Authentic 2 - Development #62710

rapatriement du script client de synchronisation depuis le plugin authentic2-gnm vers auth_oidc

13 mars 2022 09:36 - Paul Marillonnet

Statut:	Fermé	**Début:**	13 mars 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

C'est spécifique à a2 client oidc d'un autre a2 fournisseur, et c'est spécifique à une config oidc où les subs délivrés sont des pseudonymes réversibles.
Je me disais que rapatrier tout cela dans auth_oidc permettrait de mieux tester le couplage avec la réversibilité des pseudonymes servis dans la partie idp_oidc.

Demandes liées:

Lié à Authentic 2 - Development #65877: idp_oidc : les hooks de l'api /users/...	**En cours**	**01 juin 2022**
Lié à Authentic 2 - Development #65890: idp_oidc: tolérer la synchro pour les...	**Nouveau**	**01 juin 2022**
Lié à Authentic 2 - Development #70805: script de synchronisation : pour un c...	**Rejeté**	**28 octobre 2022**
Lié à Authentic 2 - Development #72418: auth_oidc : factorisation de la résol...	**Fermé**	**14 décembre 2022**

Révisions associées

Révision 2aeb5bad - 14 décembre 2022 15:31 - Paul Marillonnet

management: add a LogToConsoleCommand base class (#62710)

Révision 73ac9f07 - 14 décembre 2022 15:31 - Paul Marillonnet

auth_oidc: add an oidc-sync-provider command (#62710)

Historique

#2 - 13 mars 2022 09:40 - Paul Marillonnet

- Sujet changé de gestion des personnes morales : rapatriement de l'api de synchro dans le module auth_oidc (?) à gestion des personnes morales : rapatriement du script client de synchro dans le module auth_oidc (?)

(actuellement le script est dans le plugin authentic2-gnm, commande sync-cut.py).

#5 - 15 mars 2022 16:40 - Paul Marillonnet

- Sujet changé de gestion des personnes morales : rapatriement du script client de synchro dans le module auth_oidc (?) à rapatriement du script client de synchronisation depuis le plugin authentic2-gnm vers auth_oidc

#6 - 30 mai 2022 17:47 - Paul Marillonnet

- Statut changé de Nouveau à En cours

- Assigné à mis à Paul Marillonnet

#7 - 31 mai 2022 11:35 - Paul Marillonnet

Dans la branche, une copie assez conforme de ce qui existe dans le plugin, copie testée elle aussi. Je vais voir s'il est judicieux de rajouter des tests.

#8 - 01 juin 2022 09:51 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Une version qui se base sur deux hypothèses :
· on connaît le slug du fournisseur vers lequel on veut se synchroniser, slug que l'on passe en paramètre de la commande ;
· l'attribut 'issuer' du fournisseur correspond à son fqdn du point de vue du client.

Cela me paraît être deux hypothèses raisonnables, mais si l'une ou l'autre s'avère fausse pour le chantier qui motive ce ticket, je reverrai ma copie.

#10 - 01 juin 2022 09:56 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Paul Marillonnet a écrit :

> Une version qui se base sur deux hypothèses :
> · on connaît le slug du fournisseur vers lequel on veut se synchroniser, slug que l'on passe en paramètre de la commande ;
> · l'attribut 'issuer' du fournisseur correspond à son fqdn du point de vue du client.
> Cela me paraît être deux hypothèses raisonnables, mais si l'une ou l'autre s'avère fausse pour le chantier qui motive ce ticket, je reverrai ma copie.

Le test ne va pas, je recommence.

#11 - 01 juin 2022 10:45 - Paul Marillonnet

Et bien sûr il y a tout un pan du problème qui m'avait échappé : la synchro des usagers modifiés se fait entre un fournisseur et un rp oidc, il ne faut pas renvoyer les attributs usager bruts de fonderie, mais tenir compte de la configuration des mappings de claim entre ces deux entités OIDC.

Dans le plugin GL on se simplifiait la tâche car le mapping était connu, les modifications tenant compte de cette config avaient lieu en dur dans le code.
Ici c'est plus complexe, il va falloir détecter que l'appelant de l'/api/users/?modified__gt=… est par ailleurs un client oidc pour authentic, et parvenir à la substitution des attributs en claims conformément à la configuration de ce client.

Tâche non triviale, j'ai quelques idées mais aucune arrêtée pour l'instant. Peut-être un paramètre de qs supplémentaire dans cette api pour passer le slug du client oidc appelant ?
Je revois ma copie.

#12 - 01 juin 2022 11:34 - Frédéric Péters

> il va falloir détecter que l'appelant de l'/api/users/?modified__gt=… est par ailleurs un client oidc pour authentic, et parvenir à la substitution des attributs en claims conformément à la configuration de ce client.

Le script appelle /api/users/?... qui est une API standard d'authentic, le propos ici est que le script de synchro du dépôt authentic2-gnm fonctionne parce qu'en face l'/api/users/? n'est en fait pas l'API standard d'authentic mais une API modifiée par authentic2-cut ?

(je ne capte pas)

#13 - 01 juin 2022 12:00 - Paul Marillonnet

Frédéric Péters a écrit :

> > il va falloir détecter que l'appelant de l'/api/users/?modified__gt=… est par ailleurs un client oidc pour authentic, et parvenir à la substitution des attributs en claims conformément à la configuration de ce client.
>
> Le script appelle /api/users/?... qui est une API standard d'authentic, le propos ici est que le script de synchro du dépôt authentic2-gnm fonctionne parce qu'en face l'/api/users/? n'est en fait pas l'API standard d'authentic mais une API modifiée par authentic2-cut ?

Oui voilà, il y a ce fameux hook planqué dans un coin, qui change complètement le sérialiseur et donc le contenu de la réponse :
https://git.entrouvert.org/authentic2-cut.git/tree/src/authentic2_cut/apps.py#n290
Ici dans ce hook on sait à quoi ressemble la configuration de mapping de claims GL -> Toodego (par exemple on sait qu'on peut placer directement le contenu de user.last_name dans family_name, ligne 322), mais dans le cas général il faut inspecter cette configuration et résoudre les claims usager par usager.

#14 - 01 juin 2022 15:03 - Paul Marillonnet

- Lié à Development #65877: idp_oidc : les hooks de l'api /users/ doivent tenir compte de la résolution des claims lorsque l'appelant est un client oidc connu ajouté

#15 - 01 juin 2022 15:03 - Paul Marillonnet

Paul Marillonnet a écrit :

> Frédéric Péters a écrit :
>
> > il va falloir détecter que l'appelant de l'/api/users/?modified__gt=… est par ailleurs un client oidc pour authentic, et parvenir à la substitution des attributs en claims conformément à la configuration de ce client.

> Le script appelle /api/users/?... qui est une API standard d'authentic, le propos ici est que le script de synchro du dépôt authentic2-gnm fonctionne parce qu'en face l'/api/users/? n'est en fait pas l'API standard d'authentic mais une API modifiée par authentic2-cut ?

> Oui voilà, il y a ce fameux hook planqué dans un coin, qui change complètement le sérialiseur et donc le contenu de la réponse :
> https://git.entrouvert.org/authentic2-cut.git/tree/src/authentic2_cut/apps.py#n290
> Ici dans ce hook on sait à quoi ressemble la configuration de mapping de claims GL -> Toodego (par exemple on sait qu'on peut placer directement le contenu de user.last_name dans family_name, ligne 322), mais dans le cas général il faut inspecter cette configuration et résoudre les claims usager par usager.

J'ai créé #65877 pour cette partie, sinon on ne va pas s'en sortir.

#16 - 01 juin 2022 15:41 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Statut changé de En cours à Solution proposée

Paul Marillonnet a écrit :

> J'ai créé #65877 pour cette partie, sinon on ne va pas s'en sortir.

Et donc de ce côté ci, le patche.

#17 - 02 juin 2022 14:31 - Paul Marillonnet

- Lié à Development #65890: idp_oidc: tolérer la synchro pour les clients en identifier_policy:=POLICY_UUID ajouté

#19 - 25 juillet 2022 12:06 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

La gestion du --delta me parait un peu foireuse, il suffit qu'on saute une exécution (cron n'a rien d'exact) pour perdre des mises à jour, il faudrait plutôt ajouter un flag sur le modèle OIDCProvider pour dire "capable de synchro-authentic" (c'est super spécifique mais au point où on en est) et un champ caché avec la date de la dernière synchro, date prise à now() - 1 minute de la dernière exécution (en cas de décalage d'horloge). D'une commande ça deviendra juste une méthode de cron dans le style passerelle (je ne sais qu'il n'y a pas le cadre pour faire ça actuellement, ce sera appelé par une commande spécifique, mais partons sur la bonne forme, un peu comme la commande sync-ldap-user ne contient quasiment pas de code).

```
class AppConfig:
    def hourly(self):
        last_time = now() - timedela(minutes=1)
        for provider in providers:
            provider.oidc_provider_synchro(last_time)
        provider.sync_last_time = last_time
        provider.save(fields=['sync_last_time'])
```

#20 - 04 août 2022 09:43 - Paul Marillonnet

- Fichier 0001-WIP-auth_oidc-add-an-oidc-sync-provider-command-6271.patch ajouté

- Statut changé de En cours à Solution proposée

Ok pour virer l'option '--delta' et se baser sur des champs spécifiques de modèles.
Par contre pour virer le code de la commande, je n'arrive pas à trouver un parallèle avec sync-ldap-users (où la méthode du backend appelée, i.e. get_users, est générique et ne se restreint pas à des fins de synchronisation). Ici à vouloir sortir le code de la commande on se retrouve avec du code très spécifique dans le modèle, spécifique car propre à la synchro, qui plus est seulement lorsque le fournisseur oidc distant est un authentic.

Un exemple de patche pour illustrer mon propos. Je pourrais encore déplacer les bouts spécifiques aux appels à /api/users/?modified_gt=… et /api/synchronization/ dans authentic2_auth_oidc.utils, mais ça va pas simplifier l'affaire déjà plutôt convoluée.

Pour ma part je préfère infiniment la première version du patche, et peut-être que j'ai mal interprété les modifications demandées dans la relecture, mais si tu me confirmes que c'est bien la piste envisagée je vais quand même continuer (en remaniant un peu les tests, et en trouver une manière de logguer correctement l'affaire, pour l'instant dans le patche c'est du bricolage).

#21 - 04 août 2022 10:44 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Ok pour virer l'option '--delta' et se baser sur des champs spécifiques de modèles.
> Par contre pour virer le code de la commande, je n'arrive pas à trouver un parallèle avec sync-ldap-users (où la méthode du backend appelée, i.e. get_users, est générique et ne se restreint pas à des fins de synchronisation). Ici à vouloir sortir le code de la commande on se retrouve

> avec du code très spécifique dans le modèle, spécifique car propre à la synchro, qui plus est seulement lorsque le fournisseur oidc distant est un authentic.

Si tu veux implémenter SCIM au passage vas y :) en attendant on aura du code spécifique à une API spécifique d'authentic dans authentic oui, on vivra avec ça.

> Un exemple de patche pour illustrer mon propos. Je pourrais encore déplacer les bouts spécifiques aux appels à /api/users/?modified_gt=… et /api/synchronization/ dans authentic2_auth_oidc.utils, mais ça va pas simplifier l'affaire déjà plutôt convoluée.

Mon souci c'est d'avoir la logique dans un seul endroit et pas éparpillé dans des commandes et à terme de faire disparaître ces commandes pour avoir un système de cron unique et pas une nouvelle commande à chaque fois.

> Pour ma part je préfère infiniment la première version du patche, et peut-être que j'ai mal interprété les modifications demandées dans la relecture, mais si tu me confirmes que c'est bien la piste envisagée je vais quand même continuer (en remaniant un peu les tests, et en trouver une manière de logguer correctement l'affaire, pour l'instant dans le patche c'est du bricolage).

Disons que je ne vois pas de difficulté technique à mettre le code exactement identique ailleurs que dans la commande, si tu en vois dis moi, je ne vois qu'une objection de forme sur le fait que ce soit spécifique à un cas d'usage Publik/authentic.

C'est rouge, je regarde dès que c'est vert.

#22 - 05 août 2022 11:16 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

Benjamin Dauvergne a écrit :

> […]
>
> Si tu veux implémenter SCIM au passage vas y :) en attendant on aura du code spécifique à une API spécifique d'authentic dans authentic oui, on vivra avec ça.
>
> […]
>
> Mon souci c'est d'avoir la logique dans un seul endroit et pas éparpillé dans des commandes et à terme de faire disparaître ces commandes pour avoir un système de cron unique et pas une nouvelle commande à chaque fois.
>
> […]
>
> Disons que je ne vois pas de difficulté technique à mettre le code exactement identique ailleurs que dans la commande, si tu en vois dis moi, je ne vois qu'une objection de forme sur le fait que ce soit spécifique à un cas d'usage Publik/authentic.
>
> C'est rouge, je regarde dès que c'est vert.

Ok, donc la version avec le code dans une méthode du modèle. J'avais commencé à réfléchir à une façon dont les logs de la méthode pourraient arriver sur stdout quand celle-ci détecte qu'elle a été appelée par la commande, mais ça donne un peu n'importe quoi dans le code. Finalement une version où ce qui est dans la commande arrive sur stdout, et les logs de la méthode passent comme ailleurs dans le logging.getLogger(__name__).

#23 - 05 août 2022 11:58 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Ok, donc la version avec le code dans une méthode du modèle. J'avais commencé à réfléchir à une façon dont les logs de la méthode pourraient arriver sur stdout quand celle-ci détecte qu'elle a été appelée par la commande, mais ça donne un peu n'importe quoi dans le code. Finalement une version où ce qui est dans la commande arrive sur stdout, et les logs de la méthode passent comme ailleurs dans le logging.getLogger(__name__).

Faut rien inventer pour la sortie, utilise logging partout et adapte la configuration du handler et du logger en fonction de 'verbose'. Il me semble que Valentin a fait ça dans une autre commande, à regarder.

#24 - 05 août 2022 12:08 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

Benjamin Dauvergne a écrit :

> Faut rien inventer pour la sortie, utilise logging partout et adapte la configuration du handler et du logger en fonction de 'verbose'. Il me semble que Valentin a fait ça dans une autre commande, à regarder.

Je ne retrouve pas la commande en question. Quelque chose comme ça où un argument 'verbose' est passé à la méthode en fonction des options de la commande ?

#25 - 05 août 2022 12:33 - Frédéric Péters

sync-ldap-users, log_ldap_to_console, etc.

#26 - 05 août 2022 12:56 - Paul Marillonnet

Frédéric Péters a écrit :

> sync-ldap-users, log_ldap_to_console, etc.

Ah oui ok je n'avais pas compris que c'était de la mécanique de prévention de doublon dans les logs de commande de synchro ldap dont Benj parlait. Je vais proposer quelque chose qui va dans ce sens.

#27 - 05 août 2022 12:56 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

#28 - 05 août 2022 13:56 - Paul Marillonnet

- Fichier 0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Fichier 0001-management-add-a-LogToConsoleCommand-base-class-6271.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, plutôt que de s'inspirer un peu de ce qui a été fait dans #58404, en faire une classe parente LogToConsoleBaseCommand (0001), qu'on ré-utilise par la suite pour notre synchro OIDC (0002).

#29 - 25 octobre 2022 11:28 - Benjamin Dauvergne

- Fichier 0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Fichier 0001-management-add-a-LogToConsoleCommand-base-class-6271.patch ajouté

Rebasé et validé, à pousser vendredi.

#30 - 25 octobre 2022 11:28 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#31 - 25 octobre 2022 15:08 - Benjamin Dauvergne

- Statut changé de Solution validée à En cours

Ça synchronise sur l'email et pas sur le sub, ça ne me parait ce qui est souhaitable pour un raccordement en général, je ne sais pas trop pourquoi Fred a choisi de synchroniser sur l'email (en cas de changement d'email la synchro est perdue et le service ne verra pas le changement jusqu'à la prochaine connexion).

#32 - 26 octobre 2022 09:57 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Ça synchronise sur l'email et pas sur le sub, ça ne me parait ce qui est souhaitable pour un raccordement en général, je ne sais pas trop pourquoi Fred a choisi de synchroniser sur l'email (en cas de changement d'email la synchro est perdue et le service ne verra pas le changement jusqu'à la prochaine connexion).

Ok, je revois ça pour synchroniser sur le sub.

#33 - 28 octobre 2022 09:40 - Paul Marillonnet

- Fichier 0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Fichier 0001-management-add-a-LogToConsoleCommand-base-class-6271.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, on se base sur le sub lorsque celui-ci est fourni.

#34 - 28 octobre 2022 09:43 - Paul Marillonnet

- Lié à Development #70805: script de synchronisation : pour un client activant la gestion des profils PM, l'endpoint doit retourner les subs correspondant à ces profils ajouté

#35 - 09 décembre 2022 11:56 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Voilà, on se base sur le sub lorsque celui-ci est fourni.

Il faut virer complètement la synchro sur l'email, la synchro ne doit pas créer de nouvelles liaisons, du tout, ça n'apporte rien et ça nous a causé des soucis par le passé. La synchronisation n'est là que pour que les gens puissent éditer leur profil sans se préoccuper de sa propagation.

#36 - 12 décembre 2022 08:47 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Ok, je n'avais pas compris ça, je vire complètement toute concordance sur l'email.

#37 - 14 décembre 2022 11:30 - Paul Marillonnet

- Fichier 0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch ajouté

- Fichier 0001-management-add-a-LogToConsoleCommand-base-class-6271.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, la version sans la synchro sur le mail.

#38 - 14 décembre 2022 15:21 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ok. Dans le futur il faudrait factoriser la partie mapping des claims avec ce qui est fait dans le backend d'auth_oidc.

#39 - 14 décembre 2022 15:30 - Paul Marillonnet

- Lié à Development #72418: auth_oidc : factorisation de la résolution du mapping de claim entre le backend d'authn et la synchronisation ajouté

#40 - 14 décembre 2022 15:42 - Paul Marillonnet

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

```
commit 73ac9f079a9a916fbad3524afd8a7b481c9ab22f
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Mon May 30 17:59:15 2022 +0200

    auth_oidc: add an oidc-sync-provider command (#62710)

commit 2aeb5bad51ded7e35f4ac3feed8a6b4c7b263d8b
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Fri Aug 5 13:05:55 2022 +0200

    management: add a LogToConsoleCommand base class (#62710)
```

#41 - 23 décembre 2022 10:16 - Transition automatique

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

#42 - 26 février 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	10,6 ko	01 juin 2022	Paul Marillonnet
0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	11,7 ko	01 juin 2022	Paul Marillonnet
0001-WIP-auth_oidc-add-an-oidc-sync-provider-command-6271.patch	14,2 ko	04 août 2022	Paul Marillonnet
0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,1 ko	05 août 2022	Paul Marillonnet

0001-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,3 ko	05 août 2022	Paul Marillonnet
0001-management-add-a-LogToConsoleCommand-base-class-6271.patch	4,91 ko	05 août 2022	Paul Marillonnet
0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,2 ko	05 août 2022	Paul Marillonnet
0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,1 ko	25 octobre 2022	Benjamin Dauvergne
0001-management-add-a-LogToConsoleCommand-base-class-6271.patch	4,91 ko	25 octobre 2022	Benjamin Dauvergne
0001-management-add-a-LogToConsoleCommand-base-class-6271.patch	4,91 ko	28 octobre 2022	Paul Marillonnet
0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,5 ko	28 octobre 2022	Paul Marillonnet
0001-management-add-a-LogToConsoleCommand-base-class-6271.patch	4,91 ko	14 décembre 2022	Paul Marillonnet
0002-auth_oidc-add-an-oidc-sync-provider-command-62710.patch	15,3 ko	14 décembre 2022	Paul Marillonnet