Consortium GARR

THE ITALIAN EDUCATION & RESEARCH NETWORK

TCS Webinar: ACME Case Study: GARR

BARBARA MONTICINI

13th April 2021

Webinar

Agenda

- Why ACME?
- Welcome ACME!
- Automation strategies
- Conclusions

The server certificate is going to expire ...

- **Expiration day** is the certificate management **critical point.**
- Since 2020 commercial CAs started issuing **1 year validity** certificates -> expiration day is coming quicker and more frequently.
- Admins’ reaction

Welcome ACME

- ACME protocol is an open and flexible solution to manage certificates, providing automated requests, retrievals and renewals.

- GARR has undertaken the effort to share ACME protocol knowledge within its community by creating a Wiki page about Certbot installation, account creation (on SCM) and registration, basic certificates operations.

ACME account strategies

- Implementing Certbot/ACME in a pool of servers implies two possible scenarios:

   1. creating one ACME account on SCM for every new server setup;

   2. reusing a pre-existent ACME account (copying the folder /accounts)

Need for further automation?

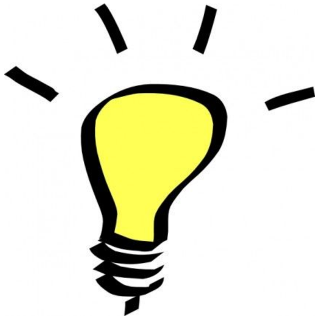
- Manually acquiring a certificate via Certbot client is quick and easy but can become tedious when deploying larger fleets.

- Solutions: using a configuration management tool, as Ansible, help to carry out these tasks completely automatic and reproducible.

Food for thoughts - ideas to share

- Ansible playbook for Debian that installs Certbot and creates a new ACME account via API for every new server setup:
    - https://github.com/francescm/acme-ansible-debian-sectigo

- A simple ansible playbook/role for Debian that sets up a new environment with Certbot reusing a pre-existent ACME account:
    - installing Certbot
    - copying folder **/etc/letsencrypt/accounts**
    - requesting the new certificate on the remote server



Conclusions

- Numbers: 350 certs out of 8000 issued via ACME
- Positive feedbacks from our community with growing interest
- Ansible + ACME is a good strategy to increase the level of automation

Questions received so far:

- Grid certificates (IGTF) via ACME?
- RAO approval on requests via ACME?
- Why aren’t ACME requested certificates visible (*yet*)?

References

- ACME RFC 8555
    - https://tools.ietf.org/html/rfc8555
- Certbot
    - https://certbot.eff.org/
- GARR TCS wiki
    - https://wiki.idem.garr.it/wiki/GARRCS:GARR-TCS-4