

# Synchronizer - Les logs d'activité des utilisateurs ( authentication et session )

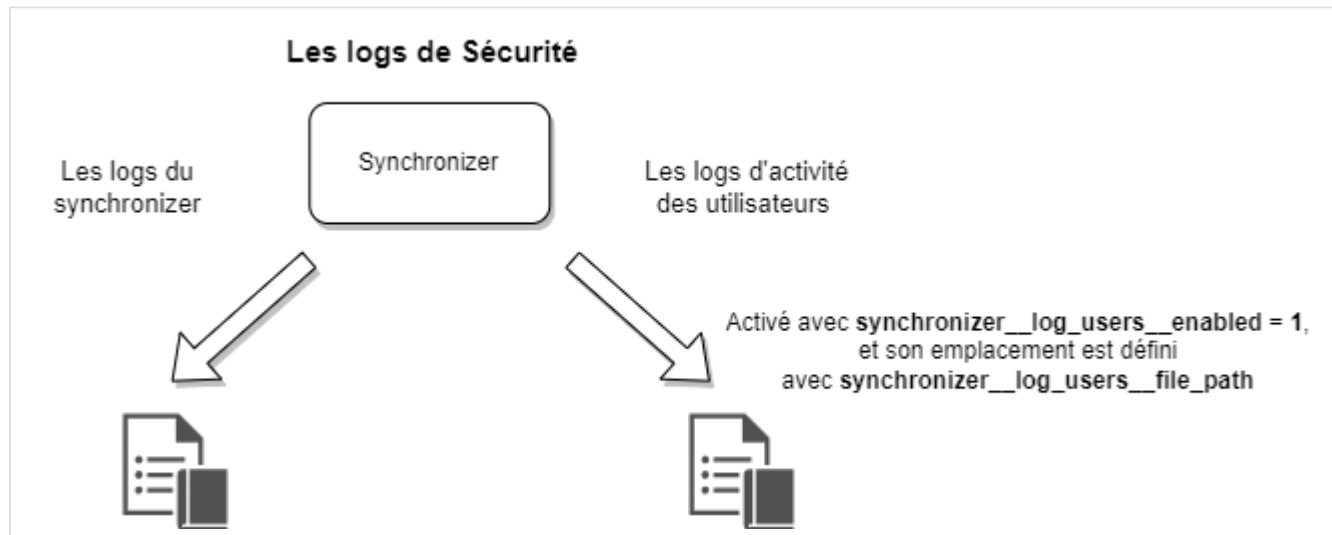
## Sommaire

[Contexte](#)  
[Mise en place](#)  
[Log d'Authentification](#)  
    [Authentification Réussi](#)  
    [Authentification Échoué](#)  
    [Déconnexion](#)  
[Log de Session](#)

## Contexte

Il est possible d'activer des logs de suivis de l'activité des utilisateurs dans un fichier spécifique.

- Ce sont des logs d'authentification et de sessions supplémentaires.
- Cela vous permet d'accéder à ces informations sans devoir parser le fichier des logs du Synchronizer.
  - Vous pourrez, par exemple, envoyer ce fichier à votre équipe de sécurité pour un audit.



## Mise en place

Cette option peut être activée grâce à l'option `synchronizer__log_users__enabled`, dans le fichier de configuration `/etc/shinken/synchronizer.cfg` ( voir la page [Paramètres globaux \( synchronizer.cfg \)](#) ).

- Par défaut, les logs seront écrits dans le fichier `/var/log/shinken/synchronizer/log_users.log`.
  - Cet emplacement peut être modifié via l'option `synchronizer__log_users__file_path`.
- Vous pouvez aussi activer l'option `synchronizer__log_users__add_user_name` pour que le nom des utilisateurs soit affiché dans les logs.
- Vous pouvez aussi modifier l'option `synchronizer__log_users__logs_rotation__nb_days_before_deletion` pour modifier la durée de rotation en jours des fichiers de logs.

## Log d'Authentification

### Authentification Réussi

Si `synchronizer__log_users__add_user_name` est activé :

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGIN ] [ RESULT:200 ] [ TIME:          1ms ] [ USER:<user_uuid> /  
<user_name> ] [ CALL_BY:<IP> ] [ AUTHENTICATED:OK ] [ BY:UI Configuration ] [ AUTHENTICATED BY THE  
MODULE:<module_name> ]
```

Sinon:

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGIN ] [ RESULT:200 ] [ TIME:          1ms ] [ USER:<user_uuid> ] [ CALL_BY:<IP> ] [ AUTHENTICATED:OK ] [ BY:UI Configuration ] [ AUTHENTICATED BY THE MODULE: <module_name> ]
```

## Authentification Échoué

Si `synchronizer__log_users__add_user_name` est activé :

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGIN ] [ RESULT:401 ] [ TIME:          4ms ] [ USER:<user_uuid> / <user_name> ] [ CALL_BY:<IP> ] [ AUTHENTICATED:FAILED ] [ BY:UI Configuration ]
```

Sinon:

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGIN ] [ RESULT:401 ] [ TIME:          4ms ] [ USER:<user_uuid> ] [ CALL_BY:<IP> ] [ AUTHENTICATED:FAILED ] [ BY:UI Configuration ]
```

## Déconnexion

Si `synchronizer__log_users__add_user_name` est activé :

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGOUT ] [ RESULT:200 ] [ TIME:          0ms ] [ USER:<user_uuid> / <user_name> ] [ CALL_BY:<IP> ] [ BY:UI Configuration ]
```

Sinon:

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ LOGOUT ] [ RESULT:200 ] [ TIME:          0ms ] [ USER:<user_uuid> ] [ CALL_BY:<IP> ] [ BY:UI Configuration ]
```

## Log de Session

Un log de session est généré à chaque fois qu'un utilisateur démarre **une nouvelle session**.

- **Une nouvelle session** est créée à chaque fois qu'un utilisateur ferme et rouvre son navigateur sur l'UI de configuration.
- Lors d'une authentification via la page d'authentification il ne sera pas créé de log de session, uniquement un log d'authentification.

Si `synchronizer__log_users__add_user_name` est activé :

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ SESSION ] [ RESULT:--- ] [ TIME:          0ms ] [ USER:<user_uuid> / <user_name> ] [ CALL_BY:<IP> ] [ BY:UI Configuration ] [ ALREADY AUTHENTICATED USERS, START A SESSION ]
```

Sinon:

```
[ YYYY-MM-DD HH:MM:SS ] [ READ ] [ SESSION ] [ RESULT:--- ] [ TIME:          0ms ] [ USER:<user_uuid> ] [ CALL_BY:<IP> ] [ BY:UI Configuration ] [ ALREADY AUTHENTICATED USERS, START A SESSION ]
```