

Amon - T che #36216

Sc nario # 36200 (Termin  (Sprint)): Le filtrage WEB ne fonctionne pas (2.8.1)

 tude

14/10/2024 15:10 - Benjamin Bohard

Statut:	Ferm�	D�but:	01/10/2022
Priorit�:	Normal	Ech�ance:	
Assign� �:	Emmanuel GARETTE	% r�alis�:	100%
Version cible:	Livraison Cadoles - MEN 31/12/2024 (100)	Temps estim�:	0.00 heure
		Temps pass�:	0.00 heure
Description			
Demandes li�es:			
Li� � Distribution EOLE - T�che #33136: Service Squid s'arr�te r�guli�rement		Ferm�	13/09/2021

Historique

#1 - 14/10/2024 15:10 - Benjamin Bohard

- Statut chang  de Nouveau   En cours

#2 - 14/10/2024 15:12 - Benjamin Bohard

```
read(58, "CONNECT www.netflix.com:443 HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0\r\nProxy-...", 4096) = 205
write(58, "HTTP/1.1 407 Proxy Authentication Required\r\nServer: squid/4.10\r\nMime-Version: 1.0\r\nDate: Mon, 14 Oct 2024 12:39:08 GMT\r\nContent-...", 4058) = 4058
read(58, "CONNECT www.netflix.com:443 HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0\r\nProxy-...", 3890) = 277
write(14, "YR TlRMTVNTUAAABAAAAB4IIAAAAAAAAAAAAAAAAAAAAA=\n", 48) = 48
read(14, "TT TlRMTVNTUAAACAAAEgASADgAAAFgokC83TdUO8yGOYAAAAAAAAAGQAZABKAAAABgEAAAAAAAA9EAE8ATQBQAEUARABBAEcATwACABIArABPAEOAUABFAEQaQQBHA"..., 32767) = 236
write(58, "HTTP/1.1 407 Proxy Authentication Required\r\nServer: squid/4.10\r\nMime-Version: 1.0\r\nDate: Mon, 14 Oct 2024 12:39:08 GMT\r\nContent-...", 4376) = 4376
read(58, "CONNECT www.netflix.com:443 HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0\r\nProxy-...", 3818) = 585
write(14, "KK TlRMTVNTUAAADAAAAGAAAYAGAAAACQAJAAeAAAAAAAAABAAAAACgAKAEAAAAAWABYASgAAAAAAAAAAAAAAAAABYIIAGEAZABtAGkAbgBXAE8AUgBLAFMAVABBAFQASQBPA"..., 356) = 356
read(14, "AF admin\n", 32767) = 9
write(10, "REQMOD icap://127.0.0.1:1340/request ICAP/1.0\r\nHost: 127.0.0.1:1340\r\nDate: Mon, 14 Oct 2024 12:39:08 GMT\r\nProxy-Authorization: N"..., 741) = 741
read(10, "ICAP/1.0 200 OK\r\nIStag:1728898587\r\nEncapsulated: res-hdr=0, null-body=111\r\n\r\nHTTP/1.1 302 Re direct\r\nLocation: http://internal.te"..., 65535) = 188
write(58, "HTTP/1.1 302 Found\r\nLocation: http://internal.test.e2guardian.org\r\nServer: e2guardian\r\nDate: Mon, 14 Oct 2024 12:39:08 GMT\r\nX-Ca"..., 240) = 240
write(58, "0\r\n\r\n", 5) = 5
write(11, "2024/10/14 14:39:08 kidl| kick abandoning local=10.1.2.1:3128 remote=10.1.2.50:34086 FD 58 flags=1\n", 99) = 99
```

#3 - 14/10/2024 15:15 - Benjamin Bohard

Peut-être pas lié au problème mais il semble que l'URL définie pour tester si e2guardian est fonctionnel (internal.test.e2guardian.org) n'est pas résolue sur le serveur de test. Je ne sais pas quelle incidence cette redirection a sur la suite du protocole ICAP.

#4 - 15/10/2024 12:14 - Benjamin Bohard

Trace de e2guardian quand il est interrogé sur <https://www.wikipedia.org> avec c-icap-client (c-icap-client -v -p 1340 -s request -req <https://www.wikipedia.org>)

```
[pid 71795] recvfrom(11, "OPTIONS icap://localhost/request ICAP/1.0\r\nHost: localhost\r\nUser-Agent: C-ICAP-Client-Library/0.5.3\r\nEncapsulated: null-body=0\r\n"... , 1024, 0, NULL, NULL) = 130
[pid 71795] sendto(11, "ICAP/1.0 200 OK\r\nMethods: REQMOD\r\nService: e2guardian 5.3.4\r\nISTag: \"1728947234\r\n\r\nEncapsulated: null-body=0\r\nAllow: 204\r\n\r\n\"", 123, 0, NULL, 0) = 123
[pid 71795] recvfrom(11, "REQMOD icap://localhost/request ICAP/1.0\r\nHost: localhost\r\nUser-Agent: C-ICAP-Client-Library/0.5.3\r\nAllow: 204\r\nEncapsulated: re"... , 1024, 0, NULL, NULL) = 260
[pid 71795] sendto(11, "ICAP/1.0 200 OK\r\nISTag:1728947234\r\nX-ICAP-E2G:-,G,0,0,0,\r\nEncapsulated: req-hdr=0, null-body=107\r\n\r\nGET https://www.wikipedia.or"... , 207, 0, NULL, 0) = 207
[pid 71795] recvfrom(11, "", 1024, 0, NULL, NULL) = 0
[pid 71795] recvfrom(11, "", 2, 0, NULL, NULL) = 0
```

Trace de e2guardian quand il est interrogé sur <https://netflix.com> avec c-icap-client (c-icap-client -v -p 1340 -s request -req <https://netflix.com>)

```
[pid 71793] recvfrom(11, "OPTIONS icap://localhost/request ICAP/1.0\r\nHost: localhost\r\nUser-Agent: C-ICAP-Client-Library/0.5.3\r\nEncapsulated: null-body=0\r\n"... , 1024, 0, NULL, NULL) = 130
[pid 71793] sendto(11, "ICAP/1.0 200 OK\r\nMethods: REQMOD\r\nService: e2guardian 5.3.4\r\nISTag: \"1728947234\r\n\r\nEncapsulated: null-body=0\r\nAllow: 204\r\n\r\n\"", 123, 0, NULL, 0) = 123
[pid 71793] recvfrom(11, "REQMOD icap://localhost/request ICAP/1.0\r\nHost: localhost\r\nUser-Agent: C-ICAP-Client-Library/0.5.3\r\nAllow: 204\r\nEncapsulated: re"... , 1024, 0, NULL, NULL) = 254
[pid 71793] sendto(11, "ICAP/1.0 200 OK\r\nISTag:1728947234\r\nEncapsulated: res-hdr=0, res-body=42\r\n\r\nHTTP/1.1 200 \r\nContent-type: text/html\r\n\r\n", 117, 0, NULL, 0) = 117
[pid 71793] sendto(11, "7e2\r\n", 5, 0, NULL, 0) = 5
[pid 71793] sendto(11, "<HTML>\n<HEAD>\n <meta charset=\"UTF-8\">\n <TITLE>EOLE Guardian - Acc&egrave;s Interdit</TITLE>\n</HEAD>\n<style type=\"text/css\">\n "... , 2018, 0, NULL, 0) = 2018
[pid 71793] sendto(11, "\r\n", 2, 0, NULL, 0) = 2
[pid 71793] sendto(11, "0\r\n", 3, 0, NULL, 0) = 3
[pid 71793] sendto(11, "\r\n", 2, 0, NULL, 0) = 2
[pid 71793] recvfrom(11, "", 1024, 0, NULL, NULL) = 0
[pid 70131] sendto(7, "<14>Oct 15 12:10:52 e2guardian0[70120]: \"2024.10.15 12:10:52\", \"-\", \"-\", \"https://netflix.com\", \"*Acc\303\250s interdit* Site interdit : n"... , 213, MSG_NOSIGNAL, NULL, 0) = 213
[pid 71793] recvfrom(11, "", 2, 0, NULL, NULL) = 0
```

Trace de e2guardian quand il est interrogé sur <https://www.wikipedia.org> depuis le navigateur du client

```
[pid 71817] recvfrom(6, "REQMOD icap://127.0.0.1:1340/request ICAP/1.0\r\nHost: 127.0.0.1:1340\r\nDate: Tue, 15 Oct 2024 10:11:25 GMT\r\nProxy-Authorization: N"... , 1024, 0, NULL, NULL) = 745
[pid 71817] sendto(6, "ICAP/1.0 200 OK\r\nISTag:1728947234\r\nX-ICAP-E2G:admin,G,0,0,0,\r\nEncapsulated: req-hdr=0, null-body=151\r\n\r\nCONNECT www.wikipedia.or"... , 255, 0, NULL, 0) = 255
[pid 70131] sendto(7, "<14>Oct 15 12:11:25 e2guardian0[70120]: \"2024.10.15 12:11:25\", \"admin\", \"10.1.2.50\", \"https://www.wikipedia.org:443\", \"-\", \"CONNECT\", \""... , 201, MSG_NOSIGNAL, NULL, 0) = 201
```

Trace de e2guardian quand il est interrogé sur <https://netflix.com> depuis le navigateur du client

```
[pid 71817] recvfrom(6, "REQMOD icap://127.0.0.1:1340/request ICAP/1.0\r\nHost: 127.0.0.1:1340\r\nDate: Tue, 15 Oct 2024 10:12:54 GMT\r\nProxy-Authorization: N"... , 1024, 0, NULL, NULL) = 741
[pid 71817] sendto(6, "ICAP/1.0 200 OK\r\nISTag:1728947234\r\nEncapsulated: res-hdr=0, null-body=111\r\n\r\nHTTP/1.1 302 Redirect\r\nLocation: http://internal.te"... , 188, 0, NULL, 0) = 188
[pid 70131] sendto(7, "<14>Oct 15 12:12:54 e2guardian0[70120]: \"2024.10.15 12:12:54\", \"admin\", \"10.1.2.50\", \"https://www.netflix.com:443\", \"*Acc\303\250s interdi"... , 245, MSG_NOSIGNAL, NULL, 0) = 245
[pid 71817] recvfrom(6, <unfinished ...>
[pid 71815] recvfrom(9, <unfinished ...>
```

```
[pid 71817] <... recvfrom resumed>"OPTIONS icap://127.0.0.1:1340/request ICAP/1.0\r\nHost: 127.0.0.1:1340\r\nAllow: 206\r\n\r\n", 1024, 0, NULL, NULL) = 84
[pid 71815] <... recvfrom resumed>"OPTIONS icap://127.0.0.1:1340/response ICAP/1.0\r\nHost: 127.0.0.1:1340\r\nAllow: 206\r\n\r\n", 1024, 0, NULL, NULL) = 85
[pid 71817] sendto(6, "ICAP/1.0 200 OK\r\nMethods: REQMOD\r\nService: e2guardian 5.3.4\r\nISTag: \"1728947234\r\n\r\nEncapsulated: null-body=0\r\nAllow: 204\r\n\r\n", 123, 0, NULL, 0 <unfinished ...>
[pid 71815] sendto(9, "ICAP/1.0 200 OK\r\nMethods: RESPMOD\r\nService: e2guardian 5.3.4\r\nISTag:1728947234\r\n\r\nEncapsulated: null-body=0\r\nAllow: 204\r\n\r\n", 121, 0, NULL, 0 <unfinished ...>
[pid 71817] <... sendto resumed>          = 123
[pid 71815] <... sendto resumed>          = 121
```

#5 - 15/10/2024 13:52 - Benjamin Bohard

Interrogé par le client c-icap-client, e2guardian renvoie bien la réponse attendue :

```
<HTML>
<HEAD>
  <meta charset="UTF-8">
  <TITLE>EOLE Guardian - Accès Interdit</TITLE>
</HEAD>
<style type="text/css">
  table{
    border: 1px solid black;
    -webkit-border-top-right-radius: 20px;
    -webkit-border-bottom-left-radius: 20px;
    -moz-border-radius-topright: 20px;
    -moz-border-radius-bottomleft: 20px;
    border-top-right-radius: 20px;
    border-bottom-left-radius: 20px;
    border-color: #98bf21;
  }
</style>
<BODY BGCOLOR="FFFFF2">
<CENTER>
  <H2>ACCÈS INTERDIT</H2>
  <br>
  <table width="650">
    <tr><td ALIGN=CENTER>
      <br>
      Utilisateur : <strong>-</strong><br>
      IP Machine : <strong></strong><br>
      <br>
      Adresse refusée :
      <br>
      <strong>https://netflix.com</strong>
      <br>
      Raison :
      <br>
      <strong><font color="#ff0000">Site interdit : netflix.com</font></strong>
      <br>
      <br>
    </td></tr>
  </table>
  <P><br>
  <table width="650" bgcolor="#C3C3C3">
    <tr>
      <td ALIGN=CENTER><H4>Toutes vos demandes sont enregistrées. Des filtres sont appliqués.</H4>
    </td>
  </tr>
  </table>
  <br>
  Vous avez fait une tentative d'accès à un site Web qui ne présente aucun intérêt pour des besoins d'information pédagogique ou technique correspondant à votre utilisation.
  </tr>
</table>
```

```
<P>Pour toute réclamation, adressez un message à :  
<A HREF='mailto:cachemaster@ac-test.fr?subject=[plainte%20e2guardian]%20établissement%20:%20etb1%20rne=00000001&body=Message%20envoyé;%20depuis%20la%20page%20de%20sites%20interdits%20%0AMail%20envoyé%20par%20:%20-%20%0AIP%20de%20la%20machine%20:%20%0ARaison%20invoqué;%20:%20Site interdit : netflix.com%0AUrl%20visité;%20:%20"https://netflix.com"%0A'>  
<font color="#0000ee">cachemaster@ac-test.fr</font></A>  
<P>&nbsp;</P>  
<P><font size=-3>Powered by <a href="http://e2guardian.org" target="_blank"><font color="#0000ee">E2guardian  
</font></A></font>  
</center>  
</BODY>  
</HTML>
```

#6 - 05/11/2024 14:11 - Emmanuel GARETTE

- Lié à Tâche #33136: Service Squid s'arrête régulièrement ajouté

#7 - 05/11/2024 14:23 - Emmanuel GARETTE

- Statut changé de En cours à À valider

- Assigné à changé de Benjamin Bohard à Emmanuel GARETTE

- % réalisé changé de 0 à 100

Il est difficile de comprendre ce qu'il se passe exactement et il est très difficile de reproduire le problème.

Voici néanmoins les informations que nous pouvons donner :

1/ la page d'erreur de firefox est normal. Si vous vous connectez à netflix, seul netflix peut afficher du contenu (il faut que cela soit chiffré avec la clé privée de netflix). Ni e2guardian, ni squid ne peut le faire à la place de netflix.

Si vous voulez réellement cette fonctionnalité il va falloir activer cette fonctionnalité :

http://eole.ac-dijon.fr/documentations/2.8/completes/HTML/ModuleAmon/co/024-configuration_squid_normal_1.html

L'erreur "kick abandoning xxxx" ne me semble pas problématique.

2/ le vrai problème est "suspending ICAP service for too many failures". Cela veut dire que squid a reçu des erreurs du service e2guardian. Mais quelles erreurs ? Je n'ai jamais réussi à avoir de log qui explique cette erreur.

Dans la demande que je viens de lier l'utilisateur dit que de mettre "icap_service_failure_limit" à "-1" permet pour lui de résoudre le souci. Je n'ai pas la capacité de tester cela.

3/ si vous avez accès temporairement à netflix c'est que lorsque le serveur ICAP est déconnecté (pendant 10 seconds) il n'y a alors plus de filtrage. Vous pouvez remplacer dans la conf de squid "bypass=on" par "bypass=0" mais attention, s'il y a des soucis avec e2guardian, tous les utilisateurs seront bloqués.

#8 - 17/12/2024 09:30 - Emmanuel GARETTE

- Statut changé de À valider à En cours

#9 - 17/12/2024 10:06 - Emmanuel GARETTE

- Statut changé de En cours à À valider

Chez un client il y a un Seth derrière un Amon.

On a fréquemment des erreurs dans le test distant du Seth.

Après analyse on s'aperçoit que le wget fait les erreurs suivantes :

```
requête Proxy transmise, en attente de la réponse... 500 Internal Server Error
2024-12-16 10:19:21 erreur 500 : Internal Server Error.
```

Dans les logs de l'Amon on retrouve les erreurs.

Sur ce serveur Amon j'ai appliqué la modification pendant 10 jours (du 5 au 14 décembre) et je n'ai plus eu l'erreur sur toute la période. Le client ne s'est pas plaint de dysfonctionnement particulier.

Le 14 le reconfigure s'est fait et a remis les valeurs par défaut. Il y a eu, durant cette période, 7 remontés d'erreur.

Le patch apporte pour moi une stabilité intéressante.

#10 - 24/02/2025 16:25 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#11 - 25/04/2025 17:23 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0