Authentic 2 - Development #6379

sync-ldap-users do not remove deleted accounts

29 janvier 2015 11:41 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	29 janvier 2015
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	future		
Patch proposed:	Oui	**Planning:**	Non

Description

If the external_id cannot be resolved in the LDAP, accounts should be removed. It should be customizable with an option like 'sync_delete': True,

The method LDAPBackend.external_id_to_filter can be used for this.

Demandes liées:

Lié à Publik - Development #26907: Cycle de vie des comptes	**Fermé**	**24 novembre 2020**
Lié à Publik - Development #42388: Ne pas envoyer de mail aux comptes désactivés	**Nouveau**	**02 mai 2020**
Lié à Authentic 2 - Development #50751: Ajout d'une fonctionnalité de suppres...	**Nouveau**	**01 février 2021**
Lié à Authentic 2 - Bug #50966: ajouter la date de desactivation du compte da...	**Fermé**	**09 février 2021**

Révisions associées

Révision 762cba9a - 26 mars 2021 10:05 - Serghei Mihai

ldap: add method and command to deactivate orphaned users (#6379)

Historique

#1 - 06 mars 2015 16:35 - Benjamin Dauvergne

- Version cible mis à future

#2 - 12 février 2019 12:42 - Paul Marillonnet

- Fichier 0001-WIP-ldap_backend-deactivate-accounts-if-ldap-entry-m.patch ajouté

- Statut changé de Nouveau à Information nécessaire

- Patch proposed changé de Non à Oui

Up car discuté ce matin sur le salon.

Pas eu le temps de réfléchir au côté CLI (une nouvelle option pour la commande de synchronisation ? une nouvelle commande à part ?)

Mais, dans l'idée, si on se contentait de désactiver les LDAPUsers dont le nom d'utilisateur n'a pas pu être retrouvé dans le LDAP, on est bon ?

#3 - 12 février 2019 12:43 - Frédéric Péters

> Mais, dans l'idée, si on se contentait de désactiver les LDAPUsers dont le nom d'utilisateur n'a pas pu être retrouvé dans le LDAP, on est bon ?

Les utilisateurs désactivés apparaissent dans le tableau des usagers.

#4 - 12 février 2019 12:50 - Paul Marillonnet

- Fichier 0001-WIP-ldap_backend-deactivate-accounts-if-ldap-entry-m.patch ajouté

Et donc on les supprime, c'est ça (voir le nouveau patch WIP) ?
Est-ce que le comportement le plus souhaitable n'est pas de changer l'affichage des usagers désactivés dans le tableau des usagers ?

#5 - 12 février 2019 15:01 - Benjamin Dauvergne

Les utilisateurs supprimés vont disparaître des historiques w.c.s sans #24430, j'aimerai vraiment que tous les aspects cycle de vie des comptes soit

reliés et discutés sur #26907 qu'on garde toujours un objectif global et qu'on ne traite chaque petit bout sans voir les conséquences.

Ensuite si c'est un problème temporaires (genre l'annuaire a été branché sur une copie vide, les ACLS sont foirées et ldapsearch ne renvoie plus rien) pim pam poum on vide tout, on perd toutes les affectations de rôle, je serai plutôt pour désactiver le compte, et dès qu'on a un compte disparu du LDAP, déjà désactivé et modifié il y a plus de 3 mois, on supprime.

#6 - 12 février 2019 16:04 - Paul Marillonnet

- Lié à Development #26907: Cycle de vie des comptes ajouté

#7 - 12 février 2019 16:07 - Paul Marillonnet

- Fichier 0001-WIP-ldap_backend-process-orphan-accounts-6379.patch ajouté

Ok d'ac. Est-ce que dans l'idée le code convient ?
(Si oui, j'écris les tests et soumet un patch pour relecture.)

#8 - 12 février 2019 16:09 - Paul Marillonnet

Paul Marillonnet a écrit :

> (Si oui, j'écris les tests et soumet un patch pour relecture.)

(Et l'ajout de logs sur la désactivation et la suppression).

#9 - 12 février 2019 16:15 - Benjamin Dauvergne

_deactivated_on ne va pas persister d'un run sur l'autre, c'est pour cela que j'ai proposé de se servir du champ modified qui existe déjà.

#10 - 12 février 2019 16:19 - Benjamin Dauvergne

Mais dans l'idée c'est pas ça du tout, il faut accumuler une liste des external_id_tuples (faut les reconstruire à la volée), extraire celle en base, extraire la première à la deuxième, et les comptes qui reste sont ceux qui sont orphelins; c'est vraiment pas un ticket évident en fait...

#11 - 19 février 2019 09:59 - Paul Marillonnet

Ah bein oui zut, j'avais pas pensé à la persistance d'une exécution à l'autre.
Un ticket faussement facile donc (et je ne me l'assigne pas, pour l'instant au moins).

#13 - 26 janvier 2020 18:53 - Benjamin Dauvergne

- Assigné à Serghei Mihai supprimé

#15 - 02 mai 2020 10:39 - Frédéric Péters

- Statut changé de Information nécessaire à Nouveau

- Patch proposed changé de Oui à Non

Ça serait bien utile, notamment parce qu'on se trouve à continuer à envoyer des mails à des agents dont le compte n'existe plus, et ça peut participer à la mauvaise réputation.

#17 - 02 mai 2020 12:13 - Benjamin Dauvergne

- Lié à Development #42388: Ne pas envoyer de mail aux comptes désactivés ajouté

#18 - 02 mai 2020 12:16 - Benjamin Dauvergne

#41922 (ne plus supprimer les comptes dans w.c.s.) fournissant ce qu'on attendait de #24430 (gérer la suppression coté w.c.s. des comptes supprimés) on peut avancer ici.

#19 - 01 février 2021 18:09 - Frédéric Péters

- Lié à Development #50751: Ajout d'une fonctionnalité de suppression automatique des comptes LDAP après disparition dans l'annuaire ajouté

#20 - 02 février 2021 11:36 - Benjamin Dauvergne

Idée en l'état :

- rechercher les comptes par source/exteral_id_tuple
- pour un compte qui n'existe plus, le marquer désactivé ainsi que la date de la désactivation (donc il faudrait un ticket pour introduire cette date)
- si un compte est désactivé depuis plus de n jours on supprime
- vérifier au passage que les comptes LDAP sont bien exclus du système de nettoyage, ce n'est pas fait pour l'instant parce qu'on suppose qu'à un annuaire LDAP correspondant une OU particulière où ce nettoyage ne doit pas être actif

#21 - 09 février 2021 09:53 - Serghei Mihai

- Lié à Bug #50966: ajouter la date de desactivation du compte dans les attributs de User ajouté

#22 - 25 février 2021 16:58 - Loïc Dachary

Bonjour,

Je souhaite participer à cet effort et je suis tenté de travailler sur un point proposé dans idée en l'état. Par exemple "rechercher les comptes par source/exteral_id_tuple pour un compte qui n'existe plus, le marquer désactivé ainsi que la date de la désactivation". Est-ce que ça vous semble pertinent ou bien est-ce que quelqu'un est déjà en train de le faire ?

En attendant votre réponse j'étudie le code, ce sera toujours ça de pris :-)

A++

#23 - 26 février 2021 09:29 - Loïc Dachary

@Serghei je vois que tu es lancé dessus donc je vais observer et apprendre. Une question (peut-être naïve): quand tu fais:

```
+            for eid in UserExternalId.objects.filter(user__is_active=True,
+                                                     source=block['realm']):
+                inactive = True
+                for external_id_tuple in map_text(block['external_id_tuples']):
+                    ldap_filter = cls.external_id_to_filter(eid.external_id, external_id_tuple)
+                    results = conn.search_s(block['basedn'],
+                                            ldap.SCOPE_SUBTREE, ldap_filter)
```

Ca fait une recherche LDAP par utilisateur ce qui peut stresser le serveur LDAP. Une autre option serait d'utiliser paged_search pour les prendre 100 par 100 et faire une liste en mémoire. Ce qui peut poser problème de RAM s'il y en a vraiment beaucoup...

Qu'en dis-tu ?

#24 - 26 février 2021 17:04 - Benjamin Dauvergne

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Serghei Mihai

#25 - 03 mars 2021 22:24 - Loïc Dachary

@Serghei si tu souhaite que j'avance sur une partie ou une autre, n'hésite pas à me solliciter, je suis disponible pour cela :-)

#26 - 08 mars 2021 12:36 - Serghei Mihai

- Assigné à Serghei Mihai supprimé

Bonjour Loïc,

Désolé pour le silence: j'étais absent quelques jours la semaine dernière.
Pas de souci de mon côté si tu as du temps pour prendre ce ticket.

#27 - 08 mars 2021 14:19 - Loïc Dachary

Merci! Je vais faire de mon mieux: je reprends Jeudi.

#28 - 18 mars 2021 13:36 - Loïc Dachary

- Fichier 0001-ldap-add-method-to-deactivate-orphaned-users-6379.patch ajouté

Bon, je n'ai pas repris jeudi dernier, ça m'apprendra à tenter de voir dans le futur. Pour archive j'ai pris des notes en parcourant des morceaux de code liés à la suppression des utilisateurs.

Voici un patch qui ajouter un test qui montre que la fonction écrite par @Serghei fonctionne parfaitement. Ne sachant pas si l'optimisation que j'ai proposée plus haut est acceptable, je me suis abstenu.

La prochaine étape semble être d'ajouter un appel à cette fonction dans le script sync-ldap-users

Qu'en pensez-vous ?

#29 - 19 mars 2021 10:33 - Serghei Mihai

Loïc Dachary a écrit :

> Voici un patch qui ajouter un test qui montre que la fonction écrite par @Serghei fonctionne parfaitement. Ne sachant pas si l'optimisation que

> j'ai proposée plus haut est acceptable, je me suis abstenu.

Désolé, je n'avais pas répondu sur ce point, mais ton idée me paraît bonne. L'usage de paged_search réduira la charge sur l'annuaire.

Je pensais à quelque chose du genre:

```
def deactivate_orphaned_users(cls):
    for block in cls.get_config():
        conn = cls.get_connection(block)
        if conn is None:
            continue
        eid_qs = UserExternalId.objects.filter(user__is_active=True, source=block['realm'])
        basedn = force_text(block.get('user_basedn') or block['basedn'])
        user_filter = force_text(block['sync_ldap_users_filter'] or block['user_filter'])
        user_filter = user_filter.replace('%s', '*')
        results = cls.paged_search(conn, basedn, ldap.SCOPE_SUBTREE, user_filter, attrlist=attribute_names)
        for dn, attrs in results:
            for eid_tuple in map_text(block['external_id_tuples']):
                external_id = self.build_external_id(eid_tuple, attrs)
                if external_id:
                   eid_qs = eid_qs.exclude(external_id=external_id)
        for eid in eid_qs:
            eid.user.mark_as_inactive()
```

à optimiser sûrement.

> La prochaine étape semble être d'ajouter un appel à cette fonction dans le script sync-ldap-users

Je pense qu'on devrait en faire une commande à part, à lancer dans un cron une fois par jour pour éviter de trop taper sur l'annuaire toutes les heure.

#30 - 19 mars 2021 11:19 - Loïc Dachary

Parfait, je prévois de faire ça le 1er avril 2021. Si l'envie te prend de le faire avant, n'hésite pas :-)

#31 - 22 mars 2021 15:54 - Serghei Mihai

- Fichier 0002-ldap-add-method-to-deactivate-orphaned-users-6379.patch ajouté

- Fichier 0001-ldap-add-DN-to-normalized-results.patch ajouté

- Statut changé de Information nécessaire à Solution proposée

- Patch proposed changé de Non à Oui

Usage de paged_search et modification légere du test proposé par Loïc (supression du DN entier au lieu juste de l'attribut uid).
Au préalable j'ajoute le dn dans les résultats normalisés pour éviter à avoir à le faire dans les méthode faisant appel à normalize_ldap_results.

#32 - 25 mars 2021 16:41 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

- get_user_filter() -> get_sync_ldap_user_filter() si ça ne sert qu'à ça
- pas la peine de récupérer tous les attributs, list(cls.attribute_name_from_external_id_tuple(block['external_id_tuples'])) suffit
- deactivate_orphaned_users n'a l'air appelé nulle part à part dans les tests

#33 - 25 mars 2021 16:41 - Benjamin Dauvergne

- Assigné à mis à Serghei Mihai

#34 - 26 mars 2021 09:32 - Serghei Mihai

- Fichier 0002-ldap-add-method-and-command-to-deactivate-orphaned-u.patch ajouté

- Fichier 0001-ldap-add-DN-to-normalized-results.patch ajouté

- Statut changé de En cours à Solution proposée

Remarques prises en compte.

Ajout de la commande et du cron (une fois par jour) pour désactiver les comptes.

#35 - 26 mars 2021 09:58 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#36 - 26 mars 2021 10:06 - Serghei Mihai

- Statut changé de Solution validée à Résolu (à déployer)

```
commit 762cba9a2de08a617bc3c17e8f5870c53edf1ed7 (HEAD -> master, origin/main)
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Thu Feb 25 18:37:59 2021 +0100

    ldap: add method and command to deactivate orphaned users (#6379)

commit 1c3bac6c87bb97da9ca860958a85a78a2e168bdc
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Mon Mar 22 15:45:20 2021 +0100

    ldap: add DN to normalized results
```

#37 - 01 avril 2021 09:16 - Frédéric Péters

- Statut changé de Résolu (à déployer) à Solution déployée

#38 - 01 avril 2021 18:17 - Loïc Dachary

J'aurais bien envie de mettre un "+1" pour dire que je suis content que le travail soit terminé, discrètement. Mais comme il n'y a pas cette fonction, intermédiaire acceptable entre l'indifférence totale et un gros pavé comme celui la, he ben vous avez droit au gros pavé :-P

Fichiers

0001-WIP-ldap_backend-deactivate-accounts-if-ldap-entry-m.patch	2,12 ko	12 février 2019	Paul Marillonnet
0001-WIP-ldap_backend-deactivate-accounts-if-ldap-entry-m.patch	2,04 ko	12 février 2019	Paul Marillonnet
0001-WIP-ldap_backend-process-orphan-accounts-6379.patch	2,84 ko	12 février 2019	Paul Marillonnet
0001-ldap-add-method-to-deactivate-orphaned-users-6379.patch	3,02 ko	18 mars 2021	Loïc Dachary
0001-ldap-add-DN-to-normalized-results.patch	2,26 ko	22 mars 2021	Serghei Mihai
0002-ldap-add-method-to-deactivate-orphaned-users-6379.patch	4,44 ko	22 mars 2021	Serghei Mihai
0002-ldap-add-method-and-command-to-deactivate-orphaned-u.patch	7,15 ko	26 mars 2021	Serghei Mihai
0001-ldap-add-DN-to-normalized-results.patch	2,26 ko	26 mars 2021	Serghei Mihai