

Distribution EOLE - T che #36738

Sc nario # 37103 (Termin  (Sprint)): EOLE 2.10 : v rifier la d tection des virus dans les mails

Correction SCRIBE-T03-011 - D tection de virus dans un mail (2.10.0-RC2)

10/04/2025 14:20 - Daniel Dehennin

Statut:	Ferm�	D�but:	14/03/2025
Priorit�:	Normal	Ech�ance:	
Assign� �:	Benjamin Bohard	% r�alis�:	100%
Version cible:	Livraison Cadoles - MEN 31/10/2025 (40)	Temps estim�:	0.00 heure
		Temps pass�:	0.00 heure
Description			
Pas N�9			
L'erreur SMTP n'est pas du tout la bonne, au lieu d'avoir			
Erreur SMTP : [550] This message contains malware (Eicar-Signature)			
J'obtiens :			
Erreur SMTP : [451] Temporary local problem - please try later			
Voici les logs de Scribe :			
<pre>avril 10 14:15:51 scribe eolessa[17547]: 2025-04-10T12:15:51+0000 [HTTPChannel (TLSProtocolWrapper),28,10.88.0.1] TGC-etblac-testfr-b4f56ed591d73e4c916b091f3d46a7c1cf494739205889679b4b010d -- tick et proxy d�livr� pour imap://10.1.3.5 avril 10 14:15:51 scribe eolessa[17547]: 2025-04-10T12:15:51+0000 [HTTPChannel (TLSProtocolWrapper),29,10.88.0.1] TGC-etblac-testfr-b4f56ed591d73e4c916b091f3d46a7c1cf494739205889679b4b010d -- tick et proxy d�livr� pour smtp://10.1.3.5 avril 10 14:15:51 scribe saslauthd[17641]: Authentication failed for prenom.elevel12@dompedago.etb1.lan/dompedago.etb1.lan: Bind to ldap server failed (invalid user/password or insufficient access) (-7) avril 10 14:15:51 scribe saslauthd[17641]: : auth failure: [user=prenom.elevel12@dompedago.etb1.lan] [service=ldap] [realm=dompedago.etb1.lan] [mech=ldap] [reason=Unknown] avril 10 14:15:51 scribe exim4[24381]: pam_ldap: error trying to bind as user "uid=prenom.elevel12,ou=local,ou=eleves,ou=utilisateurs,ou=00000001,ou=ac-test,ou=education,o=gouv,c=fr" (Invalid credentials) avril 10 14:15:51 scribe exim[24381]: 2025-04-10 14:15:51 1u2qox-000000006LF-3V8E malware acl condition: clamd /var/run/clamav/clamdctl : unable to connect to UNIX socket (/var/run/clamav/clamdctl): No such file or directory avril 10 14:15:51 scribe exim4[24381]: 2025-04-10 14:15:51 1u2qox-000000006LF-3V8E malware acl condition: clamd /var/run/clamav/clamdctl : unable to connect to UNIX socket (/var/run/clamav/clamdctl): No such file or directory avril 10 14:15:51 scribe exim[24381]: 2025-04-10 14:15:51 1u2qox-000000006LF-3V8E malware acl condition: clamd /var/run/clamav/clamdctl : unable to connect to UNIX socket (/var/run/clamav/clamdctl): No such file or directory avril 10 14:15:51 scribe exim[24381]: 2025-04-10 14:15:51 1u2qox-000000006LF-3V8E H=scribe.dompedago.etb1.lan (etb1.ac-test.fr) [10.1.3.5] X=TLS1.3:ECDHE_X25519__RSA_PSS_RSAE_SHA256__AES_256_GCM:256 CV=no F=<prenom.elevel12@i-etb1.ac-test.fr> A=login:prenom.elevel12 temporarily rejected after DATA avril 10 14:15:51 scribe exim[24381]: [1\19] 2025-04-10 14:15:51 1u2qox-000000006LF-3V8E H=scribe.dompedago.etb1.lan (etb1.ac-test.fr) [10.1.3.5] X=TLS1.3:ECDHE_X25519__RSA_PSS_RSAE_SHA256__AES_256_GCM:256 CV=no F=<prenom.elevel12@i-etb1.ac-test.fr> A=login:prenom.elevel12 temporarily rejected after DATA</pre>			

```

avril 10 14:15:51 scribe exim[24381]: [2\19] Envelope-from: <prenom.eleve112@i-etbl.ac-test.fr>
avril 10 14:15:51 scribe exim[24381]: [3\19] Envelope-to: <prenom.eleve107@i-etbl.ac-test.fr>
avril 10 14:15:51 scribe exim[24381]: [4\19] P Received: from scribe.dompedago.etbl.lan ([10.1.3.5]
] helo=etbl.ac-test.fr)
avril 10 14:15:51 scribe exim[24381]: [5\19] by scribe.dompedago.etbl.lan with esmtpsa (T
LS1.3) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
avril 10 14:15:51 scribe exim[24381]: [6\19] (Exim 4.97)
avril 10 14:15:51 scribe exim[24381]: [7\19] (envelope-from <prenom.eleve112@i-etbl.ac-tes
t.fr>)
avril 10 14:15:51 scribe exim[24381]: [8\19] id 1u2qox-000000006LF-3V8E
avril 10 14:15:51 scribe exim[24381]: [9\19] for prenom.eleve107@i-etbl.ac-test.fr;
avril 10 14:15:51 scribe exim[24381]: [10\19] Thu, 10 Apr 2025 14:15:51 +0200
avril 10 14:15:51 scribe exim[24381]: [11\19] MIME-Version: 1.0
avril 10 14:15:51 scribe exim[24381]: [12\19] Date: Thu, 10 Apr 2025 14:15:51 +0200
avril 10 14:15:51 scribe exim[24381]: [13\19] F From: "prenom.eleve112" <prenom.eleve112@i-etbl.ac
-test.fr>
avril 10 14:15:51 scribe exim[24381]: [14\19] T To: prenom eleve107 eleve <prenom.eleve107@i-etbl.
ac-test.fr>
avril 10 14:15:51 scribe exim[24381]: [15\19] Subject: Objet
avril 10 14:15:51 scribe exim[24381]: [16\19] I Message-ID: <1611be2b76a3eeb65a7bf272a1217970@i-et
bl.ac-test.fr>
avril 10 14:15:51 scribe exim[24381]: [17\19] X-Sender: prenom.eleve112@i-etbl.ac-test.fr
avril 10 14:15:51 scribe exim[24381]: [18\19] Content-Type: multipart/mixed;
avril 10 14:15:51 scribe exim[24381]: [19\19] boundary="=_8d96f17fe91c9b9bc9c48d37389d5b1a"

```

Exécution Squash-TM

- <https://dev-eole.ac-dijon.fr/squash/executions/15619>

Historique

#1 - 25/09/2025 17:09 - Joël Cuissinat

- Tâche parente changé de #36477 à #37103

#2 - 18/11/2025 16:30 - Benjamin Bohard

Le problème n'a pas encore été reproduit en suivant à nouveau les pas du test.

L'envoi avec le malware en pièce jointe déclenche bien l'erreur 550 attendue et les logs ne révèlent pas d'erreurs associées à clamav : le fichier /var/run/clamav/clamd.ctl est bien présent et l'analyse est bien effectuée.

```

nov. 18 16:26:59 scribe exim[22369]: [1\19] 2025-11-18 16:26:59 lvLNbf-000000005on-0Koi H=scribe.dompedago.etb
1.lan (etbl.ac-test.fr) [10.1.3.5] X=TLS1.3:ECDHE_X25519__RSA_PSS_RSAE_SHA256__AES_256_GCM:256 CV=no F=<prenom
.eleve112@i-etbl.ac-test.fr> A=login:prenom.eleve112 rejected after DATA: This message contains malware (Win.T
est.EICAR_HDB-1)
nov. 18 16:26:59 scribe exim[22369]: [2\19] Envelope-from: <prenom.eleve112@i-etbl.ac-test.fr>
nov. 18 16:26:59 scribe clamd[16911]: Tue Nov 18 16:26:59 2025 -> /var/spool/exim4/scan/lvLNbf-000000005on-0Ko
i/lvLNbf-000000005on-0Koi.eml: Win.Test.EICAR_HDB-1(c6ca6d130930dcb1fa852551185c7456:1377) FOUND
nov. 18 16:26:59 scribe exim[22369]: [3\19] Envelope-to: <prenom.eleve107@i-etbl.ac-test.fr>
nov. 18 16:26:59 scribe exim[22369]: [4\19] P Received: from scribe.dompedago.etbl.lan ([10.1.3.5] helo=etbl.a
c-test.fr)
nov. 18 16:26:59 scribe exim[22369]: [5\19] by scribe.dompedago.etbl.lan with esmtpsa (TLS1.3) tls TL
S_ECDHE_RSA_WITH_AES_256_GCM_SHA384
nov. 18 16:26:59 scribe exim[22369]: [6\19] (Exim 4.97)
nov. 18 16:26:59 scribe exim[22369]: [7\19] (envelope-from <prenom.eleve112@i-etbl.ac-test.fr>)
nov. 18 16:26:59 scribe exim[22369]: [8\19] id lvLNbf-000000005on-0Koi
nov. 18 16:26:59 scribe exim[22369]: [9\19] for prenom.eleve107@i-etbl.ac-test.fr;
nov. 18 16:26:59 scribe exim[22369]: [10\19] Tue, 18 Nov 2025 16:26:59 +0100
nov. 18 16:26:59 scribe exim[22369]: [11\19] MIME-Version: 1.0
nov. 18 16:26:59 scribe exim[22369]: [12\19] Date: Tue, 18 Nov 2025 16:26:58 +0100
nov. 18 16:26:59 scribe exim[22369]: [13\19] F From: "prenom.eleve112" <prenom.eleve112@i-etbl.ac-test.fr>
nov. 18 16:26:59 scribe exim[22369]: [14\19] T To: prenom eleve107 eleve <prenom.eleve107@i-etbl.ac-test.fr>
nov. 18 16:26:59 scribe exim[22369]: [15\19] Subject: test
nov. 18 16:26:59 scribe exim[22369]: [16\19] I Message-ID: <2b00e714e1feae8c1144d4efab27f44f@i-etbl.ac-test.fr
>
nov. 18 16:26:59 scribe exim[22369]: [17\19] X-Sender: prenom.eleve112@i-etbl.ac-test.fr
nov. 18 16:26:59 scribe exim[22369]: [18\19] Content-Type: multipart/mixed;
nov. 18 16:26:59 scribe exim[22369]: [19\19] boundary="=_bf34ffe3b031894252b7db9035b6707e"

```

```
nov. 18 16:26:59 scribe clamd[16911]: /var/spool/exim4/scan/1vLNbf-000000005on-0Koi/1vLNbf-000000005on-0Koi.eml: Win.Test.EICAR_HDB-1 (c6ca6d130930dcb1fa852551185c7456:1377) FOUND
```

#3 - 19/11/2025 09:02 - Benjamin Bohard

- Assigné à mis à Benjamin Bohard

#4 - 19/11/2025 09:02 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#5 - 19/11/2025 09:20 - Benjamin Bohard

Les causes de la précédente erreur ne sont pas identifiées (pourquoi le socket n'est pas présent ?).
L'erreur elle-même n'est plus observée.

#6 - 19/11/2025 09:50 - Benjamin Bohard

- Statut changé de En cours à À valider

#7 - 08/12/2025 16:38 - Laurent Gourvenec

- Statut changé de À valider à Résolu

- % réalisé changé de 0 à 100

#8 - 09/12/2025 12:09 - Joël Cuissinat

Je viens de reproduire le problème, le soucis est clamav et pas roundcube...

```
déc. 09 10:21:37 scribe systemd[1]: clamav-daemon.service - Clam AntiVirus userspace daemon was skipped because of an unmet condition check (ConditionPathExistsGlob=/var/lib/clamav/daily.{c[vl]d,inc}).
```

Visiblement à la 1ère activation, il démarre trop tôt (avant que freshclam ait terminé), j'ai ajouté un pas de test pour vérifier/compenser ce problème.

#9 - 09/12/2025 12:09 - Joël Cuissinat

- Statut changé de Résolu à Fermé