

Table des matières

Public : personnels opérant des serveurs

Journaux

Les journaux (ou *logs*) sont à garder un an minimum et un an maximum. Ils doivent permettre au moins deux choses :

- identifier quel client se connecte (adresse IP)
- identifier quel utilisateur se connecte (lorsque cela a un sens)

Il s'agit *a minima* de pouvoir répondre à une requête judiciaire. Les connexions d'utilisateurs se comprennent surtout dans le cas de modifications (accès administrateur par exemple, par RDP, WinRM ou SSH par exemple).

Le protocole habituellement utilisé est [Syslog](#). Sous Linux, c'est le protocole natif. Sous Windows, [NXlog](#) par exemple est très bien.

NB : l'horodatage des messages de journalisation est indispensable. Si les messages ne sont pas correctement horodatés, leur exploitation est difficile. Il faut donc s'assurer que le système est bien [mis à l'heure par NTP](#).

La DSI a un serveur dédié à la centralisation des journaux. Pour enregistrer les journaux d'un serveur, contacter assistance@cnam.fr en mentionnant le serveur émetteur, son rôle, ses principaux *daemons* ou services et qui l'administre.

From:
<https://assistancedsi.cnam.fr/> - Assistance DSI

Permanent link:
<https://assistancedsi.cnam.fr/srv/syslog>

Last update: **2024/10/16 14:54**

