Infra Chapril - Anomalie #3885

Impossible de configure le SSL pour un nouveau site

25/09/2019 03:10 - Christian P. Momon

Statut:	Fermé	**Début:**	25/09/2019
Priorité:	Élevée	**Echéance:**	
Assigné à:	Christian P. Momon	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			

Description

En appliquant la procédure prévue par la doc adminsys, tout se passe bien jusqu'à la création du certificat via *dehydrated*.

https://admin.chapril.org/doku.php?id=admin:procedures:ajout-host-reverse-proxy-nginx#obtention_d_un_certificat_tls

```
=(^-^)=root@bastion:/etc/nginx/sites-enabled# dehydrated -c
Processing v1.chapril.org
 + Signing domains...
 + Generating private key...
 + Generating signing request...
 + Requesting challenge for v1.chapril.org...
  + ERROR: An error occurred while sending post-request to https://acme-v01.api.letsencrypt.org/ac
me/new-authz (Status 400)

Details:
{
  "type": "urn:acme:error:badNonce",
  "detail": "JWS has no anti-replay nonce",
  "status": 400
}
```

Et impossible d'aller plus loin.

Historique

#1 - 25/09/2019 03:15 - Christian P. Momon

Après quelques recherches, un ticket semble vraiment correspondre : https://github.com/lukas2511/dehydrated/issues/559

```
FlorentCoppint commented on 9 May 2018

I think I found the issue : since Stretch, curl is using HTTP/2 as you can see in headers.
And headers names are lower case. The expected header was "Replay-Nonce:" and it is now "replay-nonce:"
Maybe just adding "-i" to all grep commands solve the problem.
```

Le fix est disponible dans la version 0.6.2 : https://github.com/lukas2511/dehydrated/releases/tag/v0.6.2

La version actuellement utilisée sur la vm lamp est la 0.3.1 :

```
=(^-^)=root@bastion:/etc/nginx/sites-enabled# dpkg -l |grep dehydrated
ii  dehydrated                          0.3.1-3+deb9u2                 all          ACME client implemented i
n Bash
```

Du coup, confirmation que nous n'avons pas la bonne version.

#2 - 25/09/2019 03:33 - Christian P. Momon

Une solution : passer le paquet *dehydrated* en debian-backports :

```
https://packages.debian.org/search?suite=stretch-backports&searchon=names&keywords=dehydrated
Exact hits
Package dehydrated
    stretch-backports (misc): ACME client implemented in Bash
    0.6.2-2~bpo9+1: all
```

Il semble être le même que pour Buster :

```
https://packages.debian.org/search?suite=buster&searchon=names&keywords=dehydrated
Exact hits
Package dehydrated
    buster (stable) (misc): ACME client implemented in Bash
    0.6.2-2+deb10u1: all
```

#3 - 25/09/2019 03:45 - Christian P. Momon

- Statut changé de Nouveau à Résolu

Déclaration du dépôt *stretch-backports* :

```
=(^-^)=root@bastion:/etc/apt/sources.list.d# cat > stretch-backports.list
deb http://deb.debian.org/debian stretch-backports main
```

Mise à jour de la liste des paquets :

```
=(^-^)=root@bastion:/etc/apt/sources.list.d# apt-get update
Atteint:1 https://apt.chapril.org/debian stretch InRelease
Atteint:2 http://security.debian.org/debian-security stretch/updates InRelease

Réception de:3 http://deb.debian.org/debian stretch-backports InRelease [91,8 kB]

Ign:4 http://ftp.de.debian.org/debian stretch InRelease

Atteint:5 http://ftp.de.debian.org/debian stretch Release
Réception de:6 http://deb.debian.org/debian stretch-backports/main amd64 Packages [607 kB]
Réception de:7 http://deb.debian.org/debian stretch-backports/main Translation-en [465 kB]
1 165 ko réceptionnés en 0s (2 885 ko/s)
Lecture des listes de paquets... Fait
```

Augmentation de version du paquet *dehydrated* :

```
=(^-^)=root@bastion:/etc/apt/sources.list.d# apt-get -t stretch-backports install dehydrated
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants seront mis à jour :
  dehydrated
1 mis à jour, 0 nouvellement installés, 0 à enlever et 72 non mis à jour.
Il est nécessaire de prendre 80,7 ko dans les archives.
Après cette opération, 35,8 ko d'espace disque supplémentaires seront utilisés.
Réception de:1 http://deb.debian.org/debian stretch-backports/main amd64 dehydrated all 0.6.2-2~bpo9+1 [80,7 k
B]
80,7 ko réceptionnés en 0s (2 365 ko/s)
[master 32eae76] saving uncommitted changes in /etc prior to apt run
 Author: Christian Pierre MOMON <cmomon@april.org>
 5 files changed, 44 insertions(+)
 create mode 100644 apt/sources.list.d/stretch-backports.list
 create mode 100644 nginx/sites-available/v1.chapril.org
 create mode 120000 nginx/sites-enabled/v1.chapril.org
Lecture des fichiers de modifications (« changelog »)... Terminé
(Lecture de la base de données... 42121 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../dehydrated_0.6.2-2~bpo9+1_all.deb ...
Dépaquetage de dehydrated (0.6.2-2~bpo9+1) sur (0.3.1-3+deb9u2) ...
Paramétrage de dehydrated (0.6.2-2~bpo9+1) ...
Traitement des actions différées (« triggers ») pour man-db (2.7.6.1-2) ...
Scanning processes...

Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
```

Vérification de la version du paquet installé :

```
=(^-^)=root@bastion:/etc/nginx/sites-enabled# dpkg -l |grep  dehydrated
ii  dehydrated                          0.6.2-2~bpo9+1                all          ACME client implemented i
n Bash
```

Tentative d'obtenir un certificat pour le nouveau site web :

```
=(^-^)=root@bastion:/etc/nginx/sites-enabled# dehydrated -c
# INFO: Using main config file /etc/dehydrated/config
# INFO: Using additional config file /etc/dehydrated/conf.d/test-ca.sh
! Reusing account from https://acme-v01.api.letsencrypt.org/directory
 + Creating chain cache directory /var/lib/dehydrated/chains
Processing chapril.org with alternative names: www.chapril.org
 + Checking domain name(s) of existing cert... unchanged.
 + Checking expire date of existing cert...
 + Valid till Nov 30 03:47:12 2019 GMT Certificate will not expire
(Longer than 30 days). Skipping renew!
Processing v1.chapril.org
 + Signing domains...
 + Generating private key...
 + Generating signing request...
 + Requesting new certificate order from CA...
 + Received 1 authorizations URLs from the CA
 + Handling authorization for v1.chapril.org
 + 1 pending challenge(s)
 + Deploying challenge tokens...
 + Responding to challenge for v1.chapril.org authorization...
 + Challenge is valid!
 + Cleaning challenge tokens...
 + Requesting certificate...
 + Checking certificate...
 + Done!
 + Creating fullchain.pem...
 + Done!
```

Ça fonctionne \o/

#4 - 25/09/2019 14:44 - Quentin Gibeaux

ça me semble bien

#5 - 11/01/2020 05:57 - Christian P. Momon

- Projet changé de Chapril à Infra Chapril

- Statut changé de Résolu à Fermé