Authentic 2 - Support #45976

Logs adaptés pour mise en place de fail2ban

20 août 2020 15:56 - Benjamin Renard

Statut:	Nouveau	**Début:**	20 août 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Nous avons cherché à mettre en œuvre fail2ban pour bloquer les tentatives d'attaque par force brute sur une installation d'A2, mais les logs qu'il émet ne sont pas adaptés en l'état :

- nous avons plusieurs blocs d'auth LDAP configurés et nous nous retrouvons, pour une même tentative de connexion, avec plusieurs lignes de logs en échec/succès :
    - Log d'une tentative de connexion avec des identifiants invalides :

```
Aug 20 15:12:36 sso-02 authentic2[19596]: 10.22.0.6 - ddc941ff INFO user 5775 failed to login
Aug 20 15:12:36 sso-02 authentic2[19596]: 10.22.0.6 - ddc941ff INFO user uid=5775,ou=people~~ fail
ed to login
```

    - Log d'une tentative de connexion avec des identifiants valides :

```
Aug 20 07:16:13 sso-02 authentic2[21957]: 192.168.3.250 - 5ec1fd1b INFO user mon failed to login
Aug 20 07:16:13 sso-02 authentic2[21957]: 192.168.3.250 mon (18a689) 5ec1fd1b INFO logged in (pass
word-on-https)
```

- nous avons aucune ligne de logs si la tentative portait sur un identifiant d'utilisateur inexistant

En regardant le code, j'ai vu un mécanisme utilisé pour compter le nombre de tentatives de connexions en échec (authentic2.user_login_failure), mais visiblement celui-ci est aussi sensible au cas avec plusieurs sources d'authentification : il semble appelé pour chaque bloc d'authentification en échec/succès et la clé d'incrémentation ne se base que sur le login (pas le bloc d'auth).