LIVRE BLANC – Network Time Protocol (NTP)

Architecture, bonnes pratiques et exploitation en production

RDEM Systems – Expertise systèmes et infrastructures critiques

Janvier 2026

Introduction

Le protocole **NTP (Network Time Protocol)** est un composant fondamental de toute infrastructure informatique moderne. Défini par la RFC 5905, NTP permet de synchroniser les horloges des systèmes informatiques avec une précision de l'ordre de la milliseconde sur Internet, et de la microseconde sur un réseau local.

Une synchronisation fiable de l'heure est indispensable pour :

- **Sécurité** : Certificats TLS/SSL, authentification Kerberos, tokens TOTP
- **Journalisation** : Corrélation des événements entre systèmes distribués
- **Conformité** : Exigences PCI-DSS, HIPAA, SOX pour l'horodatage des audits
- **Applications** : Bases de données distribuées, transactions financières, ordonnanceurs

Une dérive horaire de quelques secondes peut entraîner des échecs d'authentification, des incohérences dans les logs, voire des corruptions de données dans les systèmes distribués.

Comprendre les strates NTP

NTP utilise un système hiérarchique appelé **strates** (stratum) pour organiser les sources de temps :

Strate	Description	Précision typique
0	Horloges de référence (GPS, horloges atomiques, DCF77)	< 1 µs
1	Serveurs connectés directement à une strate 0	< 10 µs
2	Serveurs synchronisés sur des strates 1	< 100 µs
3-15	Serveurs en cascade (chaque niveau ajoute du délai)	1-100 ms
16	Non synchronisé (invalide)	-

Recommandation : Pour un usage en production, utilisez des serveurs de strate 2 ou 3. Les serveurs de strate 1 sont généralement réservés aux opérateurs du NTP Pool ou aux grandes organisations.

Pourquoi minimum 3 serveurs NTP ?

La configuration du nombre de serveurs NTP est critique pour la fiabilité :

- **1 serveur** : Point de défaillance unique. Aucune détection possible si le serveur dérive.
- **2 serveurs** : En cas de désaccord, impossible de déterminer lequel a raison.
- **3 serveurs** : Quorum possible. Si un serveur dérive, les deux autres permettent de l'identifier et de l'exclure (algorithme de sélection NTP).
- **4 serveurs** : Risque de split 2/2 en cas de désaccord, réduisant la fiabilité.
- **5 serveurs** : Configuration optimale pour les environnements critiques.

Règle générale : Utilisez un nombre **impair** de serveurs (3 ou 5) pour permettre un consensus fiable.

Pools NTP recommandés

Infrastructure RDEM Systems (recommandé)

RDEM Systems opère une infrastructure NTP **Strate 2** haute disponibilité, hébergée en France et contribuant au NTP Pool Project mondial (AS206014).

Serveur	Description
`pool-ntp.rdem-systems.com`	Pool global (11 serveurs Stratum 2)
`pa3.pool-ntp.rdem-systems.com`	Pool datacenter PA3
`pa4.pool-ntp.rdem-systems.com`	Pool datacenter PA4
`pa5.pool-ntp.rdem-systems.com`	Pool datacenter PA5

Avantages : Infrastructure monitorée 24/7, précision sub-milliseconde, hébergement européen (RGPD), contribution vérifiable : https://www.ntppool.org/a/rdem-systems

Alternatives : Pools nationaux NTP Pool Project

En fallback, utilisez les pools nationaux du projet pool.ntp.org. Chaque pays dispose de plusieurs serveurs accessibles via les préfixes 0, 1, 2 (ex: `0.fr.pool.ntp.org`).

France	Belgique	Suisse
`0.fr.pool.ntp.org`	`0.be.pool.ntp.org`	`0.ch.pool.ntp.org`
`1.fr.pool.ntp.org`	`1.be.pool.ntp.org`	`1.ch.pool.ntp.org`
`2.fr.pool.ntp.org`	`2.be.pool.ntp.org`	`2.ch.pool.ntp.org`

Autres pays disponibles : `de`, `uk`, `us`, `ca`, `au`, etc.

Pools continentaux : `europe.pool.ntp.org` | `pool.ntp.org`

Configuration Windows (W32Time)

Vérification de l'état actuel

```
w32tm /query /status
w32tm /query /configuration
w32tm /query /peers
```

Configuration recommandée (RDEM Systems)

Exécutez en **PowerShell Administrateur** :

```
net stop w32time

$NTP = "pa3.pool-ntp.rdem-systems.com,0x1 " +
       "pa4.pool-ntp.rdem-systems.com,0x1 " +
       "pa5.pool-ntp.rdem-systems.com,0x1"

w32tm /config `
      /syncfromflags:manual `
      /reliable:YES `
      /update `
      /manualpeerlist:"$NTP"

net start w32time
w32tm /resync /force
```

Alternative avec pools nationaux (fallback)

```
$NTP = "0.fr.pool.ntp.org,0x1 " +
       "1.fr.pool.ntp.org,0x1 " +
       "2.fr.pool.ntp.org,0x1"

w32tm /config /syncfromflags:manual /reliable:YES `
      /update /manualpeerlist:"$NTP"
```

Flags de configuration

Flag	Description
0x1	Utiliser comme source
0x2	Utiliser comme fallback uniquement
0x8	Utiliser le mode client (recommandé)

Active Directory

Seul le **PDC Emulator** synchronise sur des sources externes :

```
# PDC Emulator : voir configuration ci-dessus

# Autres DC (hiérarchie domaine)
w32tm /config /syncfromflags:domhier /update
```

Configuration Linux

Identifier le service actif

```
timedatectl
systemctl status chronyd ntpd systemd-timesyncd
```

Chrony (recommandé)

Chrony est le client NTP recommandé pour les distributions modernes (RHEL 8+, Ubuntu 20.04+).

Installation

```
# Debian/Ubuntu
sudo apt install chrony

# RHEL/CentOS/Rocky/Alma
sudo dnf install chrony
```

Configuration moderne (sources.d)

Créez le fichier `/etc/chrony/sources.d/rdem-systems.sources` :

```
cat << 'EOF' | sudo tee /etc/chrony/sources.d/rdem-systems.sources
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst
EOF

sudo chronyc reload sources
```

Configuration classique (/etc/chrony/chrony.conf)

```
# Serveurs RDEM Systems
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst

# Fallback
pool 0.fr.pool.ntp.org iburst

driftfile /var/lib/chrony/drift
makestep 1.0 3
logdir /var/log/chrony
```

Commandes utiles

```
chronyc tracking        # État de synchronisation
chronyc sources -v      # Liste des sources
chronyc sourcestats     # Statistiques
sudo chronyc makestep   # Correction immédiate
```

systemd-timesyncd (simple)

Configuration `/etc/systemd/timesyncd.conf` :

```
[Time]
NTP=pool-ntp.rdem-systems.com
FallbackNTP=0.fr.pool.ntp.org 1.fr.pool.ntp.org
```

Activation :

```
sudo systemctl enable --now systemd-timesyncd
timedatectl timesync-status
```

ntpd (legacy)

Configuration `/etc/ntp.conf` :

```
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst
server 0.fr.pool.ntp.org iburst

driftfile /var/lib/ntp/drift
restrict default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict ::1
```

Server vs Peer

Server (directive `server` ou `pool`)

- Source externe de confiance
- Relation client → serveur
- Utilisé pour les sources publiques

Peer (directive `peer`)

- Pair de même niveau de confiance
- Relation bidirectionnelle
- Utilisé entre serveurs internes d'une même organisation

```
Internet (pool.ntp.org)
        |
        v
   [NTP Server 1] <--peer--> [NTP Server 2]
        |                          |
        v                          v
   [Clients]                  [Clients]
```

Environnements virtualisés

Problématique

Les VMs peuvent recevoir l'heure de deux sources conflictuelles :

1. **Hyperviseur** (VMware Tools, Hyper-V, QEMU Guest Agent)
2. **NTP** (configuration système)

Recommandation

Désactivez la synchronisation hyperviseur et utilisez NTP uniquement.

Hyperviseur	Commande
VMware	`vmware-toolbox-cmd timesync disable`
Hyper-V	`Disable-VMIntegrationService -VMName "VM" -Name "Time Synchronization"`
KVM/QEMU	Retirer `kvmclock` ou `clocksource=tsc` au noyau

Exception : VMs suspendues/reprises fréquemment → garder hyperviseur pour corrections importantes.

Sécurité NTP

Risques

- **Amplification DDoS** : NTP exploité pour attaques par réflexion
- **Manipulation du temps** : Invalidation de certificats, contournement de protections

Bonnes pratiques

Pare-feu (client uniquement)

```
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT
iptables -A INPUT -p udp --sport 123 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp --dport 123 -j DROP
```

Chrony (désactiver accès distant)

```
# /etc/chrony/chrony.conf
cmdport 0
bindcmdaddress 127.0.0.1
bindcmdaddress ::1
```

Sources multiples

Configurez **au moins 4 sources** pour détecter les serveurs malveillants (Byzantine fault tolerance : 3f+1 serveurs pour tolérer f compromis).

Dépannage

Symptôme	Cause probable	Solution
“No server suitable”	Pare-feu bloquant UDP 123	Vérifier iptables/firewalld
Offset important	Premier démarrage	`chronyc makestep`
Reach = 0	Serveur injoignable	Vérifier DNS et connectivité
Stratum 16	Non synchronisé	Vérifier configuration sources

```
ntpdate -q pool.ntp.org      # Test connectivité
dig +short 0.fr.pool.ntp.org # Test DNS
nc -vzu pool.ntp.org 123     # Test UDP 123
```

Références

- RFC 5905 – Network Time Protocol Version 4
- NTP Pool Project : https://www.ntppool.org
- Chrony Documentation : https://chrony.tuxfamily.org/documentation.html
- Microsoft W32Time : https://docs.microsoft.com/windows-server/networking/windows-time-service/

RDEM Systems – Expertise systèmes et infrastructures critiques

- Contact : ntp@rdem-systems.com
- Site web : https://ntp.rdem-systems.com
- Contribution NTP Pool : https://www.ntppool.org/a/rdem-systems (AS206014)

Audit, design et support NTP avancé sur demande.