

eole-proxy - Tâche #33458

Scénario # 33299 (Terminé (Sprint)): Etude Proxy 2.8.1 krb5

Etude

29/11/2021 14:12 - Emmanuel GARETTE

Statut:	Fermé	Début:	15/11/2021
Priorité:	Normal	Echéance:	
Assigné à:	Emmanuel GARETTE	% réalisé:	100%
Version cible:	Prestation Cadoles MEN 2021 46-49	Temps estimé:	0.00 heure
		Temps passé:	0.00 heure
Description			

Historique

#1 - 29/11/2021 14:13 - Emmanuel GARETTE

- Statut changé de Nouveau à En cours

#2 - 29/11/2021 16:13 - Emmanuel GARETTE

Démarrage de l'environnement :

```
etb1.amon-2.8.1-instance-default
etb1.scribe-2.8.1-instance-AvecImport
etb1.pccprofs-10.21H1
```

Si Amon :

```
apt install krb5-user msktutil
```

Le template /usr/share/eole/creole/distrib/proxy.krb5.conf :

```
[libdefaults]
default_realm = %%nom_domaine_krb.upper()
dns_lookup_realm = false
dns_lookup_kdc = false
default_keytab_name = FILE:/etc/squid/HTTP.keytab
default_etypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5 des-cbc-crc des-cbc-md5
default_tgs_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
default_tkt_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
permitted_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5

[realms]
%%nom_domaine_krb.upper() = {
    kdc = %%nom_serveur_krb.%%nom_domaine_krb:88
    admin_server = %%nom_serveur_krb.%%nom_domaine_krb:749
    default_domain = %%nom_serveur_krb.%%nom_domaine_krb
}

[domain_realm]
.%%nom_serveur_krb.%%nom_domaine_krb = %%nom_domaine_krb.upper()
%%nom_serveur_krb.%%nom_domaine_krb = %%nom_domaine_krb.upper()
```

Le template /usr/share/eole/creole/distrib/smb-proxy_auth.conf :

```
[global]
# Oblige samba d'encrypter les échanges avec mot de passe chiffré
encrypt passwords = true
# Nom NetBios de la machine serveur squid
%if %%mode_conteneur_actif == 'non'
    netbios name = %%nom_machine
%else
    netbios name = %%container_name_proxy
```

```

interfaces = %%adresse_ip_eth1_proxy_link
%end if
server string = %h server (Samba %v)
# Amon n'a pas vocation à être contrôleur principal d'un domaine
local master = no
domain master = no
preferred master = no
os level = 0
# La plage uid/gid pour le mappage des comptes windows
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind use default domain = yes
%if %%type_squid_auth == 'NTLM/SMB'
%set %%workgroup = %%nom_domaine_smb
%set %%security = "domain"
%set %%password = %%nom_serveur_smb
%else if %%type_squid_auth == 'NTLM/KERBEROS'
%set %%workgroup = %%nom_domaine_windows
%set %%security = "ADS"
%set %%password = %%lower(%%nom_serveur_krb+"."+%%nom_domaine_krb)
%end if
# Configuration du domaine
workgroup = %%upper(%%workgroup)
security = %%security
password server = %%password
%if %%type_squid_auth == 'NTLM/SMB'
wins server = %%ip_serveur_smb
%else if %%type_squid_auth == 'NTLM/KERBEROS'
realm = %%upper(%%nom_domaine_krb)
kerberos method = secrets and keytab
%end if

```

Modifier le template /usr/share/eole/creole/distrib/01squid.conf :

Remplacer le bloc :

```

%if %%type_squid_auth == 'NTLM/KERBEROS'
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children %%number_of_ntlm_children
#auth_param ntlm max_challenge_reuses 0
#auth_param ntlm max_challenge_lifetime 2 minutes

auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
%end if

```

Par :

```

%if %%type_squid_auth == 'NTLM/KERBEROS'
auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -d -s "HTTP/%%nom_machine.%%nom_domaine_krb@%%nom_domaine_krb.upper()"
auth_param negotiate children %%number_of_ntlm_children
auth_param negotiate keep_alive on

auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
%end if

```

Dans le fichier /usr/share/eole/creole/dicos/23_proxy.xml

Ajouter après :

```
<file filelist='kerberos' name='/etc/samba/lmhosts' mkdir='True'/>
```

La ligne :

```
<file filelist='kerberos' name='/etc/krb5.conf' source="proxy.krb5.conf"/>
```

Faire reconfigurer

```
root@amon:~# kinit Administrator@DOMPEDAGO.ETB1.LAN
Password for Administrator@DOMPEDAGO.ETB1.LAN:
root@amon:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@DOMPEDAGO.ETB1.LAN
```

```
Valid starting      Expires            Service principal
29/11/2021 16:15:13 30/11/2021 02:15:13 krbtgt/DOMPEDAGO.ETB1.LAN@DOMPEDAGO.ETB1.LAN
    renew until 30/11/2021 16:15:03
```

```
mskutil -c -b "CN=COMPUTERS" -s HTTP/amon.dompedago.etb1.lan -h amon.dompedago.etb1.lan -k /etc/squid/HTTP.keytab --computer-name squid-http --upn HTTP/amon.dompedago.etb1.lan --server addc.dompedago.etb1.lan --verbose --enctypes 28
```

Vérification du ticket :

```
root@amon:~# klist -ke /etc/squid/HTTP.keytab
Keytab name: FILE:/etc/squid/HTTP.keytab
KVNO Principal
```

```
-----
 5 squid-http$@DOMPEDAGO.ETB1.LAN (arcfour-hmac)
 5 squid-http$@DOMPEDAGO.ETB1.LAN (aes128-cts-hmac-sha1-96)
 5 squid-http$@DOMPEDAGO.ETB1.LAN (aes256-cts-hmac-sha1-96)
 5 SQUID-HTTP$@DOMPEDAGO.ETB1.LAN (arcfour-hmac)
 5 SQUID-HTTP$@DOMPEDAGO.ETB1.LAN (aes128-cts-hmac-sha1-96)
 5 SQUID-HTTP$@DOMPEDAGO.ETB1.LAN (aes256-cts-hmac-sha1-96)
 5 HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (arcfour-hmac)
 5 HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (aes128-cts-hmac-sha1-96)
 5 HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (aes256-cts-hmac-sha1-96)
 5 host/amon@DOMPEDAGO.ETB1.LAN (arcfour-hmac)
 5 host/amon@DOMPEDAGO.ETB1.LAN (aes128-cts-hmac-sha1-96)
 5 host/amon@DOMPEDAGO.ETB1.LAN (aes256-cts-hmac-sha1-96)
 5 host/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (arcfour-hmac)
 5 host/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (aes128-cts-hmac-sha1-96)
 5 host/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN (aes256-cts-hmac-sha1-96)
```

On a bien le principale "[HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN](#)" encodé en "aes256-cts-hmac-sha1-96"

Tester le fonctionnement depuis l'Amon :

```
root@amon:~# kinit -k -t /etc/squid/HTTP.keytab HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN
root@amon:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN
```

```
Valid starting      Expires            Service principal
03/12/2021 12:07:50 03/12/2021 22:07:50 krbtgt/DOMPEDAGO.ETB1.LAN@DOMPEDAGO.ETB1.LAN
    renew until 04/12/2021 12:07:50
```

```
root@amon:~# /usr/lib/squid/negotiate_kerberos_auth_test amon.dompedago.etb1.lan | awk '{sub(/Token:/, "YR"); print $0}END{print "QQ"}'|/usr/lib/squid/negotiate_kerberos_auth -d -k /etc/squid/HTTP.keytab -s HTTP/amon.dompedago.etb1.lan@DOMPEDAGO.ETB1.LAN
negotiate_kerberos_auth.cc(489): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Starting version 3.1.0sq
negotiate_kerberos_auth.cc(548): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Setting keytab to /etc/squid/HTTP.keytab
negotiate_kerberos_auth.cc(571): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Changed keytab to MEMORY:negotiate_kerberos_auth_15838
negotiate_kerberos_auth.cc(612): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: DEBUG: Got 'YR YIIGdAYGKwYBBQUCoIIIGaDCCBmSgDTALBqkqhkiG9xIBAgKiggZRBIIIGTWCCBkkGCSqGSIb3EgECAgEAbOIGODCCBjSgAwIBBaEDAgEOogcDBQAAAAAo4IFLWGCBSkwggUloAMCAQWhFBsSRE9NUEVEQUdPlkVUQjEueTEFOoiIwIKADAgEDoRkWFxsESFRUUBsPcGVkYWdV0YjEubGFuo4IE4jCCBN6gAwIBEqEDAgEGooIEOASCBMyAWONhossCXTG0wNKsXzhpP2sWoYjfi0NhEp79vBVVOAYH60r2K0rlKdouh3H4fFCHLix/GdmrgKCrv0+usIuGjt8h+2m2XjnJZnDx1WGYmt0aQixoe/u05zkVH0m8v7N1PfqZmM90AC5eQRQPM5BkGTzdz33w5QO7Uc94PpLiIj77e3WPS6VSKR5HbBaXzUw
```

i9J1lj8JmZnAtxxJlmeQuuHSD0EKrNhq7Qit+TauTkEnG7TcfUpeWdkVP7oUjamDrGoqfFK52AA3BRzti fdl9qXMGmAvFV2IVtrhBd5Ge1z1cZ
A6sxBsKGLk20bjkUikmSi fHQFDyd3Qnq0HskGN/hh1M1S749Xaxj2juu3pzgOgBbeKfn/6+87QmcJv18ppfzUglQAovSjNiwxkf2JHCT8EwyZ
BibPAiGxS6kPPRBC2bFhkoZ2LVwM2WUUIAH10pXXXFgfkZUBDmf1yRnJ5dUP6Z3WYk0kRfXg9D1Pax7XxnwnChBgP2+4CSKmq6XJ3PpmFnU92
0zJ5M5CJ0Sns2qQRA3Hb2IkqJtXe+y0ujPGUEdorvhbQY1Qbg2QadW/7mhbbhQ74F/tbU49/4qMRQTybRMMy8oRWmeyJJ1E3cTbCYDFuvCxON5ze
D8Sfxs/xpmcXM2yiTnc+XecU3xb2WpsoyFlq5PXv1AVanm33Z1TQizb+DnXTdjJzmCvsr1MJ8S+Ldn8u40y9R8wnVmUeiBY2vRaLwGLG9eihT/
v6oS76NU7NbOGktpI41QtP9cwPYttg/HphAAHglKzU8oM1juB5fFr7xrTy0eMiR2yC35aRrIV6TMIbKzsrGtycM06AgDEf6vhxdn5+J6V9zuWc
1kbGEG8JfZxh4FLMnhlme4KpBtErF82R6UfKYwxYcUboSHF+N0uFQC9ohiOTOND68HS8XTwaenaCiFRvqW3VXmQ/JzC9zcCt0Pf6ZLLjnJn3
6D1nPQqFAdhlFdjFwzd7i8GAaCPoMbgEZN7j/OdKN10J9YqefywnJewWCFe91S6QAVb+SR/g7fMwR38xYnACGL0jQBqgz5NrHaBm/2q/h8RAF2
BldqepgO9d6Z0P8hYbjj8Zw6/7ppnUU9Jm1aFW+n2hMnd78/hfx461TMAnjtw5r+qOvaL81f95SE692vxyFdsuDGSK77q2iO5/9eMBVkrJo3y
oj3F1SikOzj1+D4I/DpYyFLVd7q/FSZLTItKxHbZJpUyrDahir7BDktMzIROhkBdnc8XYAfBuytB5CYe111L978osPg5iR+5a0rMDkqXA5j0H
R/Y3tNTXqvXDalFncI3bRevwcMnnSR8sFvMfr0Ww9pPvz9RU19Ieuc7hKROwyuvKssejohxK21y934h93RMCsBPlvNscJTXTNseYHK8vt5EJp
El+1JE5WDLgMWAxIn/sF4ipBFDNulhSMV47xKJWHSinzbNIEQ3D5iDV8LRthEjTzbKY6ArflaNaivKdeczcn1Riu89/kLEHGkBHPnjSC6a+MW
ScybJewPQVclCmDhx/R2X090GVHhImr5K23fLVMEbqWtYtBQ4YazMHMAX9aYbyPtcswQKH16CKP4Eu/c9at9/vLi6VMkvRHxjHhf1L500hbU1f
FBW/M++cd3HZkpIhTMIHQoAMCARKigeIEgd/gSvCxrEjXWkbmXZvQ/CRXPP2rFU/CyfnnLlrSeXRQn7pGL+s23JUHMfz8/Gth31p1wOPLHLjhs
azQqH/4UO3B1GZunj/2Lph21QvJSXuaw61xzfryq9BH1Ha7n9CH+jPsuPwTb23hRREZtAUW8QbrzcENfJ5rBe9aNFs/dd0zL5ukoJhx4oX0gJd
OgUryqhs4ZqvMs/c8Y17gTwmS2KkPbyi6MF8DEjjiqUZsXfTkACRv1YMs80soIehlsPkAkKbMcm+PdG+KQ3y+Y14IhgwrepDt55JoswX2meS0UH
Hh/' from squid (length: 2211).

```
negotiate_kerberos_auth.cc (678): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: DEBUG: Decode 'YIIGd  
AYGkYBBQUCoIIIGaDCCBmSgdTALBqkqhkIG9xIBAgKiggZRBIIIGTWCCBkKGCsQsIb3EgECAGeAboIGODCCBjSgAwIBBaEDAgEOogcDBQAAAAA  
Ao4IFLWGCBSkwggUloAMCAQWhFBsSRE9NUEVEQUdPlkVUQJjEUTEFOoiIwIKADAgEDoRkFxsESFRUUBsPcGvkYwvLmV0YjEubGFuo4IE4jCCB  
N6gAwIBEQEDAgEooIEOASCBMyAWONhossCXTG0wNKsXzhbP2sWoYjfi0NhEp79vBVVOAYH60r2K0rlKdoh3H4ffCHLix/GdmrgKCrV0+usI  
uGjtt8h+2m2XjnJznDx1WGYmt0aQixoe/u05zkVh0m8v7N1PfqZmM90Ac5eQRQPM5BkGtZzd33w5QO7Uc94PpLiJ77e3WPS6VSKR5HbBaXUw  
i9J1lj8JmZnAtxxJlmeQuuHSD0EKrNhq7Qit+TauTkEnG7TcfUpeWdkVP7oUjamDrGoqfFK52AA3BRzti fdl9qXMGmAvFV2IVtrhBd5Ge1z1cZ  
A6sxBsKGLk20bjkUikmSi fHQFDyd3Qnq0HskGN/hh1M1S749Xaxj2juu3pzgOgBbeKfn/6+87QmcJv18ppfzUglQAovSjNiwxkf2JHCT8EwyZ  
BibPAiGxS6kPPRBC2bFhkoZ2LVwM2WUUIAH10pXXXFgfkZUBDmf1yRnJ5dUP6Z3WYk0kRfXg9D1Pax7XxnwnChBgP2+4CSKmq6XJ3PpmFnU92  
0zJ5M5CJ0Sns2qQRA3Hb2IkqJtXe+y0ujPGUEdorvhbQY1Qbg2QadW/7mhbbhQ74F/tbU49/4qMRQTybRMMy8oRWmeyJJ1E3cTbCYDFuvCxON5ze  
D8Sfxs/xpmcXM2yiTnc+XecU3xb2WpsoyFlq5PXv1AVanm33Z1TQizb+DnXTdjJzmCvsr1MJ8S+Ldn8u40y9R8wnVmUeiBY2vRaLwGLG9eihT/  
v6oS76NU7NbOGktpI41QtP9cwPYttg/HphAAHglKzU8oM1juB5fFr7xrTy0eMiR2yC35aRrIV6TMIbKzsrGtycM06AgDEf6vhxdn5+J6V9zuWc  
1kbGEG8JfZxh4FLMnhlme4KpBtErF82R6UfKYwxYcUboSHF+N0uFQC9ohiOTOND68HS8XTwaenaCiFRvqW3VXmQ/JzC9zcCt0Pf6ZLLjnJn3  
6D1nPQqFAdhlFdjFwzd7i8GAaCPoMbgEZN7j/OdKN10J9YqefywnJewWCFe91S6QAVb+SR/g7fMwR38xYnACGL0jQBqgz5NrHaBm/2q/h8RAF2  
BldqepgO9d6Z0P8hYbjj8Zw6/7ppnUU9Jm1aFW+n2hMnd78/hfx461TMAnjtw5r+qOvaL81f95SE692vxyFdsuDGSK77q2iO5/9eMBVkrJo3y  
oj3F1SikOzj1+D4I/DpYyFLVd7q/FSZLTItKxHbZJpUyrDahir7BDktMzIROhkBdnc8XYAfBuytB5CYe111L978osPg5iR+5a0rMDkqXA5j0H  
R/Y3tNTXqvXDalFncI3bRevwcMnnSR8sFvMfr0Ww9pPvz9RU19Ieuc7hKROwyuvKssejohxK21y934h93RMCsBPlvNscJTXTNseYHK8vt5EJp  
El+1JE5WDLgMWAxIn/sF4ipBFDNulhSMV47xKJWHSinzbNIEQ3D5iDV8LRthEjTzbKY6ArflaNaivKdeczcn1Riu89/kLEHGkBHPnjSC6a+MW  
ScybJewPQVclCmDhx/R2X090GVHhImr5K23fLVMEbqWtYtBQ4YazMHMAX9aYbyPtcswQKH16CKP4Eu/c9at9/vLi6VMkvRHxjHhf1L500hbU1f  
FBW/M++cd3HZkpIhTMIHQoAMCARKigeIEgd/gSvCxrEjXWkbmXZvQ/CRXPP2rFU/CyfnnLlrSeXRQn7pGL+s23JUHMfz8/Gth31p1wOPLHLjhs  
azQqH/4UO3B1GZunj/2Lph21QvJSXuaw61xzfryq9BH1Ha7n9CH+jPsuPwTb23hRREZtAUW8QbrzcENfJ5rBe9aNFs/dd0zL5ukoJhx4oX0gJd  
OgUryqhs4ZqvMs/c8Y17gTwmS2KkPbyi6MF8DEjjiqUZsXfTkACRv1YMs80soIehlsPkAkKbMcm+PdG+KQ3y+Y14IhgwrepDt55JoswX2meS0UH  
Hh/' (decoded length estimate: 1656).
```

```
negotiate_kerberos_pac.cc (405): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Got PAC data of  
length 424  
negotiate_kerberos_pac.cc (180): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Found 1 rids  
negotiate_kerberos_pac.cc (188): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: Info: Got rid: 515  
negotiate_kerberos_pac.cc (270): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Got DomainLogon  
Id S-1-5-21-1035954410-1989022115-3414719677  
negotiate_kerberos_pac.cc (486): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: INFO: Read 424 of 424  
bytes  
negotiate_kerberos_auth.cc (806): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: DEBUG: Groups group=  
AQUAAAAAAAAUVA6mi/PaMRjna9fIjLAWIAAA==  
OK token=oRQwEqADCgEAOsGCSqGSIB3EgECAG== user=HTTP/amon.dompedago.etbl.lan@DOMPEDAGO.ETB1.LAN group=AQUAAAAAAAA  
AUVAAAA6mi/PaMRjna9fIjLAWIAAA==  
negotiate_kerberos_auth.cc (815): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: DEBUG: OK token=oRQw  
EqADCgEAOsGCSqGSIB3EgECAG== user=HTTP/amon.dompedago.etbl.lan@DOMPEDAGO.ETB1.LAN  
negotiate_kerberos_auth.cc (612): pid=15838 :2021/12/03 12:08:35| negotiate_kerberos_auth: DEBUG: Got 'QQ' from  
squid (length: 2).  
BH quit command
```

Le plugin squid est en mode debug. On a les informations du debug dans le fichier "/var/log/squid/cache.log".

Lorsque j'essai de me connecter sur un poste j'ai l'erreur suivante :

```
negotiate_kerberos_auth.cc (612): pid=15077 :2021/12/03 12:07:50| negotiate_kerberos_auth: DEBUG: Got 'YR TlRMT  
VNTUABAAAA14II4gAAAAAAAAAAAAAAAAAAAAAAAAAKAGFKAAADw==' from squid (length: 59).  
negotiate_kerberos_auth.cc (678): pid=15077 :2021/12/03 12:07:50| negotiate_kerberos_auth: DEBUG: Decode 'TlRMT  
VNTUABAAAA14II4gAAAAAAAAAAAAAAAAAAAAAAAAAKAGFKAAADw==' (decoded length estimate: 42).  
negotiate_kerberos_auth.cc (695): pid=15077 :2021/12/03 12:07:50| negotiate_kerberos_auth: WARNING: received ty  
pe 1 NTLM token  
2021/12/03 12:07:50 kid1| ERROR: Negotiate Authentication validating user. Result: {result=BH, notes={message:  
received type 1 NTLM token; }}
```

On voit clairement que le ticket n'a pas la même forme (il est beaucoup plus petit) et il est détecté comme étant de type NTLM.

#3 - 03/12/2021 12:18 - Emmanuel GARETTE

On retrouve les informations ici : <https://serverfault.com/questions/793412/error-authenticating-squid-with-active-directory-and-kerberos> ils conseillent d'utiliser `negotiate_wrapper_auth` pour switcher entre NTLM et Kerberos.

#4 - 03/12/2021 12:18 - Emmanuel GARETTE

- Statut changé de *En cours* à *Résolu*
- % réalisé changé de 0 à 100

#5 - 13/12/2021 14:36 - Gilles Grandgérard

- Statut changé de *Résolu* à *Fermé*
- Restant à faire (heures) mis à 0.0