Time service:

```
net start w32Time
```

Configure the synchronization of the Windows client with the NTP server (your PDC):

```
w32tm /config /manualpeerlist:"lon-dc01.adatum.com,0x9" /syncfromflags:manual /reliable:yes /update
```

group policy time settings



Restart the service:

```
net stop w32time && net start w32time
```

Update the time configuration settings:

```
w32tm /config /update
```

Synchronize the time:

```
w32tm /resync
```

Check the status:

```
w32tm /query /status
```

Enable automatic startup of the Time Service using PowerShell:

```
Set-Service –Name w32tm–StartupType Automatic
```

> **Hint**. If you need to quickly synchronize your Windows device with an accurate time server, run:
>
> ```
> net time \\your_ntp_server_name /set /y
> ```

Revision #2
Created 5 January 2024 04:58:15 by ColtM
Updated 13 June 2024 01:28:01 by ColtM