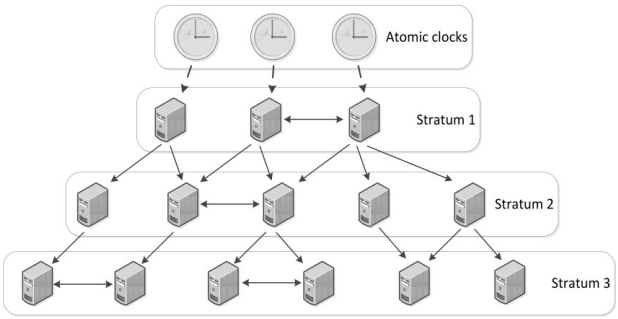
Création d'un serveur de temps (NTP)

1) Présentation du protocole NTP



Le protocole NTP (Network Time Protocol) permet de synchroniser l'horloge locale d'une machine (date et heure) avec une machine de référence appelée serveur NTP. Il existe des dizaines de serveurs NTP librement accessible dans le monde entier, mais on peut créer soit même son serveur NTP (qui se synchronisera lui aussi sur un autre serveur de temps).

NTP utilise le port 123 en UDP. C'est important à savoir (pour les règles de pare-feu 😉).

Avec NTP, tous les ordinateurs Windows et Linux mais aussi d'autres machines comme les routeurs, les commutateurs, les imprimantes, les pare-feux, les bornes Wi-Fi, etc, sont toujours à l'heure et, surtout, à la même heure.

C'est essentiel car :

- cela évite les problèmes d'authentification : en effet il y a souvent une durée de validité dans les jetons d'authentification (ex : Active Directory) et en cas de décalage important de l'horloge des blocages réseaux et systèmes peuvent se produire
- pour les fichiers logs (journaux), les évènements sont horodatés. Donc si 2 événements liés, provenant de deux machines différentes, ont des horaires différents, il ne sera pas facile de déterminer à quelle date et horaire exact l'événement à réellement eu lieu.

2) Sources de temps (serveurs de référence)

La saisie manuelle de l'horloge n'est pas recommandée. Il est préférable de synchroniser l'horloge sur un serveur NTP. Il faut juste choisir le serveur de référence, par exemple, le serveur de temps offert par l'université de Nice :

FQDN : ntp.unice.fr (adresse IP : 134.59.1.5)

On peut généralement spécifier plusieurs serveurs NTP. Il est recommandé de choisir des serveurs de temps français ou européens.

Remarque : une machine ayant rejoint un domaine Active Directory voit son horloge se synchroniser avec l'horloge du serveur contrôleur de domaine. C'est donc sur le serveur qu'il faut régler correctement l'heure.

3) Configuration de l'horloge sur les machines (pour information)

Les méthodes ci-après permettent de configurer le client NTP pour qu'il synchronise l'horloge sur un serveur NTP externe sur Internet (méthode rapide et efficace) ou sur un serveur NTP interne géré par nous-même (méthode plus professionnelle). La seule différence sera juste l'utilisation d'une IP publique (NTP disponible sur Internet) ou d'une IP privée (donc notre serveur NTP local → cf. partie 4).

Sur Windows

- Réglage manuel :
  dans « Heure et langue » des paramètres Windows.

- Réglage via NTP :
  Panneau de configuration, date et heure, configurer date et heure, bouton Temps Internet, changer les paramètres.

  Ou alors via Powershell.

Sur Linux

- Voir la date et l'heure :
  date
- Pour faire un réglage manuel :
  date -s 09:33:45
  date -s 30/09/2022

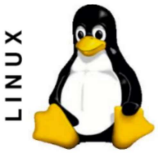
- Pour faire un réglage automatique vers des serveurs NTP proposés par Debian :
  apt update
  apt install chrony
- Ensuite, redémarrage du service :
  systemctl restart chrony
- Pour voir les serveurs NTP utilisés :
  chronyc sources

Sur Cisco

- Voir la date et l'heure :
  #show clock
- Réglage manuel :
  #clock set 09:33:45 Sep 20 2022

- Réglage via NTP :
  (config)# ntp server *adresseIPserveurNTP*
- Pour voir la configuration NTP :
  #show ntp status

4) Créer son propre serveur de temps NTP pour fournir un service en interne



NTP
Network Time Protocol

Créer son propre serveur de temps est la solution idéale pour fournir une horloge précise aux postes du réseau local sans que chacun aille sur Internet pour la synchronisation. L'objectif est que seul ce serveur soit autorisé à se synchroniser sur un serveur de temps NTP sur Internet et que toutes les machines locales se synchronisent sur ce serveur NTP interne.

Etapes de création d'un serveur NTP interne sur Linux
(machine : ntp.architek.com ; IP : 172.17.255.253)

- Installation de Chrony (service de temps) :
```
apt update
apt install chrony
```
- Configuration des serveurs de référence pour notre serveur de référence :
```
nano /etc/chrony/chrony.conf
```
Commenter le pool de serveurs déjà présent, puis ajouter la ligne ordonnant de se synchroniser sur un serveur NTP, par exemple celui de l'université de Nice :
```
server ntp.unice.fr iburst
```
Attention, étant donné qu'on utilise un FQDN, il faut qu'un serveur DNS soit disponible pour faire la résolution d'adresse (celui de Google -8.8.8.8- le fera très bien). Cela se paramètre dans le fichier /etc/resolv.conf

Ensuite, autoriser tout le monde à se synchroniser sur notre serveur (©Bader,Maksim) en ajoutant la ligne suivante :
```
allow 0.0.0.0/0
```
- Redémarrage du service :
```
systemctl restart chrony
```
- Vérification (on doit voir qu'on est synchronisé avec le NTP de unice.fr) :
```
chronyc sources
```
- Détails sur le serveur NTP vers lequel on est synchronisé :
```
chronyc tracking
```

Ensuite, sur les postes clients, il faudra préciser l'adresse IP de ce serveur NTP interne afin que les machines clientes synchronisent leur horloge avec le serveur.

Etapes de configuration d'un client NTP Linux
(machine : haproxy.architek.com ; IP : 172.16.0.1)

- Configuration du serveur vers lequel synchroniser l'horloge :
```
nano /etc/systemd/timesyncd.conf
```
Puis décommenter la ligne ordonnant de se synchroniser sur le serveur NTP de l'entreprise :
```
NTP=ntp.architek.com
```
Attention, étant donné qu'on utilise un FQDN, il faut qu'un serveur DNS soit disponible pour faire la résolution d'adresse (par exemple le serveur DNS qui gère la zone architek.com ; si on ne peut pas y avoir accès, il faudra créer un enregistrement dans le fichier « /etc/hosts » avec la valeur suivante : « 172.17.255.253 ntp.architek.com »).
- Redémarrage du service
```
systemctl restart systemd-timesyncd
```
- Vérification (on doit voir qu'on est synchronisé avec notre NTP interne à nous 😊) :
```
timedatectl timesync-status
```

Etapes de configuration d'un client NTP Windows en PowerShell
(machine : srv-ad.architek.com ; IP : 10.X.40.1)

1. Exécuter PowerShell en administrateur
2. Arrêter le service de temps :
```
net stop w32time
```
3. Synchroniser avec le serveur NTP interne :
```
w32tm /config /syncfromflags:manual /manualpeerlist:"ntp.architek.com"
w32tm /config /reliable:yes
```
Comme on utilise ici le FQDN ntp.architek.com, il faut créer un enregistrement de type A (dans le serveur DNS Windows Server) pour faire pointer le nom vers l'adresse IP du serveur NTP interne 😉.
4. Démarrer le service de temps :
```
net start w32time
```
5. Vérifier la synchronisation :
```
w32tm /query /status
```
6. Forcer une synchronisation :
```
w32tm /resync /force
```
7. Revérifier la synchronisation (on doit voir l'adresse source du serveur NTP interne) :
```
w32tm /query /status
```

Les machines clientes du domaine seront synchronisées avec le serveur contrôleur de domaine (AD). Pour les machines « hors domaine », il faudra synchroniser manuellement l'horloge (via les paramètres ou PowerShell).