ACME self-service

Certificates for the masses :-)

overall architecture
architectural details

• “certbot” is the tool developed by Electronic Frontier Foundation (EFF), to manage the certificates in an ACME infrastructure
• nas01 and nas02 are two NFS servers replicating to each other. It’s a low end NAS solution: https://forge.puppet.com/modules/maxadamo/tiny_nas
• the certificates are declared in gitlab: hieradata_extra/production_acme.yaml
• for each new certificate that we declare, a job is triggered and a crontab entry it’s added
• the cron entry checks the expiration date of the certificate
• if the certificate is expiring the tools geant_acme.py is triggered
• geant_acme.py creates a DNS challenge on Infoblox and triggers certbot with a DNS custom hook *(this line was missing during the presentation)*
• geant_acme.py uploads the public key to Redis and the private key to Vault
• for each new certificate a new monitoring check is added to Sensu
crontab example (on nas servers)

38 4 * * * /bin/check-ssl-cert.rb -c 30 -w 30 -P /etc/sectigo_ev/live/test-certificate.geant.org/fullchain.pem >/dev/null || /root/bin/geant_acme.py -p sectigo_ev -u dream_team -d test-certificate.geant.org -d certificate.geant.org -d another-sna.geant.org -x --force-renewal
adding new certificates  
gitlab@gitlab.geant.net:puppet/hieradata_extra.git
### SectiGO EV | Home

This report was generated on 2020-11-27 20:00:01 UTC

<table>
<thead>
<tr>
<th>Certificate name</th>
<th>Domains (SANs)</th>
<th>Expiry Date</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>academy.geant.org</td>
<td>academy.geant.org</td>
<td>VALID: 265 days</td>
<td>8e63e0b72036c96dfc216872</td>
</tr>
<tr>
<td>authzmanager.geant.org</td>
<td>authzmanager.geant.org</td>
<td>VALID: 340 days</td>
<td>5acbec608d62b79dc4bc0d45f</td>
</tr>
<tr>
<td>cacti.geant.org</td>
<td>cacti.geant.org</td>
<td>VALID: 346 days</td>
<td>a894b460e4f237dc33321668f</td>
</tr>
<tr>
<td>consul.geant.net</td>
<td>consul.geant.net</td>
<td>VALID: 321 days</td>
<td>5db312d336ae52b3090e1116f</td>
</tr>
<tr>
<td>events.geant.org</td>
<td>events.geant.org</td>
<td>VALID: 295 days</td>
<td>6ba20/2601a9cd4d32854e49</td>
</tr>
<tr>
<td>gdp.geant.net</td>
<td>gdp.geant.net</td>
<td>VALID: 286 days</td>
<td>3138005d2140526dc63e4fb0c</td>
</tr>
<tr>
<td>gitlab.geant.net</td>
<td>gitlab.geant.net</td>
<td>VALID: 362 days</td>
<td>5031d9e74862619460f1e68</td>
</tr>
<tr>
<td>heimdall.geant.org</td>
<td>heimdall.geant.org</td>
<td>VALID: 362 days</td>
<td>e63b590d0731a02d8667b52d</td>
</tr>
<tr>
<td>hosted.geant.org</td>
<td>hosted.geant.org</td>
<td>VALID: 295 days</td>
<td>8761af7808ba0defc7789caaf</td>
</tr>
</tbody>
</table>
clients

- **puppet agent**

  ```ruby
  geant_acme::client { "${consul_influx_service}.service.ha.geant.org":
    provider => 'sectigo_ev',
    cert_owner => 'influxdb',
    cert_group => 'influxdb',
    notify   => Service[$service_name],
    before   => File["/etc/influxdb/${conf_file}"];
  }
  
  advantages:
  it comes with the advantages of your configuration management: for instance it notifies the application (service reload)
  disadvantages:
  it can be used only internally on servers running the puppet agent

- **shell script**

  ```shell
  http://repositories.geant.org/pub/acme/acme-download.sh
  
  advantages:
  smaller and easy to modify
  disadvantages:
  it requires openssl, curl, jq, bash

- **Go application**

  ```go
  https://gitlab.geant.org/massimiliano.adamo/acme-downloader
  
  advantages:
  - it is tested on Linux and Windows but it compiles on 43 different platforms
  - zero dependencies
  disadvantages:
  - bigger size
acme-downloader output

```
C:\Users\massimilianoadam\Downloads\\.acme-downloader --redis-token --cert-token --cert-name heimdall.geant.org --team-name swd --cert-destination "c:\\acme\\cert\\heimdall.geant.org.crt" --fullchain-destination "c:\\acme\\cert\\heimdall.geant.org_fullchain.crt" --key-destination "c:\\acme\\cert\\heimdall.geant.org_key" --ca-destination "c:\\acme\\cert\\COMODO_EV.crt" --days 30
[INFO] installed: c:\\acme\\cert\\heimdall.geant.org.crt
[INFO] installed: c:\\acme\\cert\\COMODO_EV.crt
[INFO] installed: c:\\acme\\cert\\heimdall.geant.org_fullchain.crt
[INFO] installed: c:\\acme\\cert\\heimdall.geant.org_key
PS C:\Users\massimilianoadam\Downloads> \.acme-downloader --redis-token --cert-token --cert-name heimdall.geant.org --team-name swd --cert-destination "c:\\acme\\cert\\heimdall.geant.org.crt" --fullchain-destination "c:\\acme\\cert\\heimdall.geant.org_fullchain.crt" --key-destination "c:\\acme\\cert\\heimdall.geant.org_key" --ca-destination "c:\\acme\\cert\\COMODO_EV.crt" --days 30
[INFO] the certificates are still valid
PS C:\Users\massimilianoadam\Downloads> PS C:\Users\massimilianoadam\Downloads>
```

```
root visnu home maxadamo puppet6 geant_acme files production # ./acme-downloader.sh --redis-token --cert-token --cert-name foo-ev-cert.geant.org --team-name swd
installed: /etc/ssl/certs/foo-ev-cert.geant.org.crt
installed: /etc/ssl/certs/foo-ev-cert.geant.org_fullchain.crt
installed: /etc/ssl/certs/COMODO_EV.crt
installed: /etc/ssl/private/foo-ev-cert.geant.org.key
```
process flow: Foo user wants to create the certificate bar.geant.org

✓ Foo adds a certificate definition for bar.geant.org to production_acme.yaml, commits & pushes

✓ waits around 15 minutes for puppet to run either on nas01 or 02 (or run puppet manually)

✓ he can optionally check https://acme.geant.org/ to ensure that bar.geant.org is present

✓ imagine Foo having a certificate installed on Apache. He can create a crontab entry using the following command:

```bash
acme-downloader.sh --redis-token <redis-token> --vault-token <vault-token> --team-name dream_team --cert-name bar.geant.org; if [ $? -eq 64 ]; then systemctl restart httpd; fi
```
ToDo ?
Useful Links

• Hiera Redis for Puppet: https://forge.puppet.com/modules/maxadamo/hiera_redis

• Hiera Vault for Puppet: https://forge.puppet.com/modules/petems/hiera_vault

• Tiny NAS: https://forge.puppet.com/modules/maxadamo/tiny_nas

• Geant ACME (not general purpose): https://gitlab.geant.org/massimiliano.adamo/geant_acme

• ACME Downloader (Go): https://gitlab.geant.org/massimiliano.adamo/acme-downloader

Final thoughts & considerations

• You do not have Puppet?

• SaltStack has a pillar for Vault and several pillars fit to store the public keys
• Ansible/Chef? Ask the experts!