django-mellon - Support #20229

Incompatibilité avec ADFS 3.0 à cause du noeud d'extension eo:next_url

22 novembre 2017 22:14 - Olivier Larchevêque

Statut:	Fermé	**Début:**	22 novembre 2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Thomas Noël	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	1.2.34		
Patch proposed:	Oui	**Planning:**	

Description

Bonjour,

J'ai développé un SP avec django-mellon. J'ai testé le fonctionnement avec un IDP de Saleforce sans problème. Par contre avec un ADFS 3.0 (Windows Server 2012 R2)
J'obtiens cette erreur : To accept extensions, you must extend the SamlProtocolSerializer. Mais je ne peux pas...

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:eo="https://www.entrouvert.com/"
    ID="_436D5D4EED273F6DB99016A17F10AC4C"
    Version="2.0"
    IssueInstant="2017-11-21T14:13:10Z"
    Destination="https://XXXX/adfs/ls/"
    ForceAuthn="true"
    IsPassive="false">
    <saml:Issuer>https://monsp/accounts/mellon/metadata/</saml:Issuer>
    <samlp:Extensions>
        <eo:next_url>https://monsp/</eo:next_url>
    </samlp:Extensions>
    <samlp:NameIDPolicy
        AllowCreate="true"/>
</samlp:AuthnRequest>
```

Est-ce que vous avez été confronté à cette situation, ou est-ce que c'est possible tout simplement de ne pas générer la requête avec les extensions.

Merci

Demandes liées:

Lié à django-mellon - Development #18452: inclure l'url de destination dans l...	**Fermé**	**05 septembre 2017**
Lié à Hobo - Bug #22352: activer l'envoi de l'extension eo:next_url par mello...	**Fermé**	**07 mars 2018**

Révisions associées

Révision ac75dce8 - 07 mars 2018 15:59 - Thomas Noël

misc: disable AuthnRequest eo:next_url Extensions by default (fixes #20229)

Historique

#1 - 22 novembre 2017 23:51 - Thomas Noël

- Lié à Development #18452: inclure l'url de destination dans le nœud Extensions ajouté

#2 - 23 novembre 2017 00:02 - Frédéric Péters

Pas exactement cette situation mais par exemple il est arrivé qu'un IdP Sun "digère" mal nos données pourtant conforme au spécifications. J'imagine qu'on pourrait pareillement ajouter la prise en compte d'un paramètre à l'URL des métadonnées fournies par django-mellon, déclarant que le <samlp:Extension> ne doit pas être inclus.

#3 - 23 novembre 2017 00:18 - Thomas Noël

- Statut changé de Nouveau à En cours

> est-ce que c'est possible tout simplement de ne pas générer la requête avec les extensions.

Non, l'extension est toujours ajoutée (ça vient de #18452 → https://git.entrouvert.org/django-mellon.git/commit/?id=646132c661af7269def3c76a8ee3bc43854429cd)

Ce qui pourrait être envisagé, c'est l'ajout d'un settings AUTHNREQUEST_EXTENSIONS, qui serait donc à True par défaut, mais pourrait être positionné à False, pour un IdP donné ou globalement.

Quelque chose dans le genre :

```
diff --git a/mellon/app_settings.py b/mellon/app_settings.py
index aeeab73..a595dab 100644
--- a/mellon/app_settings.py
+++ b/mellon/app_settings.py
@@ -13,6 +13,7 @@ class AppSettings(object):
         'NAME_ID_POLICY_FORMAT': None,
         'NAME_ID_POLICY_ALLOW_CREATE': True,
         'FORCE_AUTHN': False,
+        'ADD_AUTHNREQUEST_EXTENSIONS': True,
         'ADAPTER': (
             'mellon.adapters.DefaultAdapter',
         ),
diff --git a/mellon/views.py b/mellon/views.py
index e01dc13..4e83bec 100644
--- a/mellon/views.py
+++ b/mellon/views.py
@@ -363,14 +363,15 @@ class LoginView(ProfileMixin, LogMixin, View):
                 authn_request.requestedAuthnContext = req_authncontext
                 req_authncontext.authnContextClassRef = authn_classref

-            authn_request.extensions = lasso.Samlp2Extensions()
-            authn_request.extensions.setOriginalXmlnode(
-                    '''<samlp:Extensions
-                            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
-                            xmlns:eo="https://www.entrouvert.com/">
-                        <eo:next_url>%s</eo:next_url>
-                    </samlp:Extensions>''' %
-                escape(request.build_absolute_uri(next_url or '/')))
+            if utils.get_setting(idp, 'ADD_AUTHNREQUEST_EXTENSIONS'):
+                authn_request.extensions = lasso.Samlp2Extensions()
+                authn_request.extensions.setOriginalXmlnode(
+                        '''<samlp:Extensions
+                                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
+                                xmlns:eo="https://www.entrouvert.com/">
+                            <eo:next_url>%s</eo:next_url>
+                        </samlp:Extensions>''' %
+                    escape(request.build_absolute_uri(next_url or '/')))
             self.set_next_url(next_url)
             login.buildAuthnRequestMsg()
         except lasso.Error, e:
```

(idée que je soumets ici à mes collègues, mais tu peux déjà l'essayer localement, en ajoutant donc un MELLON_ADD_AUTHNREQUEST_EXTENSIONS=False dans les settings ; je ne garantie pas encore cependant que ça soit intégré ainsi dans le code, même si ça marche ;))

#4 - 23 novembre 2017 10:19 - Benjamin Dauvergne

Je verrai bien la valeur par défaut à False, transmettre l'URL finale sur le SP ce n'est pas anodin.

#5 - 23 novembre 2017 10:25 - Thomas Noël

- Fichier 0001-misc-disable-AuthnRequest-eo-next_url-Extensions-by-.patch ajouté

- Patch proposed changé de Non à Oui

Yep. Pour le nom du settings, peut-être plutôt ADD_AUTHNREQUEST_NEXT_URL_EXTENSION ?

Note internet EO : ça veut dire le positionner à True sur Publik (assez facile via hobo, en fait).

#6 - 07 mars 2018 15:55 - Benjamin Dauvergne

Ça ne concerne que GNM je ne crois pas qu'on utilise ça ailleurs pour l'instant.

#7 - 07 mars 2018 15:55 - Benjamin Dauvergne

Ack.

#8 - 07 mars 2018 15:59 - Benjamin Dauvergne

- Assigné à mis à Thomas Noël

#9 - 07 mars 2018 16:00 - Thomas Noël

- Statut changé de En cours à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit django-mellon|ac75dce84f5bd029d00f5a7d96d9d9d7d773acd0.

#10 - 07 mars 2018 16:07 - Thomas Noël

Ca impose un patch dans hobo, non ? (ADD_AUTHNREQUEST_NEXT_URL_EXTENSION=True quelque part)

#11 - 07 mars 2018 16:08 - Thomas Noël

Benjamin Dauvergne a écrit :

> Ça ne concerne que GNM je ne crois pas qu'on utilise ça ailleurs pour l'instant.

Ah, non, pas de patch hobo, donc, mais une modif des settings à poser à GNM sur tous les SP ?

#14 - 07 mars 2018 16:37 - Thomas Noël

- Lié à Bug #22352: activer l'envoi de l'extension eo:next_url par mellon (ADD_AUTHNREQUEST_NEXT_URL_EXTENSION) ajouté

#15 - 12 mars 2018 14:29 - Benjamin Dauvergne

- Sujet changé de ADFS 3.0 à Incompatibilité avec ADFS 3.0 à cause du noeud d'extension eo:next_url

#16 - 12 mars 2018 14:29 - Benjamin Dauvergne

- Version cible mis à 1.2.34

#17 - 25 octobre 2018 12:25 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-misc-disable-AuthnRequest-eo-next_url-Extensions-by-.patch	2,32 ko	23 novembre 2017	Thomas Noël