Distribution EOLE - Demande #24017

Problème interconnexion Amon <-> Seth proxy authentifié LDAP

30/05/2018 14:16 - Serge COUDE

Statut:	Pas un bug	**Début:**	30/05/2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Fabrice Barconnière	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	1.00 heure

Description

Bonjour,

je découvre l'ensemble de votre solution que je trouve sensas !

Je tente de faire communiquer deux serveurs distincts au niveau de l'authentification proxy en ldap (AD) :

Amon (10.4.0.3)
et
Seth (10.4.0.245)

J'ai créé sur Seth un utilisateur "etudiant" en ligne de commande, il est bien listé en tant qu'utilisateur.

Les ports 636 et 389 sont bien ouverts et écoutés par Samba sur Seth.
Je peux faire un telnet depuis Amon vers Seth sur le port 389.

Mais lorsque je vais sur Internet, le proxy me demande bien mon identification (je lui fournis "etudiant" et le mot de passe qui va bien), mais squid ne semble pas être "d'accord" avec ce je lui fournis...

Voici le log que j'ai sur Amon:/var/log/squid/cache.log

basic_ldap_auth: WARNING, could not bind to binddn 'Strong(er) authentication required'

J'ai tenté de faire un test en ligne de commande :

/usr/lib/squid/basic_ldap_auth -d -b "cn=Users,dc=issat,dc=local" -H ldap://10.4.0.245
et d'autres encore mais le script ne semble rien faire : il attend, quoi, je ne sais pas...
et donc je fini par un ^C...

Je ne sais pas d'où viens le problème...

Pouvez-vous m'éclairer ?

Merci beaucoup par avance !

Serge COUDÉ

Historique

#1 - 31/05/2018 09:08 - Fabrice Barconnière

- Statut changé de Nouveau à En attente d'informations

- Assigné à mis à Fabrice Barconnière

Bonjour,

Merci pour le compliment.

Concernant votre problème, il se situe certainement au niveau de la configuration du serveur Amon.
Le serveur Seth est un Active Directory, il faut donc paramétrer l'authentification de Squid sur Amon de type Kerberos :
http://eole.ac-dijon.fr/documentations/2.6/completes/HTML/ModuleAmon/co/44-authentificationSquidPourSeth.html

Si ce n'est pas déjà fait, vous pouvez vous inscrire aux listes (http://listeseole.ac-dijon.fr/listes) afin d'échanger avec la communauté des utilisateurs et

développeurs.
Il existe également un canal IRC sur Freenode : #eole

En effet, les demandes sur la forges sont destinées aux bugs avérés ou aux demandes d'évolution.
Pouvez-vous faire un retour sur cette demande afin de confirmer que la réponse correspond bien à vos besoins ?

Cordialement,
Fabrice Barconnière

#2 - 31/05/2018 13:23 - Serge COUDE

Bonjour Fabrice,

merci pour votre retour. J'ai configuré comme indiqué dans la page, cela ne fonctionne toujours pas mais les messages ont évolués :

lorsque je saisi mon identifiant / mot de passe, il ne me le redemande plus, mais m'affiche une page "vide" (le navigateur affiche "Aucune donnée reçue").
J'ai regardé dans les log de squid, l'erreur que j'avais avant n'apparaît plus. Par contre dans les logs de syslog, j'ai maintenant cela :

```
2018-05-31T12:57:26.734928+02:00 amon.toto.local e2guardian0[19740]: NTLM - step 2 was not part of an auth han
dshake! (HTTP/1.1 200 OK#015)
2018-05-31T12:57:26.735085+02:00 amon.toto.local e2guardian0[19740]: Auth plugin returned error code: -1
2018-05-31T12:57:26.762235+02:00 amon.toto.local e2guardian0[19740]: NTLM - step 2 was not part of an auth han
dshake! (HTTP/1.1 200 OK#015)
2018-05-31T12:57:26.762545+02:00 amon.toto.local e2guardian0[19740]: Auth plugin returned error code: -1
2018-05-31T12:57:49.424573+02:00 amon.toto.local e2guardian0[19740]: NTLM - step 2 was not part of an auth han
dshake! (HTTP/1.1 200 Connection established#015)
2018-05-31T12:57:49.424762+02:00 amon.toto.local e2guardian0[19740]: Auth plugin returned error code: -1
```

J'ai fait un diagnose sur les deux serveurs :
amon :

```
*** Services distants
.    Passerelle 192.168.100.1 => Ok
.             DNS 10.4.0.245 => Ok

.          DNS 192.168.100.1 => Ok

.                 Statut NTP => Synchronisé

.              Accès distant => Ok
*** Validité du certificat
.                   eole.crt => Ok
.                DNS reconnus => amon.issat.local
*** DNS local
.              DNS 127.0.0.1 => Ok

*** Services Proxy
.              Service proxy => Ok
.  enregistrement NTLM/KERBEROS => Ok
.            web via proxy 1 => Ok
.            web via proxy 1 => Ok
.            web via proxy 1 => Ok
.            web via proxy 1 => Ok
```

et sur seth :

```
*** Services distants
.         Passerelle 10.4.0.1 => Ok
.                DNS 10.4.0.3 => Ok
```

```
.                  Statut NTP => Synchronisé

.               Serveur Proxy => Ok

.               Accès distant => Ok
*** Validité du certificat
.                    eole.crt => Ok
.                DNS reconnus => seth.toto.local
DNS AD :
.         Enregistrements SRV => Ok
.   Résolution seth.toto.local => Ok
```

C'est grave docteur ???

Merci par avance pour votre retour !

Bien cordialement,

Serge

#3 - 31/05/2018 13:25 - Serge COUDE

J'oubliais : j'ai réinstallé le serveur seth, avec comme nouveau domaine toto.local pour ne pas "interférer" avec le vrai domaine en prod...

#4 - 01/06/2018 08:48 - Fabrice Barconnière

Bonjour,

Il y a plusieurs points à respecter pour paramétrer ce type d'authentification. Seth est un AD, donc il devient serveur DNS master de sa zone (toto.local dans votre cas).

- Configuration de l'authentification Squid sur Amon dans l'onglet **Proxy authentifié** :
  - Type d'authentification **NTLM/Kerberos** :
    http://eole.ac-dijon.fr/documentations/2.6/completes/HTML/ModuleAmon/co/012-configurationAuthentificationNormal.html#ycN14e
    - Les postes joints au domaine AD de Seth seront authentifiés sans avoir besoin de saisir de login/MDP si le proxy IP_Amon/3128 est bien déclaré dans le navigateur
  - Pour les postes hors domaine, il faut **Activer le proxy NTLM** :
    http://eole.ac-dijon.fr/documentations/2.6/completes/HTML/ModuleAmon/co/012-configurationAuthentificationNormal.html#ycN18c
    - Les postes non joints au domaine AD de Seth seront authentifiés après avoir saisi un login/MDP si le proxy IP_Amon/3127 (port par défaut et paramétrable) est bien déclaré dans le navigateur ou en détection automatique de proxy (WPAD) :
      http://eole.ac-dijon.fr/documentations/2.6/completes/HTML/ModuleAmon/co/012-configurationAuthentificationNormal.html#ycN14e
- Amon doit être joint au domaine AD de Seth pour que cela fonctionne. Il faut lui indiquer le serveur Seth comme forward DNS pour toto.local :
  - En **mode Expert** / Onglet **Zones-dns** / **Déclarer des zones DNS à forwarder** à **oui**
    - http://eole.ac-dijon.fr/documentations/2.6/completes/HTML/ModuleAmon/co/01_ongletZonesDNS.html
    - Renseigner le domaine **toto.local** et l'adresse IP de Seth
  - Reconfigurer Amon
  - Joindre le serveur Amon au domaine AD de Seth : commande **enregistrement_domaine.sh**

Voilà, j'espère ne rien avoir oublié

#5 - 01/06/2018 10:04 - Serge COUDE

Bonjour Fabrice,

super, je viens de revérifier les différents points que vous avez donné :

il me manquait juste le proxy ntml à activer... Mon poste de test étant sous Linux, il était hors domaine, et je tentais la connexion sur le port 3128...
En démarrant le proxy ntlm, à l'écoute par défaut sur le port 3127, et en reconfigurant le proxy de mon navigateur, j'ai pu m'authentifier et avoir accès au Web !
Je vais pouvoir voir à le déployer dans l'établissement maintenant !

Merci beaucoup pour votre accompagnement !

Bien cordialement,

Serge

#6 - 06/06/2018 08:21 - Fabrice Barconnière

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

- % réalisé changé de 0 à 100

Bonjour,

Heureux de voir que tout fonctionne pour vous.
Je clôture la demande.

Cordialement,
Fabrice Baronnière