Plugin Carte elD (fedict/bosa) - Development #66876

migrer FedictAuthenticator et sa config en base

01 juillet 2022 15:20 - Paul Marillonnet

Statut:FerméDébut:01 juillet 2022Priorité:NormalEchéance:

Assigné à: Valentin Deniaud % réalisé: 0%

Catégorie: Temps estimé: 0:00 heure

Version cible:

Patch proposed: Oui Planning: Non

Description

lci pour la connexion fedict/bosa, on est sur du SAML avec quelques spécificités, on pourrait imaginer un travail reposant sur #65483 (la migration des authentificateurs SAML en base), ce qui permettrait de retirer un bout du code authentic qui (une fois #65483 passé) ne serait plus ici que pour ce plugin, i.e. authentic2.authenticators (qui en plus d'être quasi-déprécié, crée la confusion avec ce qu'on utilise maintenant, à savoir authentic2.apps.authenticators.models).

Demandes liées:

Lié à Authentic 2 - Development #66853: virer authentic2.authenticators Fermé 01 juillet 2022
Lié à Authentic 2 - Development #65483: configuration des méthodes d'authenti... Fermé 19 mai 2022
Lié à Authentic 2 - Development #67103: authenticators, éviter la modificatio... Fermé 07 juillet 2022
Bloque Authentic 2 - Development #65479: configuration de l'ordre des méthode... Fermé 19 mai 2022

Révisions associées

Révision 803d0cb3 - 07 juillet 2022 13:56 - Valentin Deniaud

misc: move authenticator code to models.py (#66876)

Révision 86033d32 - 07 juillet 2022 13:57 - Valentin Deniaud

migrate authenticator to database (#66876)

Historique

#1 - 01 juillet 2022 15:21 - Paul Marillonnet

- Lié à Development #66853: virer authentic2.authenticators ajouté

#2 - 01 juillet 2022 15:21 - Paul Marillonnet

- Lié à Development #65483: configuration des méthodes d'authentification, SAML ajouté

#3 - 01 juillet 2022 15:21 - Paul Marillonnet

- Description mis à jour

#4 - 06 juillet 2022 16:41 - Valentin Deniaud

- Assigné à mis à Valentin Deniaud

#5 - 07 juillet 2022 14:01 - Valentin Deniaud

- Fichier 0001-misc-move-authenticator-code-to-models.py-66876.patch ajouté
- Fichier 0002-migrate-authenticator-to-database-66876.patch ajouté
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

#6 - 07 juillet 2022 14:05 - Valentin Deniaud

- Lié à Development #67103: authenticators, éviter la modification du nom d'un block de login ajouté

#7 - 07 juillet 2022 14:05 - Valentin Deniaud

(rouge pour le moment en raison du ticket lié)

19 avril 2024 1/4

#11 - 07 juillet 2022 17:56 - Valentin Deniaud

- Bloque Development #65479: configuration de l'ordre des méthodes d'authentification ajouté

#12 - 21 juillet 2022 11:24 - Paul Marillonnet

Bon, 1h à tenter de remonter un environnement similaire en local, en vain et malgré la copie de ma conf qui avait fonctionné pour coder #60837. Toujours des erreurs lasso, côté idp imitant le csam, au chargement du SP authentic qui inclut l'authentificateur fedict, sans plus de précision et alors que l'enregistrement du SP à partir de l'url des MD dans l'/admin/ "csam" se passe sans souci. Ça commence à me gaver.

La migration se passe sans encombres, je vais relire le code.

#13 - 21 juillet 2022 11:58 - Frédéric Péters

Toujours des erreurs lasso, côté idp imitant le csam, au chargement du SP authentic qui inclut l'authentificateur fedict

Éventuellement sur un autre ticket mais on parle bien de https://connexion-csam.test.entrouvert.org/ quelle manip quelle erreur ? Très vite quand je compare https://connexion-csam.test.entrouvert.org/admin/saml/libertyprovider/6/change/ et https://connexion-csam.test.entrouvert.org/admin/saml/libertyprovider/4/change/ le mien n'a pas la section KeyDescriptor, ça élimine toute une classe de problèmes.

#14 - 21 juillet 2022 12:02 - Paul Marillonnet

Frédéric Péters a écrit :

Éventuellement sur un autre ticket mais on parle bien de https://connexion-csam.test.entrouvert.org/ quelle manip quelle erreur ? Très vite quand je compare https://connexion-csam.test.entrouvert.org/admin/saml/libertyprovider/6/change/ et https://connexion-csam.test.entrouvert.org/admin/saml/libertyprovider/4/change/ le mien n'a pas la section KeyDescriptor, ça élimine toute une classe de problèmes.

Je vais regarder cela ensuite par acquis de conscience, mais je n'avais pas vu passer la note 10 de ce ticket qui indique que ça a déjà été appliqué en local avec succès. Je suis en train de relire le code.

#15 - 21 juillet 2022 14:38 - Paul Marillonnet

Dans l'immédiat, ce qui m'embête un peu est cette impression que l'IdP CSAM, puisqu'apparaissant dans la liste les IdPs déclarés dans les settings mellon (avec un ENTITY_ID:="belgium.be"), va atterrir à la fois en tant qu'authentificateur SAML et en tant qu'authentificateur Fedict dans le /manage/.

Sur la machine d'Imio, les migrations authentic2_auth_saml/migrations/0002_auto_20220608_1559.py et authentic2_auth_fedict/migrations/0002_auto_20220706_1712.py vont toutes deux êtres exécutées et sauf erreur de ma part on aura deux authentificateurs différents. Il faudrait peut-être faire dépendre la migration de création de l'authentificateur Fedict de celle créant les authentificateurs SAML, ensuite dans la migration Fedict vérifier qu'un authentificateur SAML de même identifiant n'existe pas déjà, et le supprimer au besoin. Je me plante ?

D'autres remarques, pas du tout rédhibitoires et qu'on pourrait traiter dans des prochains tickets : réduire encore la dépendances aux settings et retirer des choses écrites en dur dans le code, en se rapprochant du modèle de l'authentificateur SAML. Quelques exemples comme le mapping écrit en dur dans le code de l'adaptateur et qu'on pourrait voir apparaître en lecture seule dans le /manage/, ou bien encore les AUTHN_CLASSREF qui sont ici utilisées pour déterminer si le raccordement Fedict supporte [a] le compte ItsMe et [b] les jetons personnels, avec [a] et [b] qui pourraient être des cases à cocher dans le /manage/.

#16 - 21 juillet 2022 15:07 - Valentin Deniaud

Paul Marillonnet a écrit :

Dans l'immédiat, ce qui m'embête un peu est cette impression que l'IdP CSAM, puisqu'apparaissant dans la liste les IdPs déclarés dans les settings mellon (avec un ENTITY_ID:="belgium.be"), va atterrir à la fois en tant qu'authentificateur SAML et en tant qu'authentificateur Fedict dans le /manage/.

Sur la machine d'Imio, les migrations authentic2_auth_saml/migrations/0002_auto_20220608_1559.py et authentic2_auth_fedict/migrations/0002_auto_20220706_1712.py vont toutes deux êtres exécutées

La migration SAML a déjà été exécutée, et aïe tu as raison elle a créé un authentificateur SAML, passé inaperçu et heureusement désactivé car pas de A2_AUTH_SAML_ENABLE.

Il faudrait peut-être faire dépendre la migration de création de l'authentificateur Fedict de celle créant les authentificateurs SAML, ensuite dans la migration Fedict vérifier qu'un authentificateur SAML de même identifiant n'existe pas déjà, et le supprimer au besoin.

Donc ici tu proposes de nettoyer ça au détour de la migration, aller faisons ça.

réduire encore la dépendances aux settings

19 avril 2024 2/4

Oui c'est important de noter qu'ici on a 0 migré la config en base comme dit le titre du ticket, tout reste lu depuis les settings sauf activé/désactivé, ordre, condition d'affichage.

#18 - 21 juillet 2022 15:31 - Valentin Deniaud

Valentin Deniaud a écrit :

Donc ici tu proposes de nettoyer ça au détour de la migration, aller faisons ça.

Bon en testant je me prends forcément des LookupError: No installed app with label 'authentic2_auth_saml' et même si ça pourrait marcher je suis frileux de mixer les choses comme ça, plutôt on corrigera directement sur la db d'IMIO. Pas de modif au patch donc.

#19 - 21 juillet 2022 15:35 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Valentin Deniaud a écrit :

Valentin Deniaud a écrit :

Donc ici tu proposes de nettoyer ça au détour de la migration, aller faisons ça.

Bon en testant je me prends forcément des LookupError: No installed app with label 'authentic2_auth_saml' et même si ça pourrait marcher je suis frileux de mixer les choses comme ça, plutôt on corrigera directement sur la db d'IMIO. Pas de modif au patch donc.

Oui, j'avais complètement zappé le fait que l'authentificateur SAML serait sans doute désactivé par défaut. Pour le reste tout relu et c'est bon pour moi. Ack.

#20 - 21 juillet 2022 15:38 - Valentin Deniaud

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

```
commit 86033d32ebd45214a106646562e75956e894ac1c
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date: Wed Jul 6 17:18:21 2022 +0200
```

migrate authenticator to database (#66876)

```
commit 803d0cb3e55a8022e1643a9bae195bda0688ff2c
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date: Wed Jul 6 17:02:18 2022 +0200
```

acc: Wea out o 17:02:10 2022 70200

misc: move authenticator code to models.py (#66876)

#21 - 21 juillet 2022 15:52 - Frédéric Péters

corrigera directement sur la db d'IMIO

Ça n'est pas réaliste.

#22 - 21 juillet 2022 15:55 - Paul Marillonnet

Frédéric Péters a écrit :

corrigera directement sur la db d'IMIO

Ça n'est pas réaliste.

J'étais parti dans l'idée que l'authentificateur SAML en surplus serait désactivé par défaut, sans aucune incidence sur les écrans de connexion authentic, et qu'on irait ensuite dans le /manage/ le supprimer carrément et l'oublier à jamais. J'oublie un truc ?

#23 - 21 juillet 2022 15:57 - Valentin Deniaud

Paul Marillonnet a écrit :

19 avril 2024 3/4

Frédéric Péters a écrit :

corrigera directement sur la db d'IMIO

Ça n'est pas réaliste.

J'étais parti dans l'idée que l'authentificateur SAML en surplus serait désactivé par défaut, sans aucune incidence sur les écrans de connexion authentic, et qu'on irait ensuite dans le /manage/ le supprimer carrément et l'oublier à jamais. J'oublie un truc ?

Oui ce n'est peut-être pas clair de nos discussions avec Paul mais le bug s'est déjà produit, il est sans rapport avec ce ticket. J'ai créé #67611 pour en discuter.

#24 - 05 août 2022 22:16 - Frédéric Péters

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

#25 - 09 octobre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-misc-move-authenticator-code-to-models.py-66876.patch	6,85 ko	07 juillet 2022	Valentin Deniaud
0002-migrate-authenticator-to-database-66876.patch	14,4 ko	07 juillet 2022	Valentin Deniaud

19 avril 2024 4/4