# Distribution EOLE - Tâche #36951

Scénario # 36404 (Terminé (Sprint)): Test et Doc Freeradius

## Toujours des erreurs liées aux certificats en mode tls

01/07/2025 17:32 - Joël Cuissinat

| | | | |
|---|---|---|---|
| **Statut:** | Fermé | **Début:** | 01/07/2025 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | Benjamin Bohard | **% réalisé:** | 100% |
| **Version cible:** | Livraison Cadoles - MEN 31/08/2025 (20) | **Temps estimé:** | 0.00 heure |
| | | **Temps passé:** | 0.00 heure |

**Description**

J'ai ré-exécuté la série de tests et j'obtiens de nouvelles erreurs dans SD-EOLE-RADIUS-T20-001 - Configuration d'un profil avec autorisation par certificat

1. Tout d'abord les deux fichiers étaient absents. En remontant dans l'historique du reconfigure, j'ai trouvé :

```
/usr/share/eole/posttemplate/00-freeradius: ligne 26: make : commande introuvable
```

Bizarre qu'on ne l'ait pas vu avant (en fait si mais on n'a pas creusé), le paquet make était peut-être tiré par une autre dépendance ?

=> ajouter la dépendance si on ne peut pas s'en passer

2. Après un apt install make c'est mieux mais les deux certificats sont signalés différents...

```
root@amonecole:~# diff /var/lib/lxc/internet/rootfs/etc/freeradius/3.0/ssl/certs/server.pem /usr/s
hare/eole/freeradius-certs.d/tls/certs/server.crt
1,4c1,62
< Bag Attributes
<     localKeyID: 3F D9 35 93 D9 07 6D 84 B6 8F 88 A7 06 F1 93 F6 5E AC 00 E3
< subject=C = FR, ST = Radius, O = Example Inc., CN = Example Server Certificate, emailAddress = a
dmin@example.org
< issuer=C = FR, ST = Radius, L = Somewhere, O = Example Inc., emailAddress = admin@example.org, C
N = Example Certificate Authority
---
> Certificate:
>     Data:
>         Version: 3 (0x2)
>         Serial Number: 1 (0x1)
>         Signature Algorithm: sha256WithRSAEncryption
>         Issuer: C=FR, ST=Radius, L=Somewhere, O=Example Inc./emailAddress=admin@example.org, CN=
Example Certificate Authority
>         Validity
>             Not Before: Jul  1 15:03:40 2025 GMT
>             Not After : Aug 30 15:03:40 2025 GMT
>         Subject: C=FR, ST=Radius, O=Example Inc., CN=Example Server Certificate/emailAddress=adm
in@example.org
>         Subject Public Key Info:
>             Public Key Algorithm: rsaEncryption
>                 Public-Key: (2048 bit)
>                 Modulus:
>                     00:bd:8f:3a:3f:f3:ca:f7:41:d4:27:ef:19:5b:c6:
>                     e1:a9:9d:68:41:7e:70:ec:06:92:ea:35:1d:a1:6a:
>                     65:b1:f6:60:bb:d3:d1:f6:f5:9b:7b:44:fe:1f:92:
>                     02:4a:b6:68:57:94:06:26:96:3c:8c:e5:fc:b0:b4:
>                     67:36:ce:a8:d9:fc:ee:a5:3d:15:7c:fd:5e:b8:06:
>                     da:1f:51:36:df:3f:09:2e:73:0a:74:7f:ad:0a:29:
```

```
>                     51:5e:09:c8:13:a1:25:a8:56:ae:cc:14:ae:0d:c1:
>                     f9:b7:e9:8c:d0:d8:3e:cb:7c:f8:78:7e:0e:d8:4e:
>                     72:d7:71:e5:8c:29:73:21:7c:42:33:86:f9:a7:80:
>                     48:76:fc:d3:f6:85:4d:e9:fa:82:a4:f6:f6:1d:64:
>                     25:0a:66:98:d2:4a:33:52:49:6e:cf:6f:0a:89:54:
>                     25:10:51:48:d3:81:da:34:7c:f7:64:c1:52:b0:97:
>                     50:a6:f5:ef:b3:36:3f:74:58:cb:c6:a2:a4:be:76:
>                     09:28:3d:68:f0:a7:71:48:a2:aa:00:3c:4b:fe:49:
>                     45:23:d9:ce:0e:79:16:db:f6:ae:e6:43:32:ea:0d:
>                     22:f2:94:2d:fb:4f:a6:f4:a7:fd:43:d3:26:7e:12:
>                     6f:4a:2f:87:f2:26:42:c7:09:05:d3:d6:9a:75:63:
>                     55:3f
>                 Exponent: 65537 (0x10001)
>         X509v3 extensions:
>             X509v3 Extended Key Usage:
>                 TLS Web Server Authentication
>             X509v3 CRL Distribution Points:
>                 Full Name:
>                   URI:http://www.example.com/example_ca.crl
>             X509v3 Certificate Policies:
>                 Policy: 1.3.6.1.4.1.40808.1.3.2
>             X509v3 Subject Key Identifier:
>                 1A:20:78:88:64:E9:A1:D5:B6:7E:F6:91:74:E4:6A:55:A3:B2:E3:46
>             X509v3 Authority Key Identifier:
>                 8B:A9:CD:59:22:C7:9D:B3:47:53:76:A3:85:1D:D8:3D:67:AC:8E:5F
>     Signature Algorithm: sha256WithRSAEncryption
>     Signature Value:
>         49:aa:bc:92:3c:ae:ee:98:b5:7c:dc:86:55:90:50:ac:4c:a4:
>         ef:2d:5b:a2:c2:b5:0a:b9:37:ee:44:31:07:4d:54:08:86:08:
>         18:cd:e7:a9:fd:3a:9c:21:22:5b:71:d2:48:3c:00:d1:9a:84:
>         e0:9f:c0:4b:31:74:ea:cb:80:ca:d8:bc:bd:7f:9e:8c:3c:bb:
>         8e:60:4d:4f:f0:6c:33:4f:3a:d5:8e:f4:5c:87:84:36:07:bb:
>         fc:12:6b:75:fd:e9:01:79:55:6c:c6:48:75:4a:42:71:e4:78:
>         06:69:fa:4f:cf:13:ca:1b:61:ed:17:c9:e3:8b:3c:c1:ce:91:
>         79:b0:fa:72:71:bd:b4:69:16:e3:e0:bd:ef:5d:7d:31:32:61:
>         ab:f4:f8:73:27:06:2a:09:4a:7c:ab:d7:dc:0a:0f:bc:3e:2e:
>         ee:42:f8:95:a6:76:d6:42:51:49:26:51:82:46:54:cc:91:57:
>         85:76:9b:11:b8:b7:9d:87:e4:a0:df:0a:86:4d:77:d1:7d:35:
>         74:f5:61:2a:09:9a:1e:d7:24:68:52:5b:76:01:e1:bb:19:a3:
>         84:2f:4f:f9:92:58:15:5e:4d:19:14:81:2c:62:8d:33:b0:99:
>         6f:17:9e:1b:6f:23:be:76:ce:3f:90:21:28:7a:f6:9f:d9:b0:
>         3c:71:d4:d0
30,62d87
< Bag Attributes
<     localKeyID: 3F D9 35 93 D9 07 6D 84 B6 8F 88 A7 06 F1 93 F6 5E AC 00 E3
< Key Attributes: <No Attributes>
< -----BEGIN ENCRYPTED PRIVATE KEY-----
< MIIFLTBXBgkqhkiG9w0BBQ0wSjApBgkqhkiG9w0BBQwwHAQIzeAJdyvUVxICAggA
< MAwGCCqGSIb3DQIJBQAwHQYJYIZIAWUDBAEqBBAAqvu99fytQdkI6TtBYyI+BIIE
< 0HbBTLZx4dZLjA5OCGehIKjyVdqXMVvpEMB9toK3Rl92fqFqtbSg6NYptWpgy0Xf
< LJGTFOJVJ/Nb//QafaN9HZw+4a4lI0Np7Lfk+OX1+nmhu4Mo6DdqyZd1wn12xkk5
< 7rzgKLiMWqtexK65+QIMU8TYRQcCaOb6q2mOFNlinu3W2jH+xMG/GyLiRheGpJpS
< +hPRjgb5Bae4dBUUUcX0+8HlK3RpCl3kuzptmJqFYoxA8HMLCM9kRfhu1EjsPjGl
< h8qsOnD5sogOrsbkV+Sw/40DkZOCP6oIOHFXEoY7vn9yVpR6ga7bdFyYKGWI+BxW
< AwHOIHlq2L7LQsR8bvLUNKafYv1wsi/1eNNUnjjL5HiafWP18pBx90JrHlYYzU0b
< rhSeuR/1nvYWs5TrNL+DNZFF7xPo4nh6/FS5++nJBZ134yRwgLcTgR4VligFVLSE
< D1iLpIT7q5/G2hXBgXEyfNDFTpWbq0vRNTf19kp4WwBPIApKrGiuYenk+iZc2mAo
< rIo79sK/MJtktcVuY3Drug/EVzijaS3hv0OXUgxu4fb3XCcZ+2DdzUfzDbGVGUrp
< bnijzUMIM2vpG7lUKd+hwximSqYGBJM5rF3ntDoBhaPXgismETDVkTiKXslVplNh
< 3DnYkInPz1iGgH3SxShEEMt+qD6LZr1pW07wBrzksb3yJj+XBKGfNOnJ/KV7zKfS
< UeNp1bGjRyw9gGU1u+H2WDThHZjhVl4flvgaLMHVohDlUXbzu5TNc1BOjxQkn9i1
< 0qO29hxIiFLf3wlP2pNH9+DvypBnnmrZxeQzip6Ij4ZVLbEXThvHQKg5Xr/87ywX
< KPCkK0VDuv5Ztk+0K1S/qoiybr5o+Iea2QD8DrBts0Tva58vq9vIyXHoiYPtqOR8
< MADxvW57eGKaHQBwbWillyc/p1fcD1h1brDBpkxlc3r6phP43rnEm5pyuN9qgGuv
< ugIJvhU2oEhZChoSDi+RRErynnhwQiPnyIyq1CsjtzA9dhzRowWnsnXX86193ojl
< iQjUuffD7Tc/Sr5FwB2ykVIDdPf4xfU5uqa+M4G+UQPUHwczp/14RASs8YP8U180
< +LzGekOU19bUh0eA/GcU08QXBE15HAgDPOellQ1gahyIDxbaonw/dUbJhUpbT90U
```

```
< sm1RNB+xZErDxdngTyFnoDq/RRvdc13dygpjt9hwzaGmFwoagSjfFm5csZwHBY1Y
< Dpdhxi0le7pC+41xT1ZnLB6HrOnCstiECjIA+wD0/BySflXZjTmlnbIei7U8jzIq
< 2Yq3eXXTWKuApFGy3PGq8+V61dkuMKoIcHG6F70D1ZYw+5TGx2BBGqTpnAi3Oem6
< CxBs8eRtWiRMLkXlyemVdp7NNE8WpyxfFma4SSpRyEEqiVSTTZ6zE8MyYgmfz+uO
< /M1kBSh5nhPsaEE+VyCaqjC1XVQRh1wUiCHF+i87hyX0eB/uWc1B2Ipkqz3VRWKp
< A+AaD9cqRMuTOMkJdDMKiXaBR/4EEL2WEfjituzGZul1PVhUUTg7a9tiRCV9GWqF
< qJQ93UQ7krH64qY5nexsWOmAJCAOQlbELe5WJShQVb3GGnDb5ccshilmlC/3Kro4
< bJyQInVxmkP2dquMIsih3CqsnF+bfmt7ObPdVb2toimn
< -----END ENCRYPTED PRIVATE KEY-----
```

=> vérifier si c'est bien les bons fichiers que l'on compare !

### Révisions associées

**Révision ea7d54b1 - 09/09/2025 10:55 - Benjamin Bohard**

Corrections pour le mode conteneur

Ne plus dépendre de la commande make et copier la configuration
au bon endroit.

Ref #36951

**Révision dd224456 - 11/09/2025 08:20 - Benjamin Bohard**

La récupération des variables est conditionnée par leur disponibilité

Ref #36951

### Historique

**#1 - 01/07/2025 17:52 - Joël Cuissinat**

*- Description mis à jour*

**#2 - 01/07/2025 17:53 - Joël Cuissinat**

*- Sujet changé de Toujours des erreurs avec les certificats  à Toujours des erreurs liées aux certificats en mode tls*

**#3 - 01/07/2025 17:57 - Joël Cuissinat**

*- Description mis à jour*

**#4 - 07/07/2025 16:36 - Benjamin Bohard**

*- Assigné à mis à Benjamin Bohard*

**#5 - 07/07/2025 16:36 - Benjamin Bohard**

*- Statut changé de Nouveau à En cours*

**#6 - 07/07/2025 17:05 - Benjamin Bohard**

Dans un cas, la clé privée et dans l'autre cas, ce qui ressemble à la sortie de openssl x509 […] -text. Ça me donne l'impression que ce n'est pas simplement un problème de fichiers comparés dans le test squash mais plutôt un problème dans le script joué au reconfigure.

**#7 - 04/09/2025 08:59 - Benjamin Bohard**

make est en dépendance de freeradius-config. On a donc une différence de disponibilité dans le contexte d'exécution du script reconfigure en mode

conteneur et en mode non-conteneur.

#### #8 - 04/09/2025 11:38 - Benjamin Bohard

Le fichier de certificat qui est copié est server.pem. Il n'est pas renommé une fois copié. Le test devrait donc porter sur le contenu de ce fichier et non du fichier server.crt. Le fichier de certificat chargé dans la configuration du module eap est server.pem également.

L'erreur de nom vient probablement d'une confusion avec l'autre test qui utilise le certificat par défaut de la machine avec l'extension .crt.

#### #9 - 09/09/2025 10:57 - Benjamin Bohard

*- Statut changé de En cours à À valider*

#### #10 - 23/09/2025 12:28 - Emmanuel GARETTE

*- Statut changé de À valider à Résolu*

*- % réalisé changé de 0 à 100*

#### #11 - 01/10/2025 11:35 - Joël Cuissinat

*- Statut changé de Résolu à Fermé*

*- Restant à faire (heures) mis à 0.0*

Test OK mais celui en mode ldap KO : #37114