

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

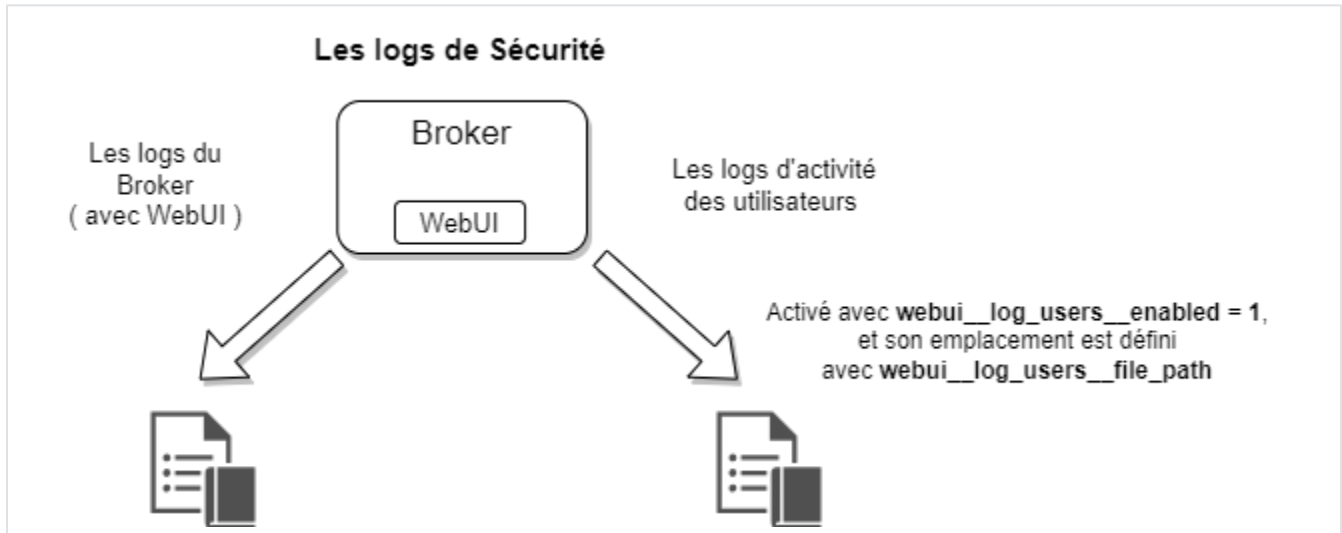
Sommaire

- Contexte
- Mise en place
- Log Externe 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 Broker.
 - 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 `webui__log_users__enabled`, dans le fichier de configuration `/etc/shinken/modules/webui cfg` (voir la page [Module WebUI](#)).

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

Log Externe d'Authentification

Authentification Réussi

Si `webui__log_users__add_user_name` est activé:

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

Authentification Échoué

Si `webui__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 Visualization:<webui_name> ]
```

Sinon:

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

Déconnexion

Si `webui__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 Visualization:<webui_name> ]
```

Sinon:

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

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 Visualisation.
- Pas de log de session créé lors d'une authentification via la page d'authentification, uniquement le log d'authentification sera créé.

Si `webui__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 Visualization:<webui_name> ] [ 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 Visualization:<webui_name> ] [ ALREADY AUTHENTICATED USERS, START A SESSION ]
```