

Authentic 2 - Development #70213

Possibilité d'attribuer des rôles à un utilisateur selon des attributs

13 octobre 2022 11:03 - Marie Kuntz -> retour le 13 mai

Statut:	Rejeté	Début:	13 octobre 2022
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Non		
Description			
Suite à #53442 , j'ai besoin de pouvoir attribuer un ou plusieurs rôles en fonction d'attributs multiples. Cas à l'université de Nantes : les agents et les étudiants se connectent en CAS et l'on récupère un attribut "population" qui peut contenir un ou plusieurs éléments. Chaque élément doit donner un rôle distinct : "agent", "étudiant", etc.			
Ticket pour chiffrage.			
Demandes liées:			
Lié à Authentic 2 - Development #77756: authenticators : AddRoleAction condit...		Fermé	21 mai 2023

Historique

#5 - 13 octobre 2022 14:51 - Valentin Deniaud

Si un attribut n'est plus présent, il faut retirer le rôle précédemment ajouté ?

#6 - 13 octobre 2022 14:56 - Marie Kuntz -> retour le 13 mai

Valentin Deniaud a écrit :

Si un attribut n'est plus présent, il faut retirer le rôle précédemment ajouté ?

Ce serait logique, oui. Comment ça fonctionne sur [#53442](#) ?

#7 - 13 octobre 2022 15:14 - Benjamin Dauvergne

Marie Kuntz a écrit :

Valentin Deniaud a écrit :

Si un attribut n'est plus présent, il faut retirer le rôle précédemment ajouté ?

Ce serait logique, oui. Comment ça fonctionne sur [#53442](#) ?

On a inventé une histoire de verrouillage des rôles une fois qu'ils sont liés au LDAP mais je ne trouve pas terrible la façon dont ça s'active. Cette fois je verrai plutôt un rôle explicite lié à la règle pour lequel la gestion des membres soit désactivée (par le même mécanisme que pour le LDAP le flag `can_manage_members`), à charge ensuite de faire hériter ce rôle à d'autres rôles "métiers" (comme ça on ne peut pas réutiliser un rôle dans lequel il y aurait déjà des utilisateurs et se retrouver dans une situation bizarre de ne pas pouvoir le gérer mais que ces utilisateurs ne soient pas retirer non plus via la connection OIDC).

On crée une règle, le rôle est créé (avec un nom un peu explicite, "Client OIDC Truc: population étudiante"; on supprime la règle le rôle est supprimé.

#8 - 13 octobre 2022 15:23 - Marie Kuntz -> retour le 13 mai

Pas sûre d'avoir compris, j'ai l'impression que tu parles de la gestion des rôles en général alors que je pensais que tu parlais du retrait du rôle à un utilisateur qui n'a plus le bon attribut.

Ce que j'ai compris :

- Jean-Michel a un attribut "agent" et un attribut "étudiant"
- il se connecte et gagne 2 rôles
- 2 ans plus tard, Jean-Michel a son master en mansplaining et n'est plus étudiant, mais il est toujours agent
- il se connecte, il perd son rôle étudiant lié à l'attribut "étudiant", il a toujours son rôle agent

#9 - 13 octobre 2022 15:26 - Benjamin Dauvergne

Marie Kuntz a écrit :

Pas sûre d'avoir compris, j'ai l'impression que tu parles de la gestion des rôles en général alors que je pensais que tu parlais du retrait du rôle à un utilisateur qui n'a plus le bon attribut.

Je répondais à ton commentaire mais c'était surtout un paragraphe pour Valentin.

Ce que j'ai compris :

- Jean-Michel a un attribut "agent" et un attribut "étudiant"
- il se connecte et gagne 2 rôles
- 2 ans plus tard, Jean-Michel a son master en mansplaining et n'est plus étudiant, mais il est toujours agent
- il se connecte, il perd son rôle étudiant lié à l'attribut "étudiant", il a toujours son rôle agent

Oui c'est ça qu'on veut et il n'y a pas de souci on sait déjà faire pour LDAP comme tu le pointes. Je me disais juste que la solution précédente était bancal sur certains aspects qu'on pourrait corriger ici (et rétropropatruc vers LDAP quand on aura la configuration LDAP dans le BO).

#10 - 26 juin 2023 14:24 - Marie Kuntz -> retour le 13 mai

- Statut changé de Nouveau à Rejeté

Je ferme, je n'en ai plus besoin pour le projet lié.

#11 - 26 juin 2023 15:05 - Valentin Deniaud

- Lié à Development #77756: authenticators : AddRoleAction conditionné par des valeurs d'attributs de profil étendu ajouté