Authentic 2 - Development #50751

Ajout d'une fonctionnalité de suppression automatique des comptes LDAP après disparition dans l'annuaire

01 février 2021 18:07 - Benjamin Renard

Statut:	Nouveau	**Début:**	01 février 2021
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Un de nos clients nous demande de mettre en place une fonctionnalité de suppression des comptes utilisateurs issus de leur annuaire LDAP lorsque ceux-ci ne s'y trouvent plus (lorsqu'il quitte la société par exemple).

J'ai bien noté l'existence de la fonctionnalité de suppression des comptes inutilisés (cron *clean-unused-accounts*), mais celle-ci ne s'y prête pas ici : la gestion du cycle de vie des comptes LDAP n'est pas géré dans Authentic2 chez ce client et Authentic2 n'est que consommateur de la base de comptes LDAP : au même titre qu'il synchronise automatiquement les nouveaux comptes de l'annuaire, ils voudraient qu'il supprime ces comptes lorsqu'ils disparaissent de l'annuaire.

Je pense qu'il serait préférable ici de passer par une étape de marquage du compte pour suppression (comme le fait le cron *clean-unused-accounts*) avant suppression définitive après un laps de temps configurable : cela permettrait d'éviter de virer un compte (et tout son historique) si celui-ci est supprimé par erreur de l'annuaire. Si je ne me trompe pas, un compte marqué pour suppression devrait pouvoir être restauré au besoin ?

Avant de me lancer dans l'implémentation de cette fonctionnalité et comme discuté ensemble, quelle serait vos conseils/demandes particulières à ce sujet pour que mon code sur cette fonctionnalité puisse être intégré upstream à terme ?

Demandes liées:

Lié à Authentic 2 - Development #6379: sync-ldap-users do not remove deleted ...	**Fermé**	**29 janvier 2015**

Historique

#1 - 01 février 2021 18:09 - Frédéric Péters

- Lié à Development #6379: sync-ldap-users do not remove deleted accounts ajouté

#2 - 02 février 2021 11:33 - Benjamin Dauvergne

Il faut continuer la discussion dans le ticket existant pointé par Fred.

#3 - 27 avril 2022 16:53 - Benjamin Renard

Il semble que la fonctionnalité de suppression des comptes LDAP 3 mois après leur désactivation comme imaginer, n'avait pas été implémenté dans https://dev.entrouvert.org/issues/6379. De votre côté, j'ai l'impression que vous aviez bossé sur le script *clean-unused-accounts* : est-ce que celui-ci pourrait prendre en compte les utilisateurs LDAP ? Ou bien faut-il plutôt prévoir un autre script dédié ou faire prendre ça en charge par *deactivate-orphaned-ldap-users* ?

#4 - 10 mai 2022 11:14 - Benjamin Renard

Benjamin Renard a écrit :

> Il semble que la fonctionnalité de suppression des comptes LDAP 3 mois après leur désactivation comme imaginer, n'avait pas été implémenté dans https://dev.entrouvert.org/issues/6379. De votre côté, j'ai l'impression que vous aviez bossé sur le script *clean-unused-accounts* : est-ce que celui-ci pourrait prendre en compte les utilisateurs LDAP ? Ou bien faut-il plutôt prévoir un autre script dédié ou faire prendre ça en charge par *deactivate-orphaned-ldap-users* ?

Je me permets une petite relance sur ce sujet : nous avons une demande client sur le sujet et nous pourrions nous occuper du dev au besoin.

#5 - 10 mai 2022 11:48 - Benjamin Dauvergne

Il y a déjà une suppression des comptes inactifs, il suffit de configurer la durée dans la configuration de la collectivité (ou plutôt unité d'organisation, j'ai toujours du mal avec la traduction qu'on a choisi). Ici ce qui manquerait ce serait une durée explicite (ou alors un paramètre à clean-unused-account) concernant les comptes désactivés explicitement (ceux pour lesquels user.is_active == False).

Je serai ouvert à l'un ou l'autre patch.

#6 - 19 mai 2022 12:59 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Il y a déjà une suppression des comptes inactifs, il suffit de configurer la durée dans la configuration de la collectivité (ou plutôt unité d'organisation, j'ai toujours du mal avec la traduction qu'on a choisi). Ici ce qui manquerait ce serait une durée explicite (ou alors un paramètre à clean-unused-account) concernant les comptes désactivés explicitement (ceux pour lesquels user.is_active False).

Hum, si je comprends bien, *clean-unused-account* s'occupe actuellement de supprimer comptes ne s'étant pas connectés depuis un certain temps. Pour le coup, nous cette suppression ne nous intéresse pas (les comptes étant gérés dans le LDAP, c'est dans le LDAP qu'il devrait être supprimé). C'est bien la suppression des comptes désactivés qui nous intéresse (user.is_active False).

Par ailleurs, à lire le code de ce script, il exclut aujourd'hui explicitement les utilisateurs provenant d'un annuaire LDAP :

```
 67          # exclude user from LDAP directories based on their source name (or realm)
 68          realms = [block['realm'] for block in LDAPBackend.get_config() if block.get('realm')]
 69          self.user_qs = (
 70              get_user_queryset().exclude(oidc_account__isnull=False).exclude(userexternalid__source__in=rea
lms)
 71          )
```

À voir si :

- on conserve cette exclusion pour la partie désactivation des comptes inutilisés et on exclut cette clause que pour la nouvelle partie suppression des comptes désactivés
- si on supprime cette clause dans tous les cas

L'idée du patch serait donc :

- de supprimer (au moins en partie) l'exclusion des comptes LDAP dans le traitement du script *clean-unused-account*
- d'ajouter aux collectivités un paramètre du genre "Nombre de jours avant la suppression des comptes désactivés :" et le rendre éditable via l'interface *manage* d'Authentic.
- de prendre en compte la suppression des comptes désactivés dans le script *clean-unused-account*. À voir, mais on pourrait également imaginer de mettre ça dans un script dédié, surtout si on fait une différence au sujet de l'inclusion ou non des utilisateurs LDAP dans le traitement

> Je serai ouvert à l'un ou l'autre patch.

OK, je pourrais bosser dessus, mettons-nous juste d'accord sur la gestion de cette clause existante d'exclusion des utilisateurs LDAP et sur la création ou non d'un script dédié pour la suppression des comptes désactivés.

#7 - 14 décembre 2022 17:16 - Benjamin Renard

Benjamin Renard a écrit :

> Benjamin Dauvergne a écrit :
>
> > Je serai ouvert à l'un ou l'autre patch.
>
> OK, je pourrais bosser dessus, mettons-nous juste d'accord sur la gestion de cette clause existante d'exclusion des utilisateurs LDAP et sur la création ou non d'un script dédié pour la suppression des comptes désactivés.

J'ai une relance client à ce sujet. Pourrais-tu me donner ton avis sur mes propositions pour l'occupe de coder ça ?