```
Auteur: SRIKANTHAN Sabiran
```

C’est quoi un log et à quoi ça sert ?

Un log, c’est simplement un fichier texte où le système note tout ce qu’il se passe : connexions, erreurs, sites visités, tentatives d’accès… Chaque ligne représente un événement avec la date et l’heure.

Pourquoi c’est utile :

- Voir qui s’est connecté, quand et à quoi
- Repérer les bugs ou pannes
- Surveiller les accès non autorisés
- Respecter la loi en gardant une trace de l’activité réseau

Où sont stockés les logs dans ALCASAR ?

ALCASAR enregistre les logs à deux endroits principaux :

- `/var/log/` : pour les services, le système, le portail captif
- `/var/Save/` : pour les sauvegardes, archives et autres fichiers spécifiques à ALCASAR

Détail du dossier `/var/Save/`

`/var/Save/activity_report/`

Contient des rapports générés automatiquement (HTML ou CSV) sur l’activité du réseau : qui s’est connecté, combien de données ont circulé, etc.

`/var/Save/archive/`

Stocke les anciens logs compressés (`.gz` , `.tar`) pour pouvoir les consulter plus tard si besoin.

`/var/Save/base/`

Contient des fichiers techniques (bases de données par exemple) utilisés en interne par ALCASAR.

`/var/Save/iot_captures/`

Ce sont des enregistrements du trafic réseau lié aux objets connectés (IoT), pour les analyser si besoin.

`/var/Save/security/`

Contient des fichiers essentiels liés à la sécurité :

Fichier	À quoi ça sert
`acc_access.log`	Liste des accès (adresse IP, utilisateur, site consulté, réponse HTTP)
`acc_access.log.1.gz`	Ancienne version du log précédent, compressée
`watchdog.log`	Surveillance des services (s'ils plantent ou redémarrent)

Détail du dossier `/var/log/`

Dossier ou fichier	Ce qu'il enregistre
`/var/log/radius/`	Connexions des utilisateurs au portail captif
`/var/log/e2guardian/`	Sites visités et filtrés (bloqués ou autorisés) si configuré
`/var/log/firewall/`	Ce qui passe ou est bloqué par le pare-feu
`/var/log/lighttpd/`	Accès au portail captif et à l'interface web
`/var/log/ulogd/`	Trafic réseau entrant et sortant
`/var/log/vnstat/`	Statistiques de bande passante
`/var/log/fail2ban.log`	IP bannies après trop de tentatives ratées si configuré
`/var/log/auth.log`	Accès administratifs (SSH, sudo)
`/var/log/php-fpm/`	Erreurs liées au traitement PHP
`/var/log/mysqld/`	Activité de la base de données utilisateurs
`/var/log/unbound/`	DNS local : résolution des noms de domaine pour les utilisateurs filtrés.
`var/log/ulogd`	Journalisation réseau avancée (netfilter + ulogd pour les connexions IP/MAC).
`/var/log/firewall/traceability.log`	Contient seulement des adresses IP, pas de noms de domaine. on dois faire une résolution DNS inverse

Types de logs selon leur usage

Connexions (authentification)

- `/var/log/radius/radius.log` : qui s'est connecté, avec quelle IP, et si ça a marché ou non

Navigation Internet

- `/var/log/e2guardian/access.log` : sites consultés, adresse IP de l'utilisateur, filtres appliqués

Sécurité

- `/var/log/fail2ban.log` : IP bannies après des échecs de connexion
- `/var/log/auth.log` : connexions SSH et actions sudo
- `/var/log/firewall/` : trafic réseau bloqué ou autorisé

Trafic réseau

- `/var/log/ulogd/` : détails sur les paquets réseau
- `/var/log/vnstat/` : volumes de données échangées

Portail captif

- `/var/log/lighttpd/access.log` : accès à la page d'identification
- `/var/log/php-fpm.log` : erreurs du backend PHP

Commandes utiles pour lire les logs

Action recherchée	Commande à exécuter
Voir les 50 dernières connexions	`tail -n 50 /var/log/radius/radius.log`
Rechercher un utilisateur	`grep 'nom_utilisateur' /var/log/radius/radius.log`
Rechercher les sites bloqués	`grep DENIED /var/log/e2guardian/access.log`
Suivre les accès en direct (live)	`tail -f /var/log/lighttpd/access.log`
Voir les adresses IP bannies	`cat /var/log/fail2ban.log`
Consulter les logs d'erreur PHP	`less /var/log/php-fpm.log`
Vérifier l'activité du pare-feu	`less /var/log/firewall/*`
Voir les statistiques de bande passante	`vnstat` ou `cat /var/log/vnstat/<interface>`

Comment les logs sont archivés

Pour éviter que les fichiers ne deviennent trop gros, ALCASAR utilise `logrotate`. Il compresse les anciens fichiers automatiquement :

- `.log.1` → version précédente
- `.log.2.gz` → encore plus ancien, compressé

Faire une archive manuellement :

```
tar czvf /root/logs_alcasar.tar.gz /var/log/radius
/var/log/e2guardian /var/log/firewall
```

Tous les fichiers importants sont aussi copiés chaque semaine dans `/var/Save/` grâce à un script automatique.