NTP en Windows Active Directory (**w32tm**)

En Active Directory, la sincronización horaria es **crítica** para el funcionamiento de la autenticación **Kerberos**, que por defecto sólo tolera una diferencia máxima de 5 minutos (skew) entre el cliente y el servidor.

La jerarquía de tiempo en AD funciona así:

1. El rol **PDC Emulator (PDCe)** del dominio raíz del bosque es el servidor de hora autorizado para toda la organización.
2. Este PDCe debe sincronizarse con una fuente de hora **externa** fiable (como `pool.ntp.org` o servidores NTP nacionales).
3. Todos los demás Controladores de Dominio (DCs) sincronizan su hora desde el PDCe.
4. Todos los servidores miembro y estaciones de trabajo sincronizan su hora desde *cualquier* DC (el que usen para autenticarse).

Este tutorial se centra en configurar correctamente el paso 2: el PDC Emulator del dominio raíz.

Paso 1: Identificar el PDC Emulator (PDCe)

Primero, debes ejecutar estos comandos en el DC que tenga el rol de **PDC Emulator** del **dominio raíz del bosque**.

Para averiguar qué servidor tiene este rol, abre un Símbolo del sistema (CMD) o PowerShell como Administrador en cualquier DC del dominio raíz y ejecuta:

Bash
netdom query fsmo

Busca la línea que dice "Maestro de emulador PDC". Ese es el servidor donde debes realizar la siguiente configuración.

Paso 2: Configurar la fuente de hora externa en el PDCe

En el servidor PDCe identificado en el paso 1, abre un Símbolo del sistema (CMD) o PowerShell **como Administrador**.

Define los servidores NTP externos. Usaremos `pool.ntp.org` como ejemplo, que es un conjunto público y fiable. El flag `0x8` le indica a `w32tm` que opere en modo "Cliente".
Bash
w32tm /config /manualpeerlist:"0.pool.ntp.org,0x8 1.pool.ntp.org,0x8 2.pool.ntp.org,0x8" /syncfromflags:manual /reliable:yes

1. *Desglose del comando:*
    - `/manualpeerlist:"..."`: Especifica la lista de servidores NTP externos. Se recomienda usar varios por redundancia.
    - `/syncfromflags:manual`: Indica al servicio que debe usar la lista manual de *peers* (la que acabamos de definir).
    - `/reliable:yes`: Configura este servidor como una fuente de hora "fiable" para el resto del dominio. Esto es **esencial** para que los otros DCs confíen en él.

Aplica la configuración. Después de definir la configuración, debes informar al servicio de tiempo para que use los nuevos cambios:
Bash
w32tm /config /update

2.

Paso 3: Reiniciar el servicio y forzar la sincronización

Reinicia el servicio de tiempo de Windows (w32time) para que cargue toda la nueva configuración.
Bash
net stop w32time
net start w32time

1. *(O en PowerShell: `Restart-Service w32time`)*

Fuerza una resincronización inmediata contra los *peers* externos que configuraste.
Bash
w32tm /resync /rediscover

2. (Puede que tengas que ejecutarlo un par de veces o esperar unos minutos para que se establezca la conexión).

Paso 4: Verificar la configuración del PDCe

Ahora, verifica que el PDCe esté sincronizado correctamente con la fuente externa.

Comprueba el estado:
Bash
w32tm /query /status

1. *Qué buscar:*
    - **Fuente (Source):** Debería mostrar uno de los servidores de `pool.ntp.org` que configuraste.
    - **Stratum:** Debería mostrar un número bajo (como 2, 3 o 4). Si muestra 1 (propia local) o un número muy alto, algo está mal.

Comprueba los *peers* (fuentes):
Bash
w32tm /query /peers

2. Esto te mostrará la lista de tus servidores externos, su estado (debería decir "Active") y la última vez que se sincronizó.

Paso 5: Verificar otros DCs y Clientes

No necesitas configurar nada en los otros DCs o en los clientes. Por defecto, ellos están configurados para usar la jerarquía del dominio (`NT5DS`).

- **Otros DCs:** Sincronizará automáticamente con el PDCe que acabas de configurar.
- **Clientes/Miembros:** Sincronizará con el DC que les haya autenticado.

Si por alguna razón un DC secundario o un cliente no está sincronizando correctamente (lo cual puedes verificar con `w32tm /query /status`), puedes forzarlo a usar la jerarquía del dominio con estos comandos en esa máquina:

Bash
w32tm /config /syncfromflags:domhier /update
w32tm /resync /rediscover

Consideraciones Importantes

Firewall

Asegúrate de que el **firewall** de tu red (y el Firewall de Windows en el PDCe) permita el tráfico **UDP saliente en el puerto 123** (NTP) hacia los servidores NTP externos.

Virtualización (¡Muy Importante!)

Si tu PDC Emulator es una **máquina virtual (VM)**, debes deshabilitar la sincronización de hora entre la VM y el *host* (Hyper-V, VMware, etc.).

- **En Hyper-V:** Ve a la configuración de la VM -> "Servicios de integración" -> Desmarca la casilla "Sincronización de hora".
- **En VMware:** Ve a la configuración de la VM -> Pestaña "Opciones" -> "Herramientas de VMware" -> Desmarca "Sincronizar hora del sistema invitado con el host".

Si dejas activada la sincronización con el host, el host y el servidor NTP externo "lucharán" por establecer la hora, causando derivas de tiempo (time drift) y problemas graves en Kerberos. El PDCe *solo* debe obtener la hora de la fuente NTP externa.