AP2 – Mise en place d'un Serveur NTP Interne avec pfSense

Compte rendu technique
BTS SIO 2 – Année 2024-2025

1. Contexte de l'infrastructure

Ce projet consiste à mettre en place un serveur NTP interne basé sur pfSense. L'objectif est de fournir une synchronisation horaire fiable et identique pour tous les équipements du réseau : serveur Active Directory, serveur de fichiers, postes clients et switch Cisco.
Une heure cohérente est indispensable au fonctionnement correct du domaine Active Directory, des journaux d'événements (logs) et de la sécurité réseau.

2. Tableau d'adressage

Ce tableau résume les adresses IP des équipements impliqués dans la synchronisation NTP.

Nom de l'équipement	Adresse IP	Masque	Passerelle
DEBIAN CLIENT	192.168.1.30	255.255.255.0	192.168.1.254
DEBIAN SRV	192.168.1.20	255.255.255.0	192.168.1.254
Oscar-GLPI	192.168.1.223	255.255.255.0	192.168.1.254
PC-CLIENT 1	192.168.2.10	255.255.255.0	192.168.1.254
PFsense	192.168.1.254	255.255.255.0	192.168.1.254
WIN-SRV-FICHIER	192.168.1.2	255.255.255.0	192.168.1.254
WinSRV	192.168.1.10	255.255.255.0	192.168.1.254
Switch Externe	192.168.1.1	255.255.255.0	192.168.1.254

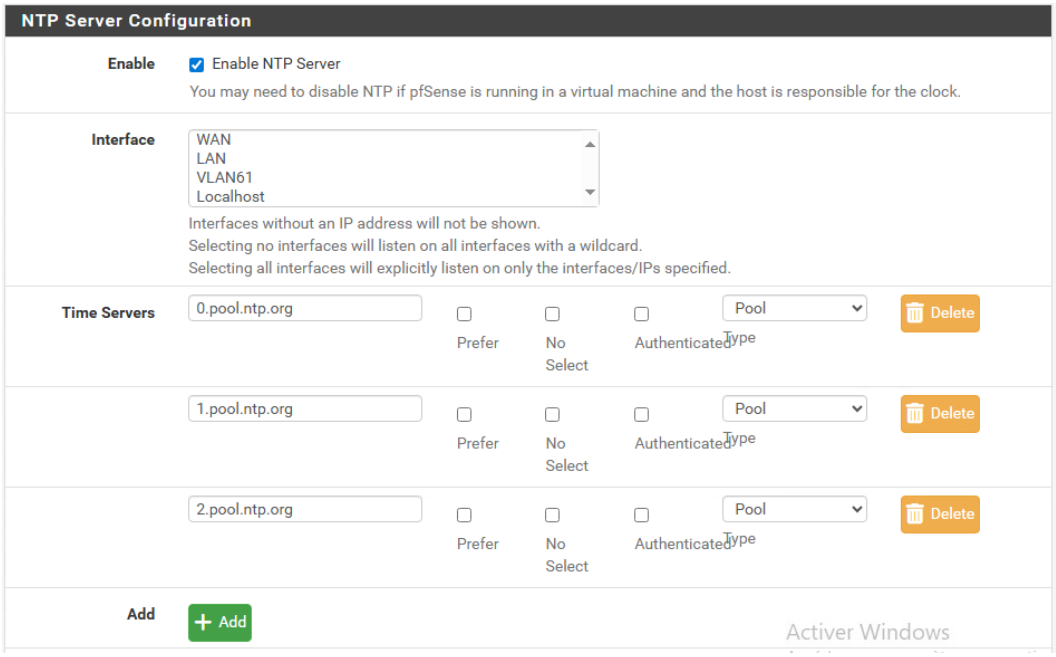
3. Pré-requis

- pfSense fonctionnel et accessible via son interface web.
- Un serveur Windows jouant le rôle de contrôleur de domaine.
- Postes clients intégrés au domaine.
- Switch Cisco accessible en CLI.
- Droits administrateur sur tous les systèmes.

4. Configuration NTP sur pfSense

Cette étape consiste à configurer pfSense pour qu'il agisse en tant que serveur NTP.

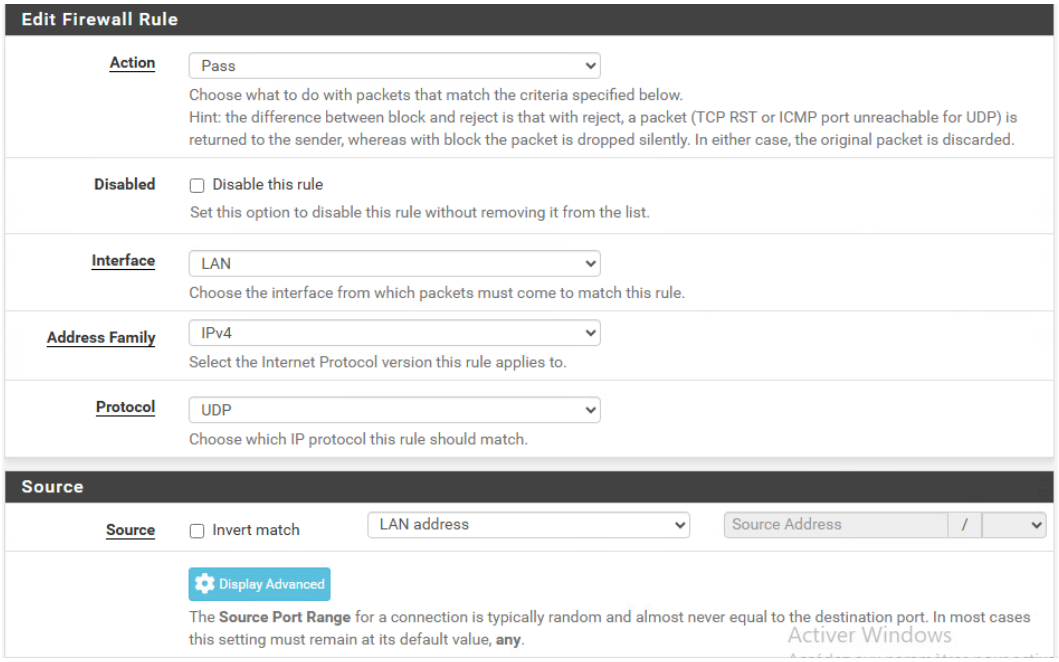
1. Aller dans Services → NTP.
2. Cocher « Enable NTP Server ».
3. Interface(s) → sélectionner LAN.
4. Ajouter les serveurs externes suivants :
   - 0.pool.ntp.org
   - 1.pool.ntp.org
   - 2.pool.ntp.org
5. Sauvegarder et appliquer.

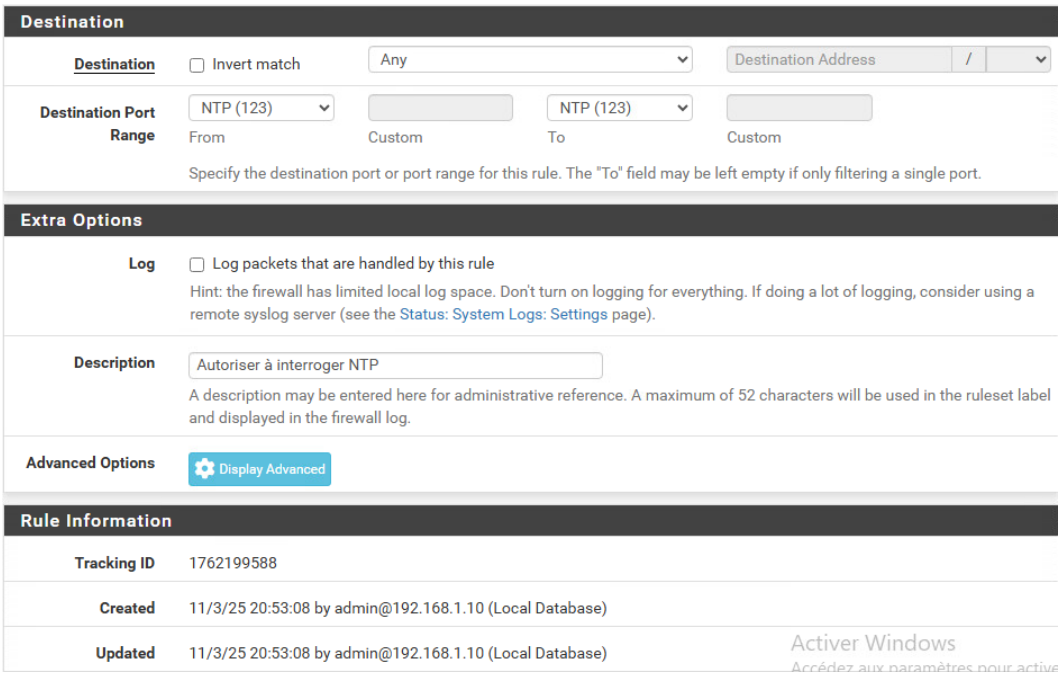


5. Configuration du pare-feu pfSense

Il est essentiel d'autoriser les clients à contacter pfSense via le port UDP 123.

Étapes :
1. Aller dans Firewall → Rules → LAN.
2. Ajouter une règle en haut de liste.
3. Action : Pass – Protocole : UDP.
4. Source : LAN net.
5. Destination : This Firewall (self).
6. Port : 123.
7. Sauvegarder et appliquer.

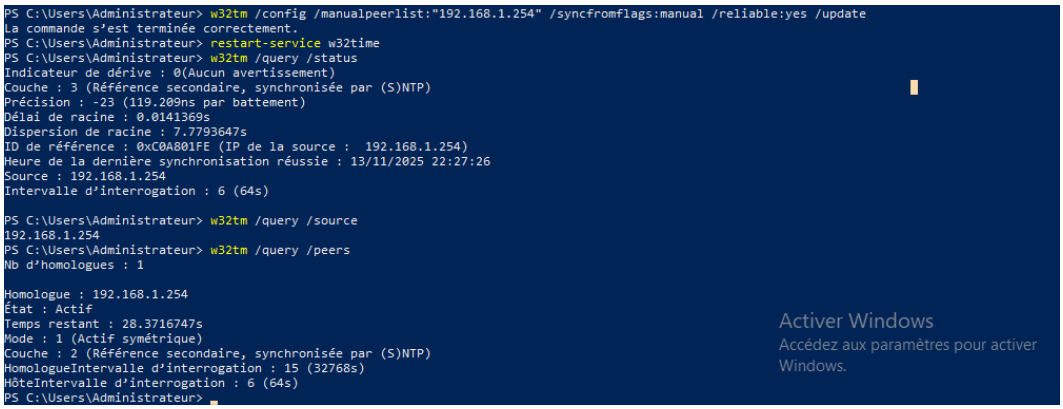




6. Configuration du contrôleur de domaine (AD)

Le contrôleur de domaine doit utiliser pfSense comme source de temps. Exécuter dans PowerShell (administrateur) :

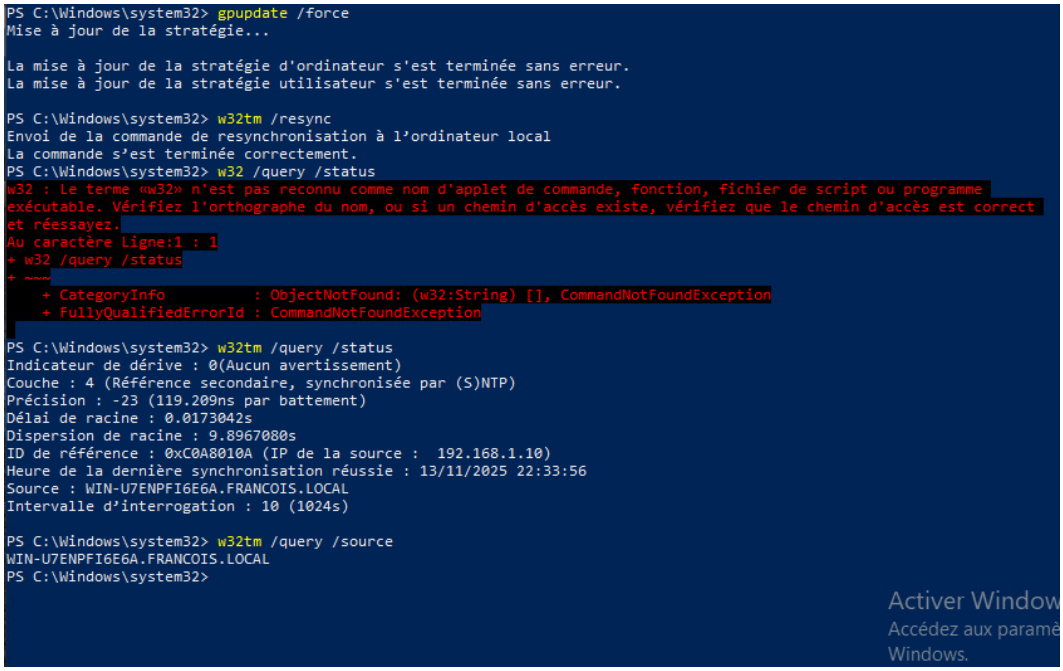
w32tm /config /manualpeerlist:"192.168.1.254" /syncfromflags:manual /reliable:yes /update
Restart-Service w32time
w32tm /resync



7. Clients Windows

Les clients récupèrent l'heure du contrôleur de domaine.
Pour forcer une mise à jour :

gpupdate /force
w32tm /resync
w32tm /query /source

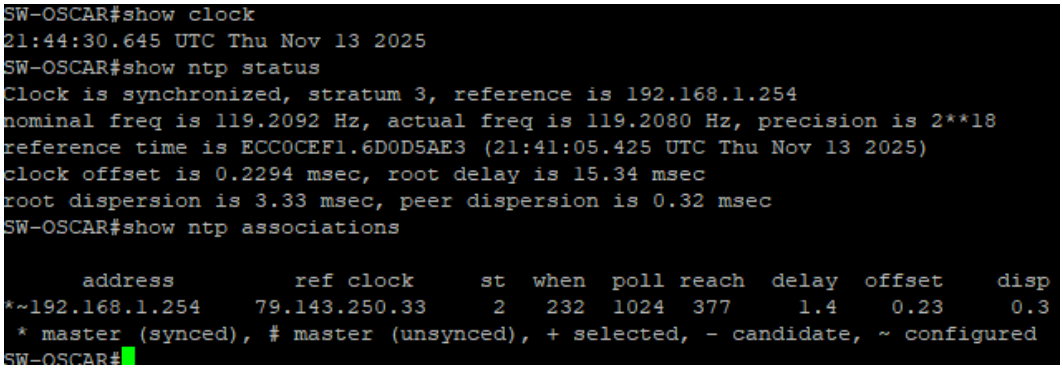


9. Configuration du switch Cisco

Configurer pfSense comme serveur NTP :

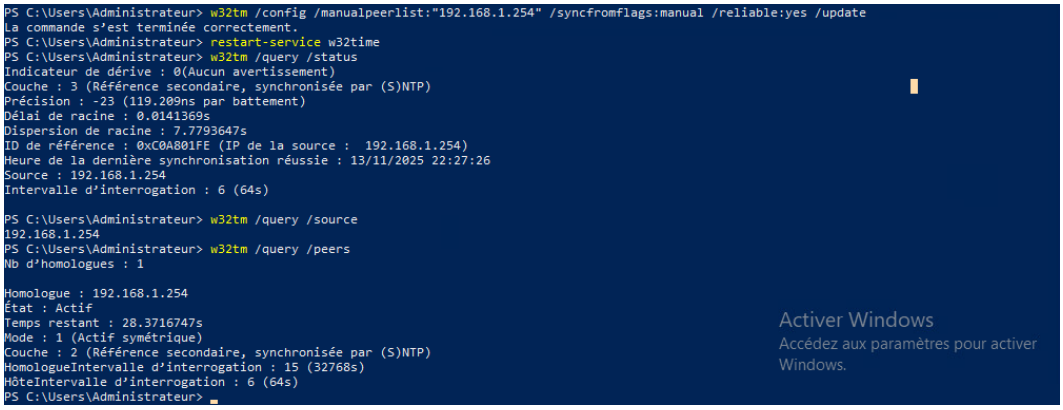
conf t
ntp server 192.168.1.254
end
write memory

Vérifications : show ntp status / show ntp associations



10. Vérifications globales

Sur pfSense : ntpq -p
Sur Windows : w32tm /query /status
Sur Cisco : show ntp status



11. Conclusion

La mise en place de ce serveur NTP interne permet de centraliser la distribution de l'heure au sein de l'infrastructure. Tous les équipements (pfSense, contrôleur de domaine, postes clients et switch Cisco) sont désormais synchronisés sur une même source fiable.

Cette synchronisation garantit un fonctionnement cohérent des services Active Directory, des journaux d'événements et des équipements réseau, tout en restant simple à administrer. La solution retenue, basée sur pfSense, est adaptée à un contexte professionnel et constitue une base solide pour de futures évolutions de l'infrastructure.