

Distribution EOLE - Tâche #31548

Scénario # 31590 (Terminé (Sprint)): Validation des scénario 'cadoles' (05-07)

Valider le scénario Valider le fonctionnement de Let's Encrypt sur AmonEcole 2.8.1 (sprint 02-04)

14/01/2021 15:29 - Joël Cuissinat

Statut:	Fermé	Début:	14/01/2021	
Priorité:	Normal	Echéance:		
Assigné à:	Daniel Dehennin	% réalisé:	100%	
Version cible:	sprint 2021 05-07 Equipe MENSR	Temps estimé:	0.00 heure	
		Temps passé:	0.00 heure	
Description				
Demandes liées:				
Lié à Distribution EOLE - Scénario #31521: Valider le fonctionnement de Let's...		Terminé (Sprint)	03/05/2018	29/01/2021
Lié à Distribution EOLE - Tâche #31722: Gestion DNS avec les modules EOLE		Fermé	19/02/2021	
Lié à Distribution EOLE - Tâche #31673: Attente de fermeture des demandes let...		Fermé	09/03/2021	

Révisions associées

Révision a9d57a9b - 25/02/2021 09:51 - Emmanuel GARETTE

utiliser les certificats samba en cas d'utilisation de let's encrypt (ref #31548)

Historique

#1 - 14/01/2021 15:32 - Joël Cuissinat

- Lié à Scénario #31521: Valider le fonctionnement de Let's Encrypt sur AmonEcole 2.8.1 ajouté

#2 - 29/01/2021 08:56 - Daniel Dehennin

- Statut changé de Nouveau à En cours

#3 - 29/01/2021 08:56 - Daniel Dehennin

- Assigné à mis à Daniel Dehennin

#4 - 19/02/2021 14:10 - Daniel Dehennin

- Lié à Tâche #31722: Gestion DNS avec les modules EOLE ajouté

#5 - 23/02/2021 14:34 - Daniel Dehennin

- Fichier amonecole-2.8.1-lets-encrypt-lab1.eol ajouté

Test

- modèle de VM `etb3.amonecole-2.8.1-daily`
- réseau 1 `labs.eole.education`, la machine obtient d'OpenNebula l'adresse IP associée à `lab1.labs.eole.education`
- réseau 2 `pedago3`
- nom_domaine_local `dompedago.lab1.labs.eole.education`
- web_url `lab1.labs.eole.education`

Lors de l'instance j'ai plusieurs erreurs :

- Une erreur directement liée à Let's Encrypt, le **postservice** semble ne pas supporter la non activation de certaines variables :

```
run-parts: executing /usr/share/eole/postservice/00-letsencrypt instance
root - Erreur creole 1 : ne peut accéder à l'option "Nom de domaine ou IP à rediriger" a cause de la propriété disabled (la valeur de "Activer le reverse proxy Nginx pour http/https" est "non")
root - Erreur creole 1 : ne peut accéder à option "Activer la redirection pour tous les sous-domaines" par
```

```
ce que "Nom de domaine ou IP à rediriger" a de la propriété disabled (la valeur de "Activer le reverse proxy Nginx pour http/https" est "non")
- Demande de certificat pour amonecole.dompedago.lab1.labs.eole.education lab1.labs.eole.educationFailed to stop apache2.service: Unit apache2.service not loaded.
[OK]
run-parts: executing /usr/share/eole/letsencrypt/hooks-post.d/00-copy full
run-parts: executing /usr/share/eole/letsencrypt/hooks-post.d/99-restart full
```

- mais cela ne semble pas avoir impacter la génération d'un certificat pour les deux noms **nom_domaine_machine** et **web_url**

```
root@amonecole:~# openssl x509 -in /etc/ssl/letsencrypt/conf/live/amonecole.dompedago.lab1.labs.eole.education/cert.pem -noout -subject -ext subjectAltName
subject=CN = amonecole.dompedago.lab1.labs.eole.education
X509v3 Subject Alternative Name:
    DNS:amonecole.dompedago.lab1.labs.eole.education, DNS:lab1.labs.eole.education
```

- Le test de connection kerberos/AD échoue :

```
Test connection kerberos/AD
kinit: Cannot contact any KDC for realm 'DOMPEDAGO.LAB1.LABS.EOLE.EDUCATION' while getting initial credentials
Connection kerberos/AD impossible
```

- La modification des schémas échoue

```
run-parts: executing /usr/share/eole/postservice/26-ad_schema instance
Modified 136 records successfully
Modified 68 records successfully
Modified 14 records successfully
Modified 128 records successfully
Modified 234 records successfully
Added 24 records successfully
Modified 1 records successfully
Ajout du compte de jonction au domaine 'eole-seth-education'...
User 'eole-seth-education' created successfully
Mise en conformité de l'utilisateur 'eole-seth-education'...
Expiry for user 'eole-seth-education' disabled.
Added members to group Domain Admins
Changed password OK
Erreur : {'desc': "Can't contact LDAP server", 'errno': 107, 'info': 'Transport endpoint is not connected'}
run-parts: /usr/share/eole/postservice/26-ad_schema exited with return code 1
Erreur : postservice
```

Au final, l'instance ne va pas au bout.

#6 - 23/02/2021 14:37 - Daniel Dehennin

- Lié à Tâche #31673: Attente de fermeture des demandes let's encrypt ajouté

#7 - 24/02/2021 08:58 - Joël Cuissinat

- Sujet changé de Valider le scénario Valider le fonctionnement de Let's Encrypt sur AmonEcole 2.8.1 à Valider le scénario Valider le fonctionnement de Let's Encrypt sur AmonEcole 2.8.1 (sprint 02-04)

#8 - 24/02/2021 08:59 - Joël Cuissinat

- Tâche parente changé de #31494 à #31590

#9 - 25/02/2021 09:46 - Emmanuel GARETTE

Le certificat n'est pas copié dans le cas de let's encrypt : [#24151](#)

Dans ce cas, samba ne peut pas démarrer.

#10 - 25/02/2021 10:39 - Daniel Dehennin

Avec les dernières mises à jour :

- instance réussie
- connexion à EAD2 depuis mon poste OK avec certificat Let's Encrypt
- connexion à roundcube depuis mon poste OK avec certificat Let's Encrypt
- intégration d'un poste client windows 10 OK
- le certificat samba est celui auto-généré par samba lui-même

```
root@amonecole:~# openssl s_client -host addc.dompedago.lab1.labs.eole.education -port 636
CONNECTED(00000003)
depth=0 O = Samba Administration, OU = Samba - temporary autogenerated HOST certificate, CN = ADDC.dompedago.lab1.labs.eole.education
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 O = Samba Administration, OU = Samba - temporary autogenerated HOST certificate, CN = ADDC.dompedago.lab1.labs.eole.education
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:O = Samba Administration, OU = Samba - temporary autogenerated HOST certificate, CN = ADDC.dompedago.lab1.labs.eole.education
  i:O = Samba Administration, OU = Samba - temporary autogenerated CA certificate, CN = ADDC.dompedago.lab1.labs.eole.education
---
[...]
```

#11 - 25/02/2021 10:39 - Daniel Dehennin

- Statut changé de *En cours* à *Résolu*

- % réalisé changé de 0 à 100

#12 - 25/02/2021 10:52 - Daniel Dehennin

- Statut changé de *Résolu* à *Fermé*

- Restant à faire (heures) mis à 0.0

Fichiers

amonecole-2.8.1-lets-encrypt-lab1.eol

3,65 ko

23/02/2021

Daniel Dehennin