Mise en place de certificats SSL Let's Encrypt wildcard avec API Gandi LiveDNS

Le titre parle de lui même. En validation DNS-01 Let's Encrypt a besoin de mise à jour des LiveDNS chez Gandi. Voici les scripts et commandes pour automatiser le processus.

Prérequis

- Avoir cotre clé API Gandi
- Avoir activé LiveDNS pour votre domaine
- Certbot installé sur votre serveur linux, version 0.22 minimum
- Avoir déjà une connaissance de Certbot

Scripts

Script pour déclarer votre clé API Gandi

```
#!/bin/bash
APIKEY="XXXXXXXXXXXXXXXXXXXXXXXXXXX"
```

Script Auth pour mettre à jour le live DNS

```
#!/bin/bash

# Appel clé API
source ./gandi-api-key.sh

API="https://dns.api.gandi.net/api/v5/"
DOMAIN=$CERTBOT_DOMAIN
RECORD="_acme-challenge"


#Debug
echo "DOMAIN :" $CERTBOT_DOMAIN
echo "VALIDATION :" $CERTBOT_VALIDATION

# Données à envoyer
DATA='{"rrset_values": ["'$CERTBOT_VALIDATION'"]}'
```

```
# Appel API
curl -s -XPUT -d "$DATA" \
    -H"X-Api-Key: $APIKEY" \
    -H"Content-Type: application/json" \
    "$API/domains/$DOMAIN/records/$RECORD/TXT"

# Sleep pour propager au Gandi LiveDNS
sleep 60
```

Utilisation

```
#!/bin/bash
certbot-auto certonly --server
https://acme-v02.api.letsencrypt.org/directory --manual-public-ip-logging-ok
--preferred-challenges dns-01 --manual-auth-hook ./gandi-auth.sh --manual -d
*.mondomaine.net -d mondomaine.net
```

Rajoutez le paramètre –dry-run pour effectuer d'abord vos tests.

Ces scripts ne gèrent aucunement les erreurs. Utilisation quick and dirty uniquement. A vos risques et périls.

Ne déplacez pas le script d'auth, le renew automatique de certbot fais appel à lui.

Sources

doc.livedns.gandi.net