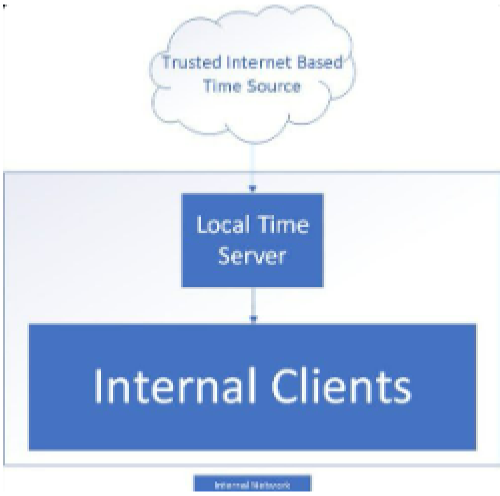
Proper Active Directory Time Sync Methods

Network Time Protocol (NTP) is a long-standing standard for computers to synchronize time between systems. NTP can be used to ensure that all synchronized computer clocks maintain the same time within a very small margin, usually measured in milliseconds. While making sure all your devices report the correct time is convenient in and of itself, ensuring proper time settings is paramount to security in ways you might not expect. Here are a few security-related items that rely on accurate time settings to work correctly:

- Certificate verification
- Kerberos authentication
- Log integrity
- One-time password (OTP) two-factor authentication

Generally, the best practice setup involves creating a trusted time source for internal clients to use as a reference to sync against. This internal time source in turn syncs against a trusted external time source. Following the trail of time syncing, we would expect time to sync from the trusted external source to the trusted local source to all other clients as seen in Figure 1. You may consider having the Active Directory domain controller (DCs) sync to an external time source independently rather than use a single trusted internal source, but this would cause additional overhead and problems such as clock drift that you may not realize until it becomes an issue.

Figure 1 – Proper syncing from an external time source to a trusted internal source



Take an example where the external time source is no longer available. Your clocks will slowly begin to drift until they eventually desynchronize, causing issues such as failed Kerberos authentication. The worst-case scenario for a single trusted time source is that the entire environment “fails together” but clients still have accurate time relative to each other, allowing your critical services to keep moving. All internal clocks would have the same time even if synchronization to the external source were to stop working.

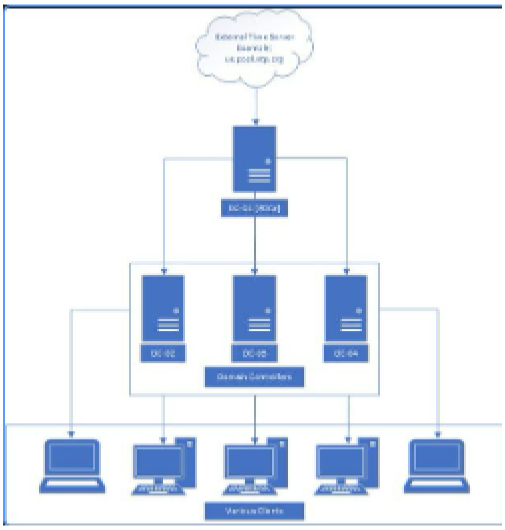
Because time services are a necessity for any network, there are many trusted sources that offer public NTP servers for clients and other networks to sync against. While not nearly an exhaustive list, the following table lists a few example sources.

Provider	URL
Google	http://time.google.com
CloudFlare	time.cloudflare.com
Microsoft	time.windows.com
Apple	time.apple.com
NIST	time.nist.gov
NTP Project	pool.ntp.org

Microsoft’s Recommendations

Active Directory (AD) has a built-in NTP server configured on DCs. Modern DCs leverage NTP with backward compatibility support for Simple Network Time Protocol (SNTP) used in some older Windows environments such as Windows 2000. In most situations where Active Directory Domain Services (AD DS) is already installed, a Domain Controller makes a great candidate for internal time servers that can support both NTP and SNTP. There are usually multiple DCs in any given environment, so the role of determining the base time for all other DCs and by extension all other clients is the responsibility of the DC with the Primary Domain Controller Emulator (PDCe) Flexible Single-Master Operation (FSMO) role in the forest root domain. Figure 2 shows an example configuration using DCs as time servers.

Figure 2 – Example time sync configuration for a single AD domain



While the PDC emulator will likely be using the standard NTP protocol to sync from an external source, all other DCs, member servers, and client computers joined to the domain will typically be configured to forego use of the NTP protocol for the Microsoft-specific NT5DS time synchronization method. Typically, any client joined to the domain should be configured to use NT5DS to synchronize time through AD automatically. In most situations, no actual client configuration should be required unless an existing configuration that uses NTP needs to be removed.

Multi-Domain Forest NTP Considerations

Time synchronizations for forests that have multiple domains don’t all sync directly with the parent domain PDCe DCs. In a situation where one or more child domains exist, time synchronization can be determined using the following table.

Domain	Device Type	Syncs Time From
Parent	PDCe DC	External time source
Parent	Non-PDCe DC	Parent domain PDCe DC
Parent	Domain-joined client	Parent domain DC
Child	PDCe DC	Any parent domain DC
Child	DC	Any child domain DC
Child	Domain-joined client	Child domain DC

Note: this table assumes the CrossSiteSync flag is set to the Microsoft default of 2; other configurations are possible and will be elaborated on in a future blog post

Configuring a Robust Internal Time Syncing Infrastructure

While it’s trivial to configure external NTP synchronization from the PDCe, it becomes another item to manage and configure in the event of transferring FSMO roles. A more robust solution that would allow for external NTP configurations to be transferred along with the PDC emulator role would be ideal. To this end, the following configuration items are recommended:

- Create a Group Policy Windows Management Instrumentation (WMI) filter to target the PDCe role holder.
- Create a Group Policy Object (GPO) to allow the PDCe to sync time from a trusted external source, apply the WMI filter you previously created, and link the GPO to the default Domain Controllers organizational unit (OU).

This means that if the PDCe role is transferred from one Windows server to another, Group Policy will enforce external time syncing on the DC with the newly acquired PDCe role. Once the policy for the PDCe is unlinked due to role change, the old PDCe returns to the normal NT5DS synchronization—allowing it to gather time from the new PDCe rather than the originally configured external time source.

Requirements for Configuration

- The DC(s) that may be serving as PDCe are allowed to access the configured external trusted time server using the NTP protocol [UDP Port 123].
- The DCs not serving as the PDCe are allowed to access the PDCe using the NT5DS protocol [UDP Port 123].
- Clients can reach the DCs serving as NTP servers using both the NTP and NT5DS protocol [UDP Port 123].

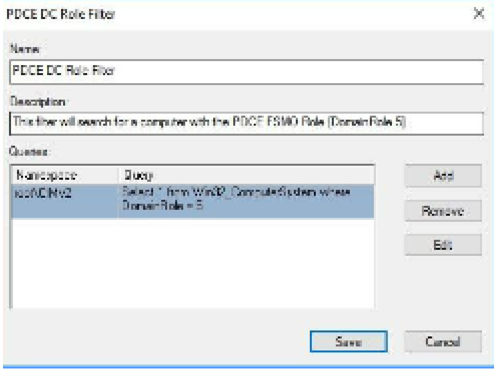
PDCe DC Role Filter Configuration

The first required step is to create the WMI filter that will be used to ensure only the PDCe is allowed to sync from an external time source. This can be configured from the Microsoft Management Console (MMC) Active Directory Group Policy Management snap-in, as Figure 3 shows.

1. Right-click the **WMI Filters** folder and right-click **New**
2. Give the new filter a meaningful name, for example **PDCe DC Role Filter**

3. Give the new filter a meaningful description such as “**This filter will search for a computer with the PDCe FSMO Role [DomainRole 5]**”
4. Create a new query by clicking **Add**
5. Leave the **Namespace** field at the default value of **root\CIMv2**
6. Enter the following text for the **Query** value: **Select * from Win32_ComputerSystem where DomainRole = 5**

Figure 3 – Example role filter to target only the PDCeNote: this query will specifically look for the DomainRole value of 5 which is only used by the DC with the PDCe FSMO role



PDCE DC Role Filter

Name: PDCE DC Role Filter

Description: This filter will search for a computer with the PDCE FSMO Role (DomainRole 5)

Queries:

Namespace	Query
root\CIMv2	Select * from Win32_ComputerSystem where DomainRole = 5

PDCe NTP Configuration GPO Creation

The next step is to create a GPO that will configure the PDCe to sync time from an external source. This can be configured from the MMC **Active Directory Group Policy Management** snap-in.

1. Right-click the **Group Policy Objects** folder and click **New**
2. Give the new GPO a meaningful name such as **Configure PDCe Time Server**
3. Select **Configure PDCE Time Server GPO** and set the **WMI Filtering** filter to **PDCE DC Role Filter**
4. Edit the **Configure PDCE Time Server GPO** and navigate to: Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time Providers
5. Edit the **Configure Windows NTP Client** setting and set the following values:

Status	**Enabled**
NtpServer	http://us.pool.ntp.org **,0x9** http://1.us.pool.ntp.org **,0x9** **2.us.pool.ntp.org**,0x9 http://3.us.pool.ntp.org **,0x9;**
Type	NTP

CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	3600
EventLogFlags	3

Note: You may choose different external time servers based on your location and needs; these values are only given as an example but will work.

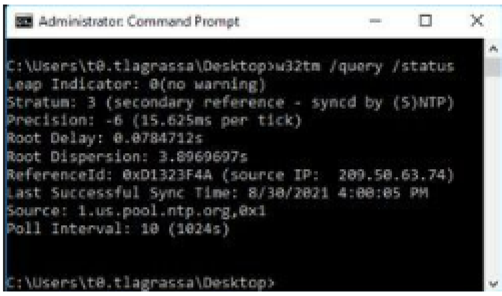
1. Edit the **Enable Windows NTP Client** setting and set the following value: **Status**: **Enabled**
2. Edit the **Enable Windows NTP Server** setting and set the following value: **Status**: **Enabled**
3. Exit the **Configure PDCE Time Server** Group Policy window
4. Right-click the **Domain Controllers** OU and select **Link an Existing GPO**
5. Select **Configure PDCE Time Server** and click **OK**

Testing NTP Configuration on the PDCe

1. Log on to the **PDCe** DC and open an administrative CMD prompt
2. Perform a Group Policy update by entering the following command: **gpupdate /force**
3. Confirm that Group Policy has been updated successfully
4. Check the NTP client configuration by entering the following command: **w32tm /query /status**

The output should confirm that the source is one of the external time servers configured in the GPO, as seen in Figure 4.

Figure 4 – The PDCe is correctly syncing from an external source



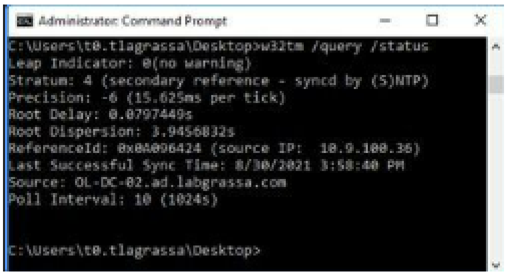
```
C:\Users\t0.tlagrassa\Desktop>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0784712s
Root Dispersion: 3.8969697s
ReferenceId: 0xD1323F4A (source IP:  209.50.63.74)
Last Successful Sync Time: 8/30/2021 4:00:05 PM
Source: 1.us.pool.ntp.org,0x1
Poll Interval: 10 (1024s)


C:\Users\t0.tlagrassa\Desktop>
```

Testing NTP Configuration on a Non-PDCe DC or Client

1. Log on to a non-PDCe DC and open an administrative CMD prompt
2. Perform a Group Policy update by entering the following command: **gpupdate /force**
3. Confirm that Group Policy has been updated successfully
4. Check the NTP client configuration by entering the following command: **w32tm /query /status**

The output should confirm that the source is the PDCe or DC, as seen in Figure 5.

Figure 5 – The DC is correctly syncing time from the PDCe



```
C:\Users\t0.tlagrassa\Desktop>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0797449s
Root Dispersion: 3.9456832s
ReferenceId: 0x0A096424 (source IP:  10.9.100.36)
Last Successful Sync Time: 8/30/2021 3:58:40 PM
Source: OL-DC-02.ad.labgrassa.com
Poll Interval: 10 (1024s)


C:\Users\t0.tlagrassa\Desktop>
```

Final Considerations

Time synchronization is an important yet sometimes overlooked part of security. Luckily, the tools offered through AD allow for a relatively simple time synchronization configuration that proves to be robust and survivable even through FSMO role changes. It may also be worth investigating other NTP configurations, such as configuring DHCP Option #42 to automatically configure NTP sources on your network for non-domain-joined devices.

Revision #1
Created 2 September 2024 20:34:58 by Steve Ling
Updated 2 September 2024 20:42:00 by Steve Ling