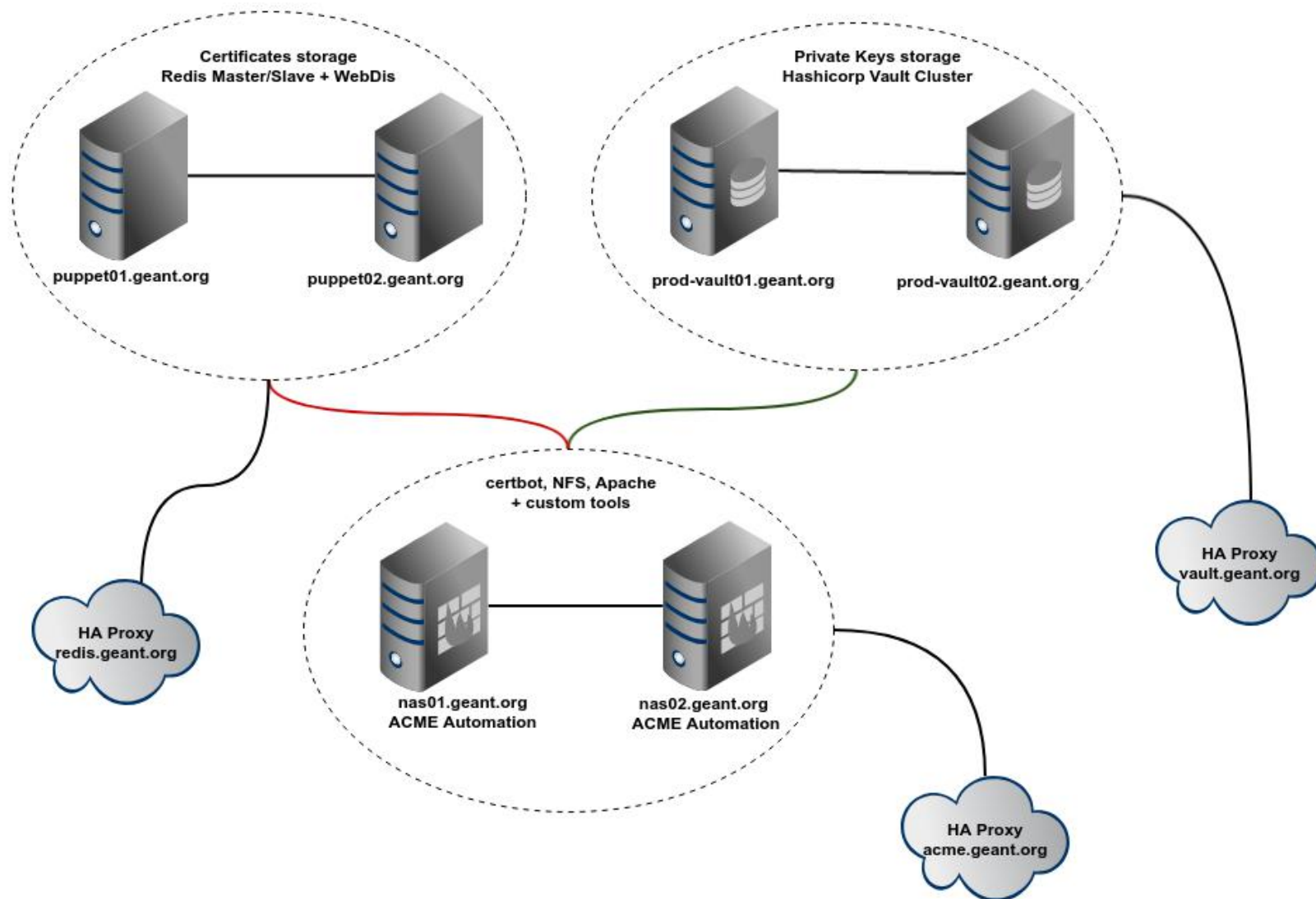


ACME self-service

Certificates for the masses :-)

overall architecture



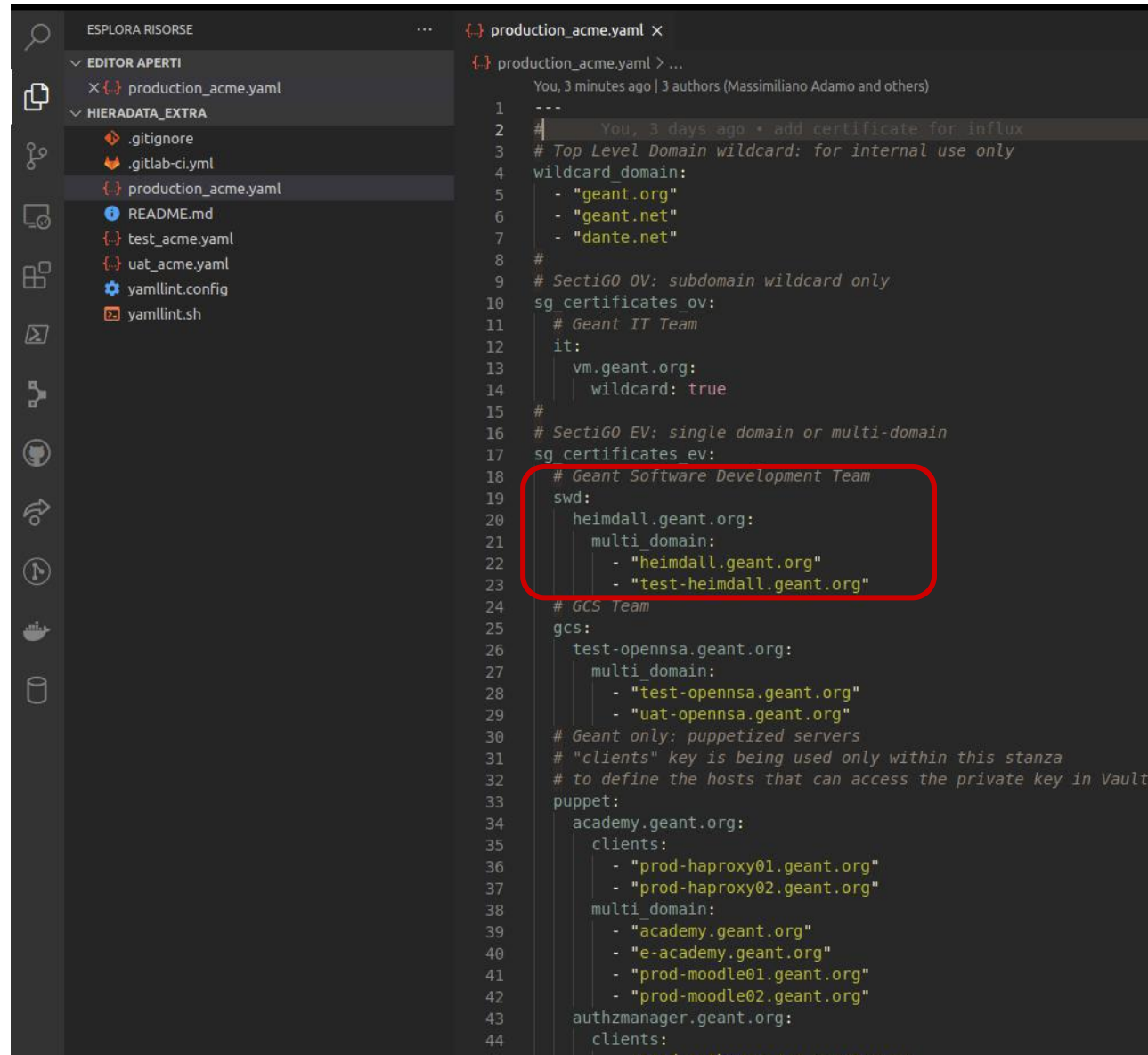
architectural details

- “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`



```
1 ---
2 # You, 3 days ago * add certificate for influx
3 # Top Level Domain wildcard: for internal use only
4 wildcard_domain:
5   - "geant.org"
6   - "geant.net"
7   - "dante.net"
8 #
9 # SectiGO OV: subdomain wildcard only
10 sg_certificates_ov:
11   # Geant IT Team
12   it:
13     vm.geant.org:
14       wildcard: true
15 #
16 # SectiGO EV: single domain or multi-domain
17 sg_certificates_ev:
18   # Geant Software Development Team
19   swd:
20     heimdall.geant.org:
21       multi_domain:
22         - "heimdall.geant.org"
23         - "test-heimdall.geant.org"
24 # GCS Team
25 gcs:
26   test-opennsa.geant.org:
27     multi_domain:
28       - "test-opennsa.geant.org"
29       - "uat-opennsa.geant.org"
30 # Geant only: puppetized servers
31 # "clients" key is being used only within this stanza
32 # to define the hosts that can access the private key in Vault
33 puppet:
34   academy.geant.org:
35     clients:
36       - "prod-haproxy01.geant.org"
37       - "prod-haproxy02.geant.org"
38     multi_domain:
39       - "academy.geant.org"
40       - "e-academy.geant.org"
41       - "prod-moodle01.geant.org"
42       - "prod-moodle02.geant.org"
43   authzmanager.geant.org:
44     clients:
```

https://acme.geant.org

https://acme.geant.org/sectigo

SectiGO EV | Home

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

Certificate name	Domains (SANs)	Expiry Date	Serial Number
academy.geant.org	academy.geant.org	VALID: 295 days	8e63e0ba72036c96dfc216872
authzmanager.geant.org	authzmanager.geant.org	VALID: 340 days	5acbde508d62b79dc4bc0d45f
cacti.geant.org	cacti.geant.org	VALID: 346 days	a894b460a40237dc32321668f
consul.geant.net	consul.geant.net	VALID: 321 days	55db312d336ac52e3008e116f
events.geant.org	events.geant.org	VALID: 295 days	6ba20f2601a9cd4d392854e49
gidp.geant.net	gidp.geant.net	VALID: 286 days	3138005d2140526cd63c4fb0c
gitlab.geant.net	gitlab.geant.net	VALID: 362 days	5031dce74862619f46cd1ae68
heimdall.geant.org	heimdall.geant.org	VALID: 362 days	e63b59f0d9731a02d8667b52d
hosted.geant.org	hosted.geant.org	VALID: 295 days	876f1af780f8ba9defc7789caaf

clients

- **puppet agent**

```
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**

<http://repositories.geant.org/pub/acme/acme-download.sh>

advantages:

smaller and easy to modify

disadvantages:

it requires openssl, curl, jq, bash

- **Go application**

<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

```
Windows PowerShell
PS C:\Users\massimiliano.adamo\Downloads> .\acme-downloader --redis-token [REDACTED] --vault-token [REDACTED] --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\\key\\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\\key\\heimdall.geant.org.key
PS C:\Users\massimiliano.adamo\Downloads>
PS C:\Users\massimiliano.adamo\Downloads> .\acme-downloader --redis-token [REDACTED] --vault-token [REDACTED] --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\\key\\heimdall.geant.org.key" --ca-destination "c:\\acme\\cert\\COMODO_EV.crt" --days 30
[INFO] the certificates are still valid
PS C:\Users\massimiliano.adamo\Downloads>
PS C:\Users\massimiliano.adamo\Downloads>
```

```
root visnu home maxadamo puppet6 geant_acme files production # ./acme-downloader.sh --redis-token [REDACTED] --vault-token [REDACTED] --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:

```
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>
- ACME Downloader (shell): https://gitlab.geant.org/massimiliano.adamo/geant_acme/-/blob/master/files/acme-downloader.sh

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!