

EoleSSO - Demande #16712

Problème de validation de mon portail posh en proxy CAS via eole-sso

06/07/2016 17:27 - Nicolas Penot

Statut:	Pas un bug	Début:	06/07/2016
Priorité:	Normal	Echéance:	
Assigné à:	Bruno Boiget	% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:		Temps passé:	0.50 heure
Description			
Bonjour, J'ai actuellement un problème lorsque mon portail posh demande à devenir proxy CAS auprès du eole-sso. <u>Petit état des lieux :</u> 1er serveur 2.5.2 : eole-base + eole-sso => seshat1.ac-caen.fr => Le serveur est derrière une VIP sso.ac-caen.fr détenue par notre répartiteur de charge F5 Big IP. 2ème serveur 2.5.2 : eole-base + eole-web + envole => applicas1.ac-caen.fr => Le serveur est derrière une VIP appintranet.ac-caen.fr détenue par notre répartiteur de charge F5 Big IP. Le serveur seshat1 est configuré avec un LDAP distant, l'authentification sur l'adresse sso.ac-caen.fr fonctionne bien avec les identifiants LDAP. <pre>2016-07-06T15:23:18.922784+02:00 seshat1.ac-caen.fr eolessso: [LDAPClient,client] user authentication verified uid: lsaroyan, cn: Leopoldine Saroyan. Session ID : TGC-sso.ac-caen.fr-272ce351808eccd015fbb73cd359d9f34af98ef9c021dd67e56c7e30 (1 sessions)</pre> Le serveur applicas1 a son serveur web qui tourne sur l'adresse appintranet.ac-caen.fr. Le eole-sso distant défini est sso.ac-caen.fr. J'accède à mon portail en tapant directement l'adresse appintranet.ac-caen.fr. Il me redirige correctement vers le sso. https://sso.ac-caen.fr/login?service=http://appintranet.ac-caen.fr/envole/portal/login.php Quand je rentre mes identifiants et les valide, je suis redirigé puis je reste bloqué sur : <pre>https://appintranet.ac-caen.fr/envole/portal/login.php?ticket=ST-sso.ac-caen.fr-a30319bfe4812b39ad6520892a0df55a6e58970c1a16509f746227fd</pre> Et dans les logs eolessso-infos : <pre>2016-07-06T15:44:44.106379+02:00 seshat1.ac-caen.fr eolessso: [LDAPClient,client] user authentication verified uid: lsaroyan, cn: Leopoldine Saroyan. Session ID : TGC-sso.ac-caen.fr-f0be78e0715dfb6965f352308a6cea030c45f6741ablef035d3d4669 (1 sessions) 2016-07-06T15:44:44.106763+02:00 seshat1.ac-caen.fr eolessso: [LDAPClient,client] TGC-sso.ac-caen.fr-f0be78e0715dfb6965f352308a6cea030c45f6741ablef035d3d4669 -- Session autorisée pour le service http://appintranet.ac-caen.fr/envole/portal/login.php (filtre de données : default) 2016-07-06T15:44:44.106927+02:00 seshat1.ac-caen.fr eolessso: [LDAPClient,client] Redirection vers l'application appelante avec le ticket : http://appintranet.ac-caen.fr/envole/portal/login.php 2016-07-06T15:44:44.545216+02:00 seshat1.ac-caen.fr eolessso: [HTTPChannel (TLSProtocolWrapper),66714,192.168.5.155] TGC-sso.ac-caen.fr-f0be78e0715dfb6965f352308a6cea030c45f6741ablef035d3d4669 -- Demande d'un ticket PGT pour devenir proxy CAS auprès du service http://appintranet.ac-caen.fr:443/envole/portal/login.php 2016-07-06T15:44:44.545556+02:00 seshat1.ac-caen.fr eolessso: [HTTPChannel (TLSProtocolWrapper),667</pre>			

```

14,192.168.5.155] Starting factory <HTTPClientFactory: https://appintranet.ac-caen.fr:443/envole/p
ortal/login.php>
2016-07-06T15:44:44.545697+02:00 seshat1.ac-caen.fr eolessso: [HTTPChannel (TLSProtocolWrapper),667
14,192.168.5.155] Starting factory <twisted.protocols.policies.WrappingFactory instance at 0x7fc96
ec49f80>
2016-07-06T15:44:44.598688+02:00 seshat1.ac-caen.fr eolessso: [HTTPPageGetter (TLSProtocolWrapper),
client] Stopping factory <twisted.protocols.policies.WrappingFactory instance at 0x7fc96ec49f80>
2016-07-06T15:44:44.803701+02:00 seshat1.ac-caen.fr eolessso: [HTTPPageGetter (TLSMemoryBIOProtocol
),client] !! Unable to obtain PGT for service http://appintranet.ac-caen.fr:443/envole/portal/logi
n.php !!
2016-07-06T15:44:44.803967+02:00 seshat1.ac-caen.fr eolessso: [HTTPPageGetter (TLSMemoryBIOProtocol
),client] ! Lecture des données utilisateur : session invalide !
2016-07-06T15:44:44.804089+02:00 seshat1.ac-caen.fr eolessso: [HTTPPageGetter (TLSMemoryBIOProtocol
),client] ! Lecture des données utilisateur refusée pour le service http://appintranet.ac-caen.fr:
443/envole/portal/login.php !
2016-07-06T15:44:44.804586+02:00 seshat1.ac-caen.fr eolessso: [HTTPPageGetter (TLSMemoryBIOProtocol
),client] Stopping factory <HTTPClientFactory: https://sso.ac-caen.fr:443/login?service=http://app
intranet.ac-caen.fr/envole/portal/login.php>

```

Sur IRC, chan ENVOLE, Arnaud m'a conseillé de mettre le debug du phpcas pour voir si il n'y avait pas d'erreur de certificat. Sur applicas1, j'ai donc activé le debug dans /usr/share/php/configCAS/cas.inc.php. Je joins le fichier phpcas-posh.log à ce ticket.

Concernant les certificats...

1er certif : sso.ac-caen.fr => positionné sur la VIP, j'ai choisi de l'utiliser sur mon serveur seshat1 car le but est de faire du failover et d'avoir un seshat2 dans un futur très proche.

Chemin du certif : voir capture GenConfig-certifssl-seshat1.png et GenConfig-eolessso-seshat1.png

J'ai concaténé dans mon certif sso.ac-caen.fr.crt l'ensemble de la chaîne de certification :

```

root@seshat1:/etc/ssl/certs# ./voir_all_certif.sh sso.ac-caen.fr.crt
-----
      Not After : Jul  6 12:00:00 2018 GMT
      Subject: businessCategory=Government Entity/1.3.6.1.4.1.311.60.2.1.3=FR/serialNumber=Gover
nment Entity/street=168 rue Caponi\xC3\xA8re/postalCode=14061, C=FR, ST=Normandie, L=Caen Cedex, O
=Acad\xC3\xA9mie de Caen, OU=ac-caen.fr, CN=sso.ac-caen.fr
      Subject Public Key Info:
      X509v3 Subject Key Identifier:
      X509v3 Subject Alternative Name:
-----

      Not After : Nov 18 12:00:00 2024 GMT
      Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL High Assurance CA 3
      Subject Public Key Info:
      X509v3 Subject Key Identifier:
-----

      Not After : Nov 10 00:00:00 2031 GMT
      Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA
      Subject Public Key Info:
      X509v3 Subject Key Identifier:
-----

```

Les certificats intermédiaires et racines (de sso.ac-caen.fr et appintranet.ac-caen.fr) ont été placés dans le local_ca de seshat1, ce qui nous fait un ca.crt :

```

root@seshat1:/etc/ssl/certs# ./voir_all_certif.sh ca.crt
-----
      Not After : Jun 24 13:24:41 2019 GMT
      Subject: C=FR, O=Ministere Education Nationale (MENESR), OU=110 043 015, OU=ac-caen, CN=CA
-seshat1
      Subject Public Key Info:
      X509v3 Subject Key Identifier:
-----

```

```

    Not After : Dec 22 10:00:00 2015 GMT
    Subject: C=FR, O=Ministere education nationale (MENESR), OU=110 043 015, CN=AC Infrastruct
ures
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Dec 22 11:00:00 2015 GMT
    Subject: emailAddress=igc@orion.education.fr, C=FR, O=Ministere Education Nationale (MENES
R), OU=110 043 015, CN=AC Enseignement Scolaire
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Dec 22 14:00:00 2015 GMT
    Subject: emailAddress=igc@orion.education.fr, C=FR, O=Ministere Education Nationale (MENES
R), OU=110 043 015, CN=AC Education Nationale
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Oct 17 14:29:22 2020 GMT
    Subject: C=FR, ST=France, L=Paris, O=PM/SGDN, OU=DCSSI, CN=IGC/A/emailAddress=igca@sgdn.pm
.gouv.fr
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Nov 18 12:00:00 2024 GMT
    Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL High Assurance CA 3
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Nov 10 00:00:00 2031 GMT
    Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Feb 15 12:00:00 2019 GMT
    Subject: C=FR, ST=Normandie, L=Caen Cedex, O=Acad\xC3\xA9mie de Caen, OU=ac-caen, CN=appin
tranet.ac-caen.fr
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
    X509v3 Subject Alternative Name:
-----
    Not After : Feb 8 16:06:30 2019 GMT
    Subject: C=FR, O=Ministere Education Nationale (MENESR), OU=110 043 015, OU=ac-caen, CN=ap
plicas1.014080216A.ac-caen.fr
    Subject Public Key Info:
    X509v3 Subject Alternative Name:
-----
    Not After : Nov 18 12:00:00 2024 GMT
    Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----
    Not After : Nov 10 00:00:00 2031 GMT
    Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA
    Subject Public Key Info:
    X509v3 Subject Key Identifier:
-----

```

2ème certif : appintranet.ac-caen.fr => positionné sur la VIP, j'ai choisi de l'utiliser sur mon serveur applicas1 car le but est de la répartition de charge dans un futur un peu moins proche avec un applicas2.

Chemin du certif : voir capture GenConfig-certifssl-applicas1.png

Mon certif appintranet.ac-caen.fr :

```
root@applicas1:/etc/ssl/certs/PIA# ./voir_all_certif.sh appintranet.ac-caen.fr.crt
-----
Not After : Feb 15 12:00:00 2019 GMT
Subject: C=FR, ST=Normandie, L=Caen Cedex, O=Acad\xC3\xA9mie de Caen, OU=ac-caen, CN=appin
tr Janet.ac-caen.fr
Subject Public Key Info:
X509v3 Subject Key Identifier:
X509v3 Subject Alternative Name:
-----
```

Les certificats intermédiaires et racines (de sso.ac-caen.fr et appintranet.ac-caen.fr) ont été placés dans le local_ca de seshat1, ce qui nous fait un ca.crt :

```
root@applicas1:/etc/ssl/certs/PIA# ./voir_all_certif.sh ../ca.crt
-----
Not After : Feb 8 16:06:30 2019 GMT
Subject: C=FR, O=Ministere Education Nationale (MENESR), OU=110 043 015, OU=ac-caen, CN=CA
-appl icas1
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Dec 22 10:00:00 2015 GMT
Subject: C=FR, O=Ministere education nationale (MENESR), OU=110 043 015, CN=AC Infrastruct
ures
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Dec 22 11:00:00 2015 GMT
Subject: emailAddress=igc@orion.education.fr, C=FR, O=Ministere Education Nationale (MENES
R), OU=110 043 015, CN=AC Enseignement Scolaire
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Dec 22 14:00:00 2015 GMT
Subject: emailAddress=igc@orion.education.fr, C=FR, O=Ministere Education Nationale (MENES
R), OU=110 043 015, CN=AC Education Nationale
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Oct 17 14:29:22 2020 GMT
Subject: C=FR, ST=France, L=Paris, O=PM/SGDN, OU=DCSSI, CN=IGC/A/emailAddress=igca@sgdn.pm
.gouv.fr
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Nov 10 00:00:00 2031 GMT
Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Jul 6 12:00:00 2018 GMT
Subject: businessCategory=Government Entity/1.3.6.1.4.1.311.60.2.1.3=FR/serialNumber=Gover
nment Entity/street=168 rue Caponi\xC3\xA8re/postalCode=14061, C=FR, ST=Normandie, L=Caen Cedex, O
=Acad\xC3\xA9mie de Caen, OU=ac-caen.fr, CN=sso.ac-caen.fr
Subject Public Key Info:
X509v3 Subject Key Identifier:
X509v3 Subject Alternative Name:
-----
Not After : Nov 18 12:00:00 2024 GMT
Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL High Assurance CA 3
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
```

```
Not After : Nov 10 00:00:00 2031 GMT
Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
Not After : Nov 18 12:00:00 2024 GMT
Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
Subject Public Key Info:
X509v3 Subject Key Identifier:
-----
```

Voilà, désolé pour la longueur du ticket mais je voulais vous donner le maximum d'infos dès le début.
En vous remerciant d'avance,

Nicolas PENOT, Rectorat de Caen.

Historique

#1 - 07/07/2016 12:00 - Bruno Boiget

- Statut changé de Nouveau à En attente d'informations

A priori, le problème ne doit pas venir du certificat, dans ce cas eole-sso aurait indiqué une erreur ssl soit par rapport à un nom de domaine invalide, soit par rapport à la signature du certificat par la CA.

Au vu du message suivant, je pense que le problème vient plutôt du fait que le service est en http et non https (https est obligatoire pour les applications en mode proxy) :

```
!! Unable to obtain PGT for service http://appintranet.ac-caen.fr:443/envole/portal/login.php !!
```

Il faudrait peut être vérifier la configuration du reverse-proxy pour qu'il renvoie toujours en https (surtout qu'ici, on a http sur le port 443, ce n'est pas logique) .

#2 - 07/07/2016 17:37 - Bruno Boiget

- Assigné à mis à Bruno Boiget

#3 - 07/07/2016 17:39 - Nicolas Penot

Je vois pour forcer la redirection http vers https et je te tiens au courant !

Merci ;)
Nicolas.

#4 - 08/07/2016 11:31 - Nicolas Penot

Bonjour Bruno,

Effectivement, c'était un paramètre sur notre répartiteur de charge qui n'était pas correct et qui redirigé en HTTP au lieu du HTTPS... L'équipe réseau

l'a corrigé.

Tout ça, pour ça... Que de temps perdu.

En tout cas, je tiens à te remercier chaudement pour l'œil avisé dont tu as fait preuve ! Je n'avais pas vu que j'étais redirigé en HTTP...

Encore merci !

Nicolas.

#5 - 11/07/2016 09:51 - Bruno Boiget

- Statut changé de *En attente d'informations* à *Pas un bug*

Je clôture la demande.

Fichiers

authentif-ldap-ok.png	132 ko	06/07/2016	Nicolas Penot
authentif-redirect-posh-sso.png	128 ko	06/07/2016	Nicolas Penot
GenConfig-certifssl-applicas1.png	37,9 ko	06/07/2016	Nicolas Penot
GenConfig-certifssl-seshat1.png	41,9 ko	06/07/2016	Nicolas Penot
GenConfig-eolessso-seshat1.png	26 ko	06/07/2016	Nicolas Penot
phpcas-posh.log	10,3 ko	06/07/2016	Nicolas Penot