Distribution EOLE - Demande #17944

Rétrocompatibilité SSL de eole-sso en version 2.5

17/11/2016 22:58 - Jean-Marc MELET

Statut:	Ne sera pas résolu	**Début:**	17/11/2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Daniel Dehennin	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.25 heure

Description

Bonjour,

Dans notre académie nous sommes confrontés au problème suivant:
Le temps d'effectuer les campagnes de migrations de tous les modules de la version 2.3 en 2.5, nous maintenons un environnement mixte des 2 versions.
En particulier, nous avons actuellement des serveurs Amon 2.5.2 qui cohabitent avec des Horus et Scribe 2.3.16.
Cela nous pose un problème de compatibilité de eole-sso au niveau du contexte SSL.
En effet, nous utilisons le service eole-sso de l'Amon 2.5 pour gérer l'authentification des EAD de tous les modules (backend des Amon, Horus et Scribe sur le frontend d'Amon et configurés avec le SSO de l'Amon). Depuis le passage en Amon 2.5, nous ne pouvons plus accéder aux backend des EAD des modules 2.3.
Apres investigation, le problème semble se situer au niveau de la librairie SSL utilisée par le service eole-sso de la version 2.5:

Lorsque l'on tente d'accéder aux EAD des modules 2.3, rien ne se passe. Voici les logs de eole-sso sur l'Amon 2.5:

```
2016-11-17T21:30:09.804577+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] Unhandled Error
2016-11-17T21:30:09.812583+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011Traceback (most recent call last):
2016-11-17T21:30:09.812608+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/python/log.py", line 88, in c
allWithLogger
2016-11-17T21:30:09.812617+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    return callWithContext({"system": lp}, func, *args, **kw)
2016-11-17T21:30:09.812625+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/python/log.py", line 73, in c
allWithContext
2016-11-17T21:30:09.812633+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    return context.call({ILogContext: newCtx}, func, *args, **kw)
2016-11-17T21:30:09.812642+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/python/context.py", line 118,
 in callWithContext
2016-11-17T21:30:09.812650+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    return self.currentContext().callWithContext(ctx, func, *args, **kw)
2016-11-17T21:30:09.812657+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/python/context.py", line 81,
in callWithContext
2016-11-17T21:30:09.812665+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    return func(*args,**kw)
2016-11-17T21:30:09.812672+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011--- <exception caught here> ---
2016-11-17T21:30:09.812680+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/internet/posixbase.py", line
614, in _doReadOrWrite
2016-11-17T21:30:09.812707+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    why = selectable.doRead()
2016-11-17T21:30:09.812762+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/internet/tcp.py", line 215, i
n doRead
2016-11-17T21:30:09.812803+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    return self._dataReceived(data)
2016-11-17T21:30:09.812840+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/twisted/internet/tcp.py", line 221, i
```

```
n _dataReceived
2016-11-17T21:30:09.812950+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    rval = self.protocol.dataReceived(data)
2016-11-17T21:30:09.812990+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011  File "/usr/lib/python2.7/dist-packages/M2Crypto/SSL/TwistedProtocolWrapper.p
y", line 312, in dataReceived
2016-11-17T21:30:09.813027+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011    raise e
2016-11-17T21:30:09.813103+01:00 amon25.maket-labo.local eolesso: [HTTPChannel (TLSProtocolWrapper
),7,10.4.201.7] #011M2Crypto.BIO.BIOError: (0L, 'wrong version number')
```

Et les logs de ead-server sur les modules 2.3:

```
        Traceback (most recent call last):
          File "/usr/lib/python2.6/dist-packages/twisted/web/server.py", line 125, in process
            self.render(resrc)
          File "/usr/lib/python2.6/dist-packages/twisted/web/server.py", line 132, in render
            body = resrc.render(self)
          File "/usr/share/ead2/backend/lib/eadserver.py", line 190, in render
            defer.maybeDeferred(function, client_ip, *args).addErrback(
          File "/usr/lib/python2.6/dist-packages/twisted/internet/defer.py", line 117, in maybeDef
erred
            result = f(*args, **kw)
        --- <exception caught here> ---
          File "/usr/share/ead2/backend/lib/eadserver.py", line 406, in xmlrpc_get_magic_number
            app_path)
          File "/usr/lib/python2.6/xmlrpclib.py", line 1199, in __call__
            return self.__send(self.__name, args)
          File "/usr/lib/python2.6/xmlrpclib.py", line 1489, in __request
            verbose=self.__verbose
          File "/usr/lib/python2.6/xmlrpclib.py", line 1235, in request
            self.send_content(h, request_body)
          File "/usr/lib/python2.6/xmlrpclib.py", line 1349, in send_content
            connection.endheaders()
          File "/usr/lib/python2.6/httplib.py", line 904, in endheaders
            self._send_output()
          File "/usr/lib/python2.6/httplib.py", line 776, in _send_output
            self.send(msg)
          File "/usr/lib/python2.6/httplib.py", line 735, in send
            self.connect()
          File "/usr/lib/python2.6/httplib.py", line 1112, in connect
            self.sock = ssl.wrap_socket(sock, self.key_file, self.cert_file)
          File "/usr/lib/python2.6/ssl.py", line 350, in wrap_socket
            suppress_ragged_eofs=suppress_ragged_eofs)
          File "/usr/lib/python2.6/ssl.py", line 118, in __init__
            self.do_handshake()
          File "/usr/lib/python2.6/ssl.py", line 293, in do_handshake
            self._sslobj.do_handshake()
        ssl.SSLError: [Errno 8] _ssl.c:480: EOF occurred in violation of protocol
```

Apres avoir effectué quelques tests, nous avons pu constater que le fait de remplacer ctx = SSL.Context(protocol='tlsv1') par ctx = SSL.Context(protocol='sslv23') dans le fichier /usr/lib/python2.7/dist-packages/eolesso/libsecure.py règle le problème.

Est-il donc possible d'apporter un correctif afin d'assurer la compatibilité SSL entre les différentes versions?

Historique

#1 - 21/11/2016 09:22 - Daniel Dehennin

- Assigné à mis à Daniel Dehennin

#2 - 21/11/2016 10:19 - Daniel Dehennin

- Statut changé de Nouveau à Ne sera pas résolu

Bonjour,

Les protocoles SSL2 et SSL3 sont dépréciés depuis longtemps et des attaques sur ces protocoles existent, l'ANSII préconise donc leur désactivation.

La désactivation du support de SSLv3 a été initié sur EOLE 2.4 et complètement finalisé sur EOLE 2.5.

Vous pouvez contourner ce problème en activant la **redirection de l'EAD Scribe** sur l'Amon :

- **activer_revprox_ead** ⇒ **oui**
- **revprox_ead** ⇒ IP du scribe
- **revprox_ead_port** ⇒ port de l'EAD du scribe

Ainsi, la communication entre les stations clientes et l'établissement se fait avec un protocole de chiffrement récent, seul la communication entre le reverse proxy et le scribe sont en SSLv3.

#3 - 23/11/2016 15:15 - Jean-Marc MELET

Oui sauf que, sauf erreur de ma part, cela ne résoud pas le problème évoqué car il concerne la communication entre les backend des 2.3 et le service SSO de la 2.5 (nous utilisons le serveur eole-sso de l'amon 2.5), je peux me tromper mais à priori je ne vois pas ce que l'utilisation du reverse proxy changerait à ce niveau. De plus:

- Votre proposition implique de devoir modifier toutes nos conf pour passer en mode reverse proxy
- Sauf erreur de ma part, nous ne pourrons pas gérer un Scribe ET un Horus par cette méthode (il faudrait rediriger 2 EAD et le reverse proxy n'en prévoit qu'un seul)

Bon je ne vais pas vous déranger plus là-dessus surtout qu'il est question de se conformer aux recommandations SSI, mais cela nous handicape car ce problème est ressenti pour les correspondants administrateurs locaux comme une régression.
Nous allons consulter notre pôle SSI pour voir si on peut faire une entorse à la sécurité et faire un patch pour activer le support SSLv2/v3, au moins le temps que nous basculions tous nos modules en 2.5

P.S: merci de me faire savoir (par mail par ex) si mon analyse est bonne et mes remarques sont justifiées car je suis peut-être dans l'erreur.

Cordialement

#4 - 23/11/2016 15:32 - Daniel Dehennin

Jean-Marc MELET a écrit :

> Oui sauf que, sauf erreur de ma part, cela ne résoud pas le problème évoqué car il concerne la communication entre les backend des 2.3 et le service SSO de la 2.5 (nous utilisons le serveur eole-sso de l'amon 2.5), je peux me tromper mais à priori je ne vois pas ce que l'utilisation du reverse proxy changerait à ce niveau. De plus:

Exact, j’ai cru qu’il s’agissait d’avoir les serveurs référencés dans l’EAD de l’amon pour l’accès extérieur.

- Votre proposition implique de devoir modifier toutes nos conf pour passer en mode reverse proxy
- Sauf erreur de ma part, nous ne pourrons pas gérer un Scribe ET un Horus par cette méthode (il faudrait rediriger 2 EAD et le reverse proxy n'en prévoit qu'un seul)

Le dictionnaire de l’Amon ne prévoir de facilité que la mise en place du reverse proxy pour le scribe, il est possibl d’ajouter un reverse proxy de plus en spécifiant tous les paramètres.

Bon je ne vais pas vous déranger plus là-dessus surtout qu'il est question de se conformer aux recommandations SSI, mais cela nous handicape car ce problème est ressenti pour les correspondants administrateurs locaux comme une régression.
Nous allons consulter notre pôle SSI pour voir si on peut faire une entorse à la sécurité et faire un patch pour activer le support SSLv2/v3, au moins le temps que nous basculions tous nos modules en 2.5

Malheureusement, sur ce genre de point il est de plus en plus difficile de trouver des « solution », les navigateurs web devenant eux aussi de plus en plus restrictifs.

P.S: merci de me faire savoir (par mail par ex) si mon analyse est bonne et mes remarques sont justifiées car je suis peut-être dans l'erreur.

Je pense qu’il est préférable d’avoir l’avis de votre RSSI avant toute modification, pour notre part nous ne pouvons pas ouvrir ces brêches pour tous les serveurs de nos utilisateurs.