Authentic 2 - Development #50928

Prévenir les typo lors du provisionning des groupes via LDAP

05 février 2021 17:40 - Nicolas Roche

Statut:	Fermé	**Début:**	05 février 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

En voulant provisionner les groupes (pour inclure les utilisateurs dans des Rôles),

```
    "group_to_role_mapping": [
      ["CN=GRU-Agent,OU=GRU,OU=Groupes,OU=VILLEJUIF,DC=villejuif,DC=fr", ["gru-agent"]],
    ],
    "member_of_attribute": "memberof",
```

j'ai fait une typo dans le DN (j'ai mis "OU=Groups" sans le 'e').
J'aurais été aiguillé si le backend LDAP m'avait dit que ce ~~rôle~~ groupe n'existait pas.

Révisions associées

Révision 3cdd9e7d - 01 mars 2021 09:05 - Serghei Mihai

ldap: log missing group dn when mapped to a role (#50928)

Historique

#1 - 05 février 2021 17:41 - Benjamin Dauvergne

- Description mis à jour

#2 - 05 février 2021 17:44 - Nicolas Roche

(ou plus simplement si j'avais eu un peu plus de logs)

#3 - 15 février 2021 14:58 - Serghei Mihai

- Statut changé de Nouveau à Solution proposée

- Fichier 0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch ajouté

- Patch proposed changé de Non à Oui

#4 - 15 février 2021 15:47 - Paul Marillonnet

On confond les deux cas différents où (i) l'usager n'est plus dans le groupe et (ii) le DN du groupe ne correspond pas à une entrée connue du LDAP.

(Cf. quelques lignes plus bas, en fonction de l'attribution du rôle, on peut tomber dans :

```
                # Remove extra roles
                elif group_dn not in group_dns and role in roles:
                    user.roles.remove(role)
```

qui ne signifie pas pour autant que le groupe est inexistant.)

Est-ce qu'il y aurait moyen de faire, à l'initialisation du backend, un search_s sur le nœud seul (pas le sous-arbre) pour chacune des clés de group_to_role_mapping et voir si ça correspond à quelque chose ?

#5 - 15 février 2021 16:56 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Est-ce qu'il y aurait moyen de faire, à l'initialisation du backend, un search_s sur le nœud seul (pas le sous-arbre) pour chacune des clés de group_to_role_mapping et voir si ça correspond à quelque chose ?

Oui c'est exactement ça, l'idée c'est de récupérer la totalité des groupes de temps en temps et de vérifier que les groupes pointés dans la configuration en font partie. En pseudo-code :

```
group_dns = set(dn for dn, attributes in self.normalize_results(conn.search_s(group_basedn, ldap.SCOPE_SUBTREE
, group_filter, ['1.1'])  # 1.1 is special attribute meaning, "no attribute requested"
for dn in self.gather_all_group_dns_from_config():
    if dn not in group_dns:
        log.warning('ldap: unknown group %s referenced in configuration', dn)
```

Je ne sais pas si on veut faire ça tout le temps ou juste lors des synchros par exemple.

#6 - 15 février 2021 16:56 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

#7 - 16 février 2021 18:22 - Serghei Mihai

- Fichier 0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch ajouté

- Statut changé de En cours à Solution proposée

Ok pour récupérer la liste des groupes et vérifier si chaque DN défini dans group_to_role_mapping est dédans.

#8 - 17 février 2021 12:26 - Paul Marillonnet

Je note qu'on change de fonctionnalité par rapport à la description du ticket, on passe de (i) "avertissement sur les groupes inexistants déclarés dans la config de mapping" à (ii) "avertissement sur les groupes déclarés dans la config de mapping mais qui ne sont pas dans le sous-arbre du group_basedn". Je ne sais pas si c'est ce qu'on veut.

Autre chose encore, je pense qu'indépendamment du choix de partir vers (i) ou (ii) il faut placer cette vérification plus tôt dans le backend, pas dans une méthode qui est appelée à chaque authentification d'un usager. Si — (i) seulement — le group_to_role_mapping est conséquent voire — (i) ou (ii) au choix — le group_basedn contient beaucoup de groupes, ça va taper sévère niveau requêtes.

#9 - 18 février 2021 16:27 - Serghei Mihai

- Fichier 0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch ajouté

Paul Marillonnet a écrit :

> Je note qu'on change de fonctionnalité par rapport à la description du ticket, on passe de (i) "avertissement sur les groupes inexistants déclarés dans la config de mapping" à (ii) "avertissement sur les groupes déclarés dans la config de mapping mais qui ne sont pas dans le sous-arbre du group_basedn". Je ne sais pas si c'est ce qu'on veut.

Ok, un check lors de la lecture de la config et s'il y a group_to_role_mapping de défini, on vérifie si les DNs existent dans l'annuaire.

#10 - 18 février 2021 17:57 - Benjamin Dauvergne

Serghei Mihai a écrit :

> Paul Marillonnet a écrit :
>
> > Je note qu'on change de fonctionnalité par rapport à la description du ticket, on passe de (i) "avertissement sur les groupes inexistants déclarés dans la config de mapping" à (ii) "avertissement sur les groupes déclarés dans la config de mapping mais qui ne sont pas dans le sous-arbre du group_basedn". Je ne sais pas si c'est ce qu'on veut.
>
> Ok, un check lors de la lecture de la config et s'il y a group_to_role_mapping de défini, on vérifie si les DNs existent dans l'annuaire.

Pour le point 1 de Paul, je ne comprends pas la différence entre i et ii, pour moi c'est la même chose.

Pour le point 2 de Paul, tu n'a pas apporté de changement non plus, car get_config() est de toute façon appelé à chaque authentification. Je penche plutôt pour une validation faite dans sync-ldap-users via get_users(), ça fera un warning par heure au pire. En attendant une configuration graphique pour afficher les erreurs c'est suffisant.

#11 - 19 février 2021 09:43 - Serghei Mihai

Benjamin Dauvergne a écrit :

> Pour le point 2 de Paul, tu n'a pas apporté de changement non plus, car get_config() est de toute façon appelé à chaque authentification. Je penche plutôt pour une validation faite dans sync-ldap-users via get_users(), ça fera un warning par heure au pire.

Tu penses juste au cas des synchros toutes les heures, or il y a aussi celui où l'usager se connecte et qu'à ce moment un rôle déclaré dans la conf n'existe pas. C'est le cas couvert par le test. Mais ok, on peut se dire que lever le warning uniquement lors de sync-ldap-users suffit.

> En attendant une configuration graphique pour afficher les erreurs c'est suffisant.

Cela ne nous dispense pas de logguer le warning car une fois l'annuaire configuré dans le manager, on va pas y retourner tous les jours pour voir s'il y a des éventuelles alertes.

#12 - 19 février 2021 09:43 - Serghei Mihai

- Statut changé de Solution proposée à En cours

#13 - 19 février 2021 10:10 - Serghei Mihai

- Fichier 0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, vérification uniquement lors du get_users.

#14 - 22 février 2021 16:56 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Oui ok je trouve ça bien comme ça.

#15 - 01 mars 2021 09:07 - Serghei Mihai

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

- Assigné à mis à Serghei Mihai

```
commit 3cdd9e7d29320796fff4fb3c5460cce5a1020eb3 (origin/main)
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Mon Feb 15 14:32:38 2021 +0100

    ldap: log missing group dn when mapped to a role (#50928)
```

#16 - 04 mars 2021 10:16 - Frédéric Péters

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

Fichiers

0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch	2,71 ko	15 février 2021	Serghei Mihai
0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch	3,64 ko	16 février 2021	Serghei Mihai
0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch	3,74 ko	18 février 2021	Serghei Mihai
0001-ldap-log-missing-group-dn-when-mapped-to-a-role-5092.patch	3,73 ko	19 février 2021	Serghei Mihai