



# Notes

<a href="#">⌚ Date de création</a>	@2 mai 2025 15:04
<a href="#">☰ Étiquettes</a>	

[Serveur de Temps](#)

[À quoi sert un serveur de temps sur Linux ?](#)

[Ouvrir le port UDP 123 \(NTP\) dans le \*\*security group AWS\*\*](#)

[Exemple chrony.conf pour l'Europe](#)

[DNS bind](#)

[Structure des fichiers](#)

[Variables nécessaires](#)

[Résultat de script](#)

[Commandes utiles](#)

[Debug du DNS Publique](#)

[Changement d'IPv4 publique](#)

[FTP](#)

[Changement d'Ipv4 publique](#)

[Se connecter au serveur web en tant que client](#)

[Connexion navigateur](#)

[Changement dns par le notre](#)

[Sites accessibles](#)

[Mysql & PhpMyAdmin](#)

[Samba](#)

[Se connecter en tant qu'user](#)

[Procédure pour se connecter en tant que Guest sur le partage public](#)

[Déployer les scripts](#)

[Ajouter une IP à une instance](#)

[NMAP](#)

[ServerWeb](#)

[DNS+NTP](#)

[Backend](#)

[Admin-backup](#)

# Serveur de Temps

Critère	Chrony	NTP ( <code>ntpd</code> )	<code>systemd-timesyncd</code>
🔧 Type	Client/Serveur	Client/Serveur	Client uniquement
🚀 Précision	Très élevée (μs)	Bonne (ms)	Moyenne (secondes)
💻 Environnement recommandé	Serveurs, machines virtuelles	Réseaux anciens/stables	Desktops, systèmes légers
⚡ Temps de convergence	Très rapide	Lent	Moyen
🔒 Sécurité	Plus moderne, sandboxé	Ancienne base de code	Intégré à systemd
🛠 Configuration	Flexible et simple	Plus complexe	Minimaliste
🕒 Correction temps réel	Oui, même avec mauvaise connec.	Moins efficace	Oui, mais basique
📍 Serveur NTP intégré	Oui	Oui	Non
📦 Paquet	chrony	ntp	Inclus avec systemd

## How to serve the Network Time Protocol with Chrony

timesyncd and timedatectl will generally do the right thing in keeping your time in sync. However, if you also want to serve NTP information then you need an NTP server. Between chrony, the now-dep...

🔗 <https://documentation.ubuntu.com/server/how-to/networking/serve-ntp-with-chrony/index.html>



## À quoi sert un serveur de temps sur Linux ?

Un **serveur de temps** permet de **synchroniser l'horloge système** avec une **source de temps précise** (souvent un serveur NTP – Network Time Protocol). Cela garantit que l'heure est correcte, ce qui est **essentiel** pour :

- les **logs** système et réseau (pour diagnostiquer des erreurs ou corrélérer des événements),
- les **certificats SSL/TLS** (dates d'expiration, validation),
- les **bases de données** (timestamps cohérents),
- la **sécurité** (authentification basée sur l'heure),

## Ouvrir le port UDP 123 (NTP) dans le security group AWS

- Protocole : **UDP**
- Port : **123**
- Source : l'IP de ton sous-réseau AWS (ex : `10.0.0.0/16`)

## Exemple `chrony.conf` pour l'Europe

```
server 0.europe.pool.ntp.org iburst
server 1.europe.pool.ntp.org iburst
server 2.europe.pool.ntp.org iburst
server 3.europe.pool.ntp.org iburst
```

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

- `iburst` - accélère la première synchronisation après le démarrage.  
Envoie plusieurs requêtes d'un coup (au lieu d'attendre plusieurs minutes).
- `makestep 1.0 3` - Corrige immédiatement l'heure si l'écart est trop grand au démarrage.
  - `1.0` → seuil : si l'heure système est décalée de plus de **1 seconde**, Chrony peut "faire un saut" (step).
  - `3` → autorisé seulement pour les 3 premiers ajustements après le lancement du service.
- `rtcsync` - synchronise l'horloge matérielle de BIOS (RTC) avec l'heure système
- `driftfile /var/lib/chrony/drift` Enregistre le taux de dérive de l'horloge locale.
- `logdir /var/log/chrony` - précise l'endroit de stockage de logs

## DNS bind

### Structure des fichiers

```
/etc/named.conf           ← Fichier principal de config BIND
/var/named/forward.NAME.lan   ← Fichier de zone directe (nom → IP)
/var/named/reverse.NAME.lan    ← Fichier de zone inverse (IP → nom)
/var/named/keys                ← (Facultatif) Clés DNSSEC
```

### Variables nécessaires

```
DNS_DOMAIN="tomananas.lan"
VPC_PUBLIC_SUBNET_CIDR="172.31.0.0/20"
REVERSE_ZONE="31.172.in-addr.arpa"
ZONE_DIR="/var/named"
DNS_SERVER_IP="172.31.5.243"
WEB_SERVER_NAME="www"
WEB_SERVER_IP="172.31.5.170"
```

### Résultat de script

```
# /etc/named.conf

options {
    directory "/var/named";
    allow-query { any; };
    # allow-recursion { 127.0.0.1; 172.31.0.0/20; };
    recursion yes;
    dnssec-validation auto;
```

```

};

dnssec-policy "default-policy" {
    keys {
        ksk lifetime P10Y algorithm RSASHA256;
        zsk lifetime P1Y algorithm RSASHA256;
    };
};

zone "tomananas.lan" IN {
    type master;
    file "forward.tomananas.lan";
    dnssec-policy "default-policy";
    inline-signing yes;
};

```

```

# /var/named/forward.tomananas.lan

$TTL 86400
@ IN SOA ns1.tomananas.lan. admin.tomananas.lan. (
    2024050201 ; Serial
    3600      ; Refresh
    604800    ; Expire
    86400     ; Minimum TTL
ns1 IN A 172.31.5.243
www IN A 13.49.221.174
titi IN A 13.49.221.174
tutu IN A 13.49.221.174
web-ftp-01 IN A 172.31.10.47
mysql-mail-04 IN A 172.31.7.29
backup-01 IN A 172.31.11.182
dns-ntp-01 IN A 172.31.5.243

```

```

# /var/named/reverse.tomananas.lan

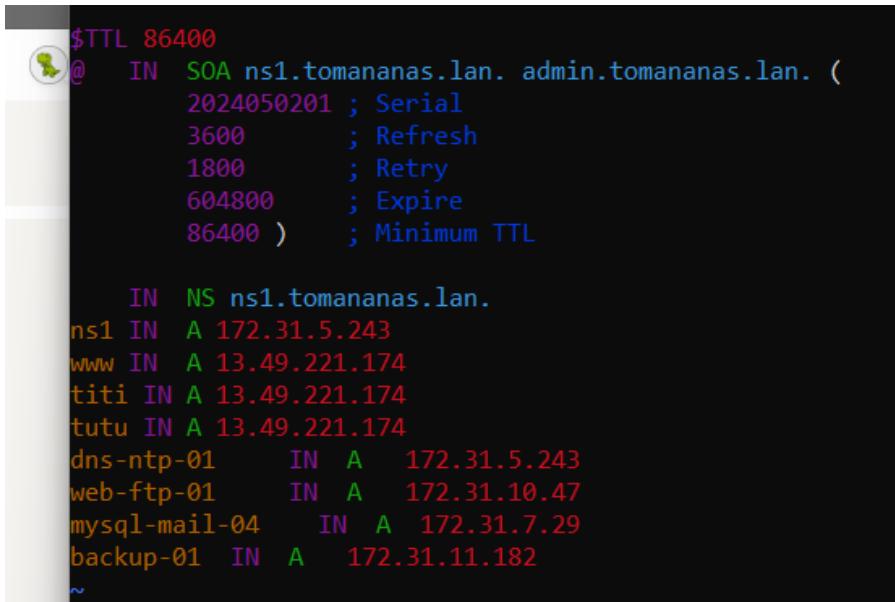
$TTL 86400
@ IN SOA ns1.tomananas.lan. admin.tomananas.lan. (
    2024050201 ; Serial
    3600      ; Refresh
    1800      ; Retry
    604800    ; Expire
    86400     ; Minimum TTL

    IN NS      ns1.tomananas.lan.

172.31.5.243 IN PTR ns1.tomananas.lan.

```

```
13.53.136.242 IN PTR www.tomananas.lan.
```



```
$TTL 86400
@ IN SOA ns1.tomananas.lan. admin.tomananas.lan. (
    2024050201 ; Serial
    3600        ; Refresh
    1800        ; Retry
    604800      ; Expire
    86400 )     ; Minimum TTL

    IN NS ns1.tomananas.lan.
ns1 IN A 172.31.5.243
www IN A 13.49.221.174
titi IN A 13.49.221.174
tutu IN A 13.49.221.174
dns-ntp-01    IN A 172.31.5.243
web-ftp-01    IN A 172.31.10.47
mysql-mail-04  IN A 172.31.7.29
backup-01     IN A 172.31.11.182
~
```

## Commandes utiles

```
# Après un changement dans config bind
rm -f /var/named/forward.tomananas.lan.signed
rm -f /var/named/forward.tomananas.lan.jbk
systemctl restart named
```

## Debug du DNS Publique

16.171.69.125 = ip publique du serveur dns, à modifier au changement d'ip !

```
nslookup tutu.tomananas.lan 16.171.69.125
```

```
Serveur : UnKnown
Address: 16.171.69.125
```

```
Nom : tutu.tomananas.lan
Address: 13.53.136.242
```

## Changement d'IPv4 publique

- modifier enregistrement A dans /var/named/forward.tomananas.lan
- supprimer anciens fichiers signés
- redémarrer le service named

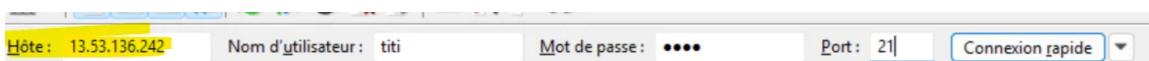
## FTP

## Changement d'Ipv4 publique

- Récupération de l'ip publique de l'instance web-ftp dédiée
- Connexion ssh à l'instance
- Modification dans `/etc/vsftpd/vsftpd.conf` de la variable `pasv_address=x.x.x.x` avec ip publique
- systemctl restart/reload vsftpd

## Se connecter au serveur web en tant que client

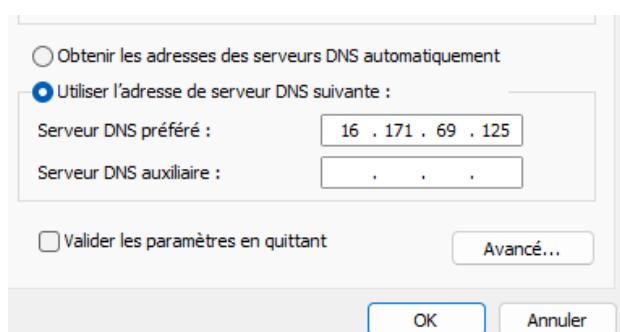
- Récupération de l'ip publique
- Entrer user/password port 21



## Connexion navigateur

### Changement dns par le notre

Modifier le dns préféré windows par notre ip publique de dns



## Sites accessibles

taper url dans navigateur <http://client.tomananas.lan>

## Mysql & PhpMyAdmin

Déployer en utilisant `setup_mysql.sh`

Accessible après sur `http://<adresse_IP_publique>/phpmyadmin"`

## Samba

### Se connecter en tant qu'user

- Linux

```
sudo yum install -y samba-client cifs-utils
# Lister les partages dispo
smbclient -L //<SERVER_IP> -U <username>
```

```
smbclient //<SERVER_IP>/public -U <username>

smb>
commandes dispo dans samba:
ls    # lister
cd dir  # changer de répertoire
get file # télécharger un fichier
put file # envoyer un fichier
```

- Windows
  1. Win+R \\10.42.0.207\www ou \\10.42.0.207\public
  2. Autre → mettre login, mdp (si impossible à cause de l'historique, stop et start workstation)

## Procédure pour se connecter en tant que Guest sur le partage public

- Windows
  - Win+R **regedit**
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
  - Nouveau → Valeur DWORD 32 bits**
  - Nom : AllowInsecureGuestAuth, valeur - 1
  - ```
net stop workstation
net start workstation
net use \\10.42.0.177\public /user:guest /persistent:no
```

- Linux

```
smbclient //10.42.0.177/public -U guest -N
```

## Déployer les scripts

Problèmes parfois avec des encodages windows (\r à la fin des lignes)

Alors exécuter ceci:

```
sudo yum install -y dos2unix # ou dnf install -y dos2unix
dos2unix script.sh
```

## Ajouter une IP à une instance

- EC2 → **Instances**
- Instance → onglet "**Networking**"
- Cliquer sur l'**interface réseau (ENI)** liée à l'instance
- Dans l'écran de l'ENI :
  - Actions → "**Manage IP addresses**"

- Cliquer sur "Assign new private IP"
- Entre l'IP souhaitée
- Save et run ça sur la machine:

```
ip addr add 10.42.0.96/24 dev ens5
```

## NMAP

Script de scan tcp des ports des serveurs:

```
for ip in 10.42.0.87 10.42.0.37 10.42.0.113 10.42.0.170; do
  echo "==== Scan $ip ==="
  nmap -Pn -p- --min-rate=1000 -oA scans/${ip}-allports $ip
done
```

## ServerWeb

```
==== Scan 10.42.0.87 ===
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-13 20:47 CEST
Nmap scan report for 10.42.0.87
Host is up (0.00029s latency).

Not shown: 65401 filtered tcp ports (no-response), 71 filtered tcp ports (host-unreach), 53 closed
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
19999/tcp open  dnp-sec
20048/tcp open  mountd
```

## DNS+NTP

```
==== Scan 10.42.0.37 ===
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-13 20:49 CEST
Nmap scan report for 10.42.0.37
Host is up (0.00022s latency).

Not shown: 65456 filtered tcp ports (no-response), 76 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
19999/tcp open  dnp-sec
```

## Backend

```
==== Scan 10.42.0.170 ====
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-13 20:51 CEST
Nmap scan report for 10.42.0.170
Host is up (0.00028s latency).

Not shown: 65451 filtered tcp ports (no-response), 80 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
19999/tcp open  dnp-sec
```

## Admin-backup

```
==== Scan 10.42.0.113 ====
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-13 20:51 CEST
Nmap scan report for 10.42.0.113
Host is up (0.00019s latency).

Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
19999/tcp open  dnp-sec
```