KMG GROUP
No news is good news

Ansible meetup

Managing Letsencrypt SSL certificates in NGINX clusters

Magnus Lübeck, Zürich, 2. April. 2019
http://kmg.group

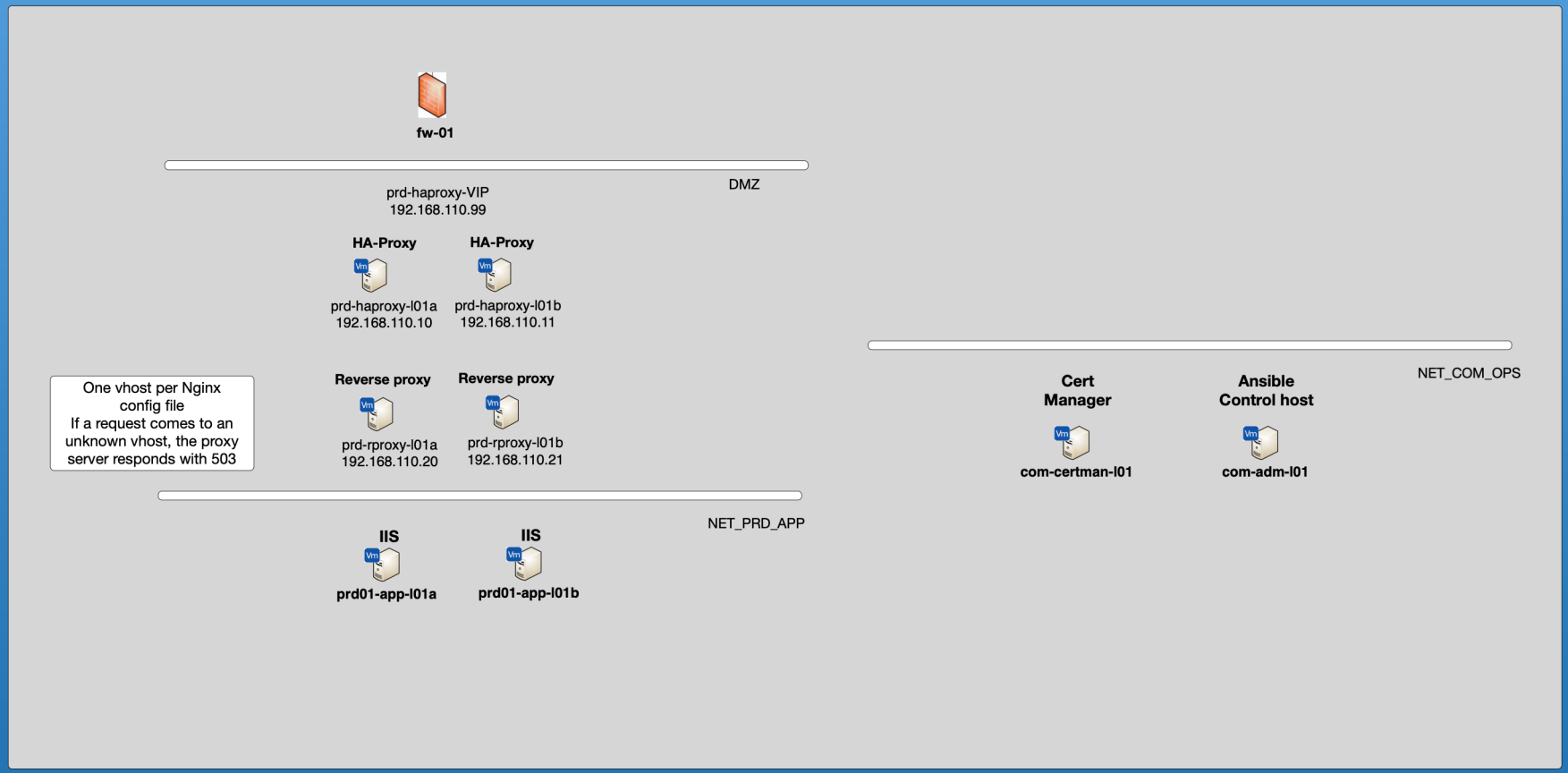
Outline

KMG GROUP
No news is good news

- **Quick overview**
- **HAProxy**
- **Round robin vs hashing**
- **HAProxy protocol**
- **Nginx config for logging correct IP**
- **Nginx dummy certificate**
- **DNS Wildcard vs single hosts**
  - SSL for internal systems
- **Letsencrypt**
  - Cert manager host
  - /.well-known location in nginx config
  - New certificates
  - Renew
- **Testing and Troubleshooting**
  - Curl
  - Testssl.sh

Quick overview

KMG GROUP
No news is good news



HAProxy

KMG GROUP
No news is good news

- We usually use a mix between
  - VRRP / keepalived
  - Haproxy
  - Nginx as ssl termination point
- HAProxy protocol
- Nginx config for logging correct IP

Nginx dummy certificate

KMG GROUP
No news is good news

- Default installation sets up a dummy certificate
- This way nginx starts, and we are ready for when we can deploy the certificate

```
- stat: path=/etc/nginx/{{sslDhCert}}
  register: dhKeyExist
  tags:
    - config
    - ssl
    - nginx-config

- stat: path={{sslKeysPath}}/{{sslKeyCert}}
  register: sslKeysExist
  tags:
    - config
    - ssl

- file: name={{sslKeysPath}} state=directory mode=0755 owner=root
  become: true
  tags:
    - config
    - ssl

- name: Generate self-signed keys (for Vagrant box)
  become: yes
  become_method: sudo
  shell: 'openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout {{sslKeysPath}}/{{sslKeyCert}} -out {{sslKeysPath}}/{{sslKeyBundle}} -subj "/C=CH/ST=Zurich/L=Zurich/O=Mycompany/CN=dummy.ch" '
  when: sslKeysExist.stat.exists == False
  notify:
    - restart nginx
  tags:
    - config
    - ssl

- name: Generate DH-cert ({{sslDhKeySize}} bit)
  become: yes
  become_method: sudo
  shell: 'openssl dhparam -out /etc/nginx/{{sslDhCert}} {{sslDhKeySize}}'
  when: dhKeyExist.stat.exists == False
  notify:
    - restart nginx
  tags:
    - config
    - ssl
```

Haproxy protocol and HTTPS

KMG GROUP
No news is good news

- You can listen to multiple ports in one server section for NGINX
- Use port 443 for normal HTTPS
- Use port 444 for haproxy protocol between HAProxy and NXINX

```
server {
  listen 443;
  listen 444 ssl proxy_protocol;
```

DNS Wildcard vs single hosts

KMG GROUP
No news is good news

- Wildcards are debated, and are usually not offered by default
- Allows for letsencrypt SSL certificates for internal systems where you might not be able to use letsencrypt's wildcard certificate

- Example: myhost.internal.smalometern.com

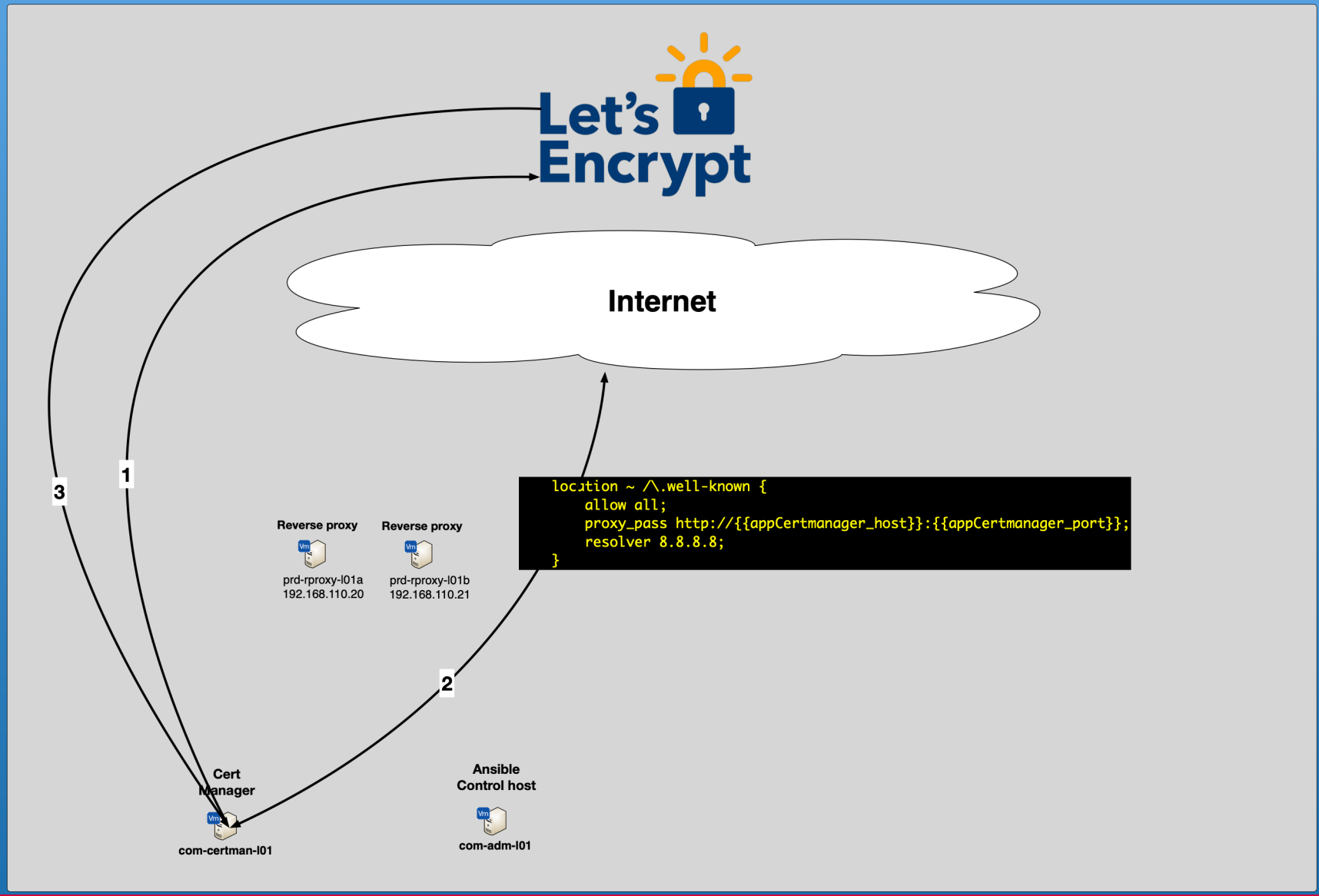
Cert manager host

KMG GROUP
No news is good news

- packages: nginx, letsencrypt
- /.well-known location in nginx config
- New certificates
- Renew

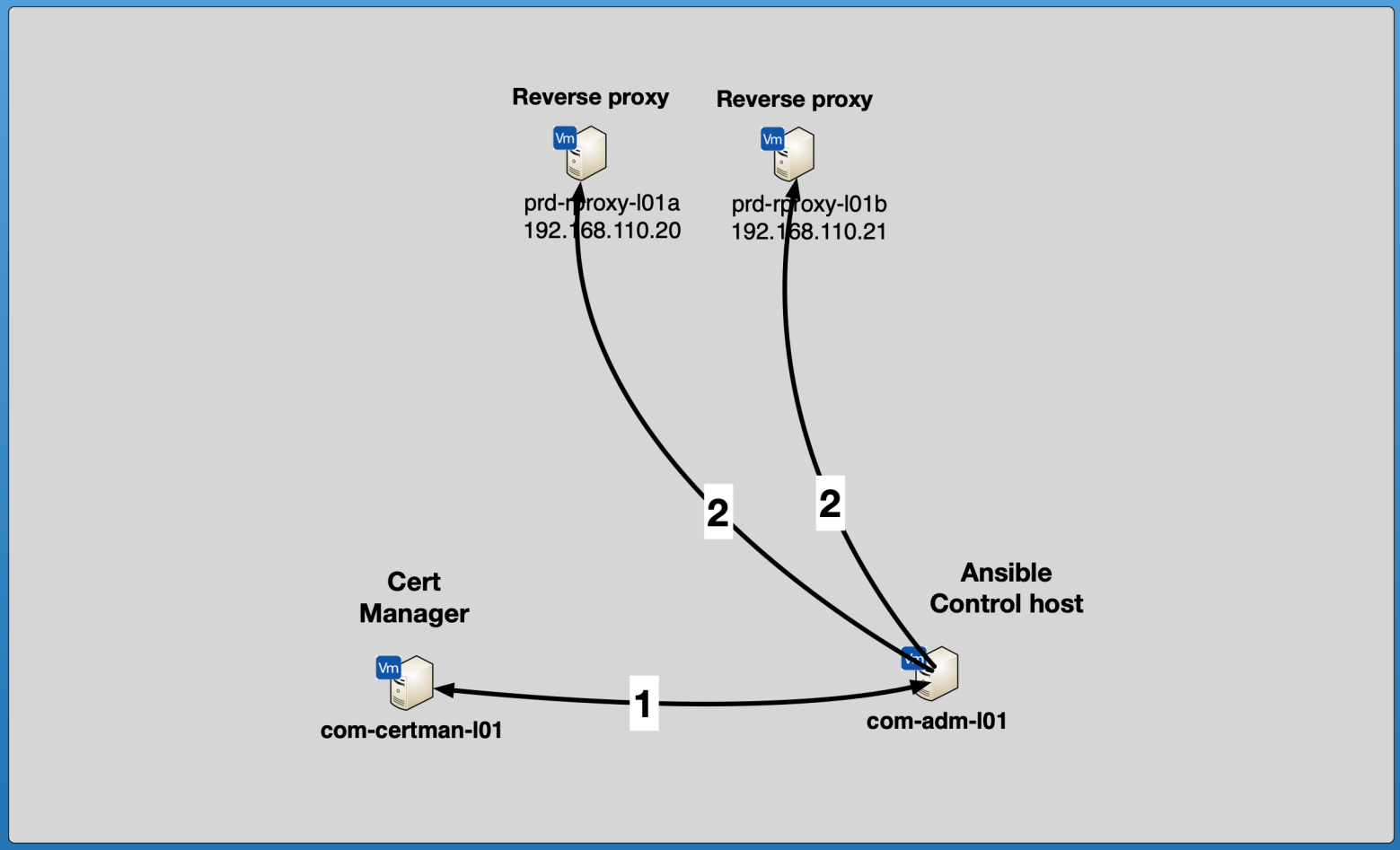
Letsencrypt

KMG GROUP
No news is good news



Pushing certificates

KMG GROUP
No news is good news



Pushing certificates – playbook

KMG GROUP
No news is good news

```
[maglub@Magnuss-MacBook-Pro-2:~/dev/kmg/20190402-ansible-meetup/ansible (master)]$ cat playbooks/letsencrypt-deploy-certs.yml
---
- hosts: demo-rproxy
  become: true
  roles:
    - { role: KMG.letsencrypt-deploy-certs }
  vars:
    letsencrypt_certmanager_sites:
      - "demo.smalometern.com"
  tags:
    certs-rproxy
```

Pushing certificates – main.yml

KMG GROUP
No news is good news

- The main.yml loops through the certificates and includes deploy-ssl.yml

```
[maglub@Magnuss-MacBook-Pro-2:~/dev/kmg/20190402-ansible-meetup/ansible (master)]$ cat roles.galaxy/KMG.letsencrypt-deploy-certs/tasks/main.yml
---
# tasks file for letsencrypt-deploy-certs
- name: Create ssl directories in /etc/nginx/ssl
  file: name=/etc/nginx/ssl/{{item}} state=directory mode=0755 owner=root
  become: true
  tags:
    - letsencrypt
  with_items: "{{ letsencrypt_certmanager_sites }}"

- include: deploy-ssl.yml
  vars:
    ssl_proxy_domain: "{{outer_item}}"
  tags:
    - letsencrypt
    - bapp
  with_items: "{{ letsencrypt_certmanager_sites }}"
  loop_control:
    loop_var: outer_item
```

Pushing certificates – deploy-ssl.yml

KMG GROUP
No news is good news

- Slurp the file from the certmanager host
- Copy it to the nginx servers

```
[maglub@Magnuss-MacBook-Pro-2:~/dev/kmg/20190402-ansible-meetup/ansible (master)]$ cat roles.galaxy/KMG.letsencrypt-deploy-certs/tasks/deploy-ssl.yml
---
- name: read certificate for {{ ssl_proxy_domain }} from {{ appCertmanager_host }}
  become: true
  slurp:
    src: '/etc/letsencrypt/live/{{ ssl_proxy_domain }}/{{item}}'
  register: certificate
  delegate_to: "{{ appCertmanager_host }}"
  remote_user: "{{appCertmanager_user}}"
  with_items:
    - fullchain.pem
    - privkey.pem
  tags:
    - letsencrypt

- name: put certificate onto the proxy server for {{ ssl_proxy_domain }}
  become: true
  copy:
    content: "{{ item.content | b64decode }}"
    dest: /etc/nginx/ssl/{{ssl_proxy_domain}}/{{item['item']}}
    owner: root
    group: root
    mode: 0640
  notify:
    - restart nginx
  tags:
    - letsencrypt
  with_items: "{{certificate['results']}}"
```

Demo

KMG GROUP
No news is good news

Troubleshooting

KMG GROUP
No news is good news

- Curl
- Testssl.sh

cUrl

KMG GROUP
No news is good news

- -k => insecure
- -v => verbose (headers and redirection)
- --resolve => the swiss army knife
- --haproxy-protocol => (in newer curl, 7.60.0) helps a lot when debugging HAProxy with nginx

```
curl -k https://asdf.smalometern.com/.well-known/apa.html
curl -k --resolve asdf.smalometern.com:443:192.168.111.39 https://asdf.smalometern.com/.well-known/apa.html
curl --resolve demo.smalometern.com:443:192.168.111.20 https://demo.smalometern.com/demo/welcome.html
curl --resolve demo.smalometern.com:443:192.168.111.21 https://demo.smalometern.com/demo/welcome.html
curl -v -k --resolve demo.smalometern.com:443:192.168.111.20 https://demo.smalometern.com/demo/welcome.html
curl -v -k --resolve demo.smalometern.com:443:192.168.111.21 https://demo.smalometern.com/demo/welcome.html
curl -k --resolve demo.smalometern.com:443:192.168.111.20 https://demo.smalometern.com/demo/welcome.html
curl -k --resolve demo.smalometern.com:443:192.168.111.21 https://demo.smalometern.com/demo/welcome.html
```

Testssl.ch

KMG GROUP
No news is good news

- https://testssl.sh
- ./testssl.sh -S --ip 192.168.111.99 demo.smalometern.com
- --ip => helps when checking a specific proxy server
- -S => shows certificate info (not the whole test suite)

References

KMG GROUP
No news is good news

- https://kmg.group
- Questions?