

DNS + Certificates

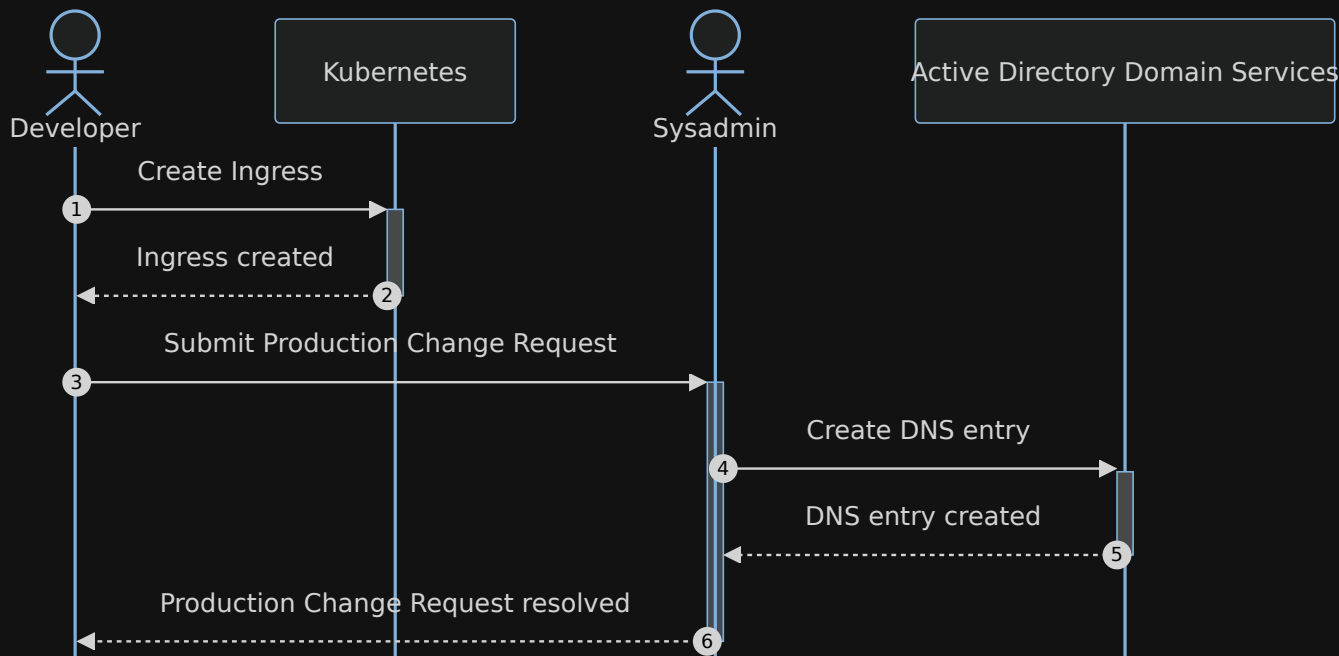
Automated generation of DNS A records and TLS certificates for multi-cluster Kubernetes

CHUA SONG ANN

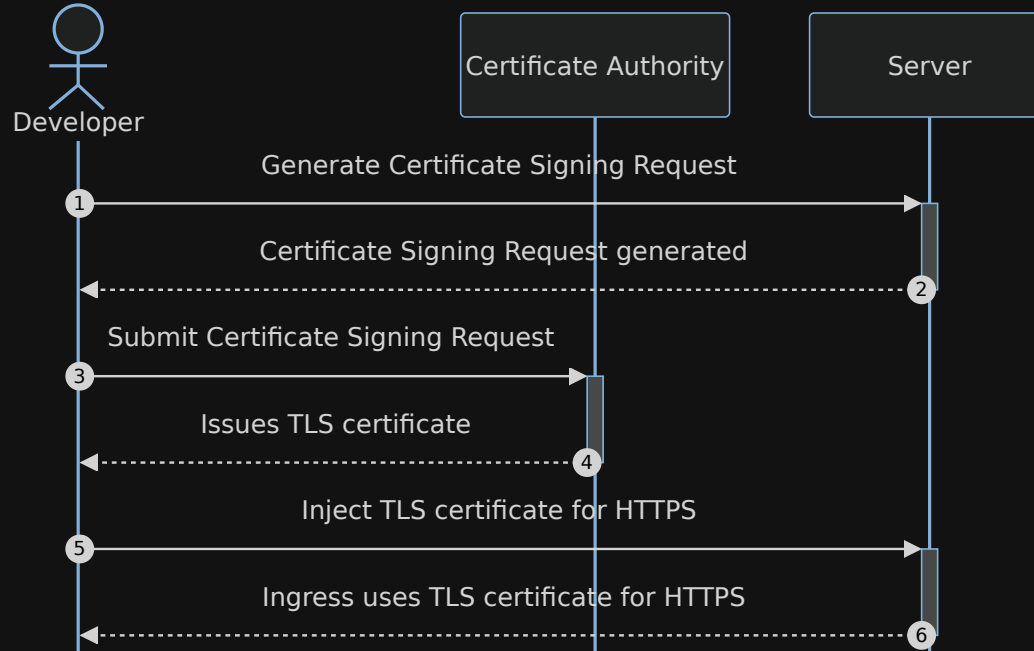
We don't enjoy manual work



Manual DNS Creation



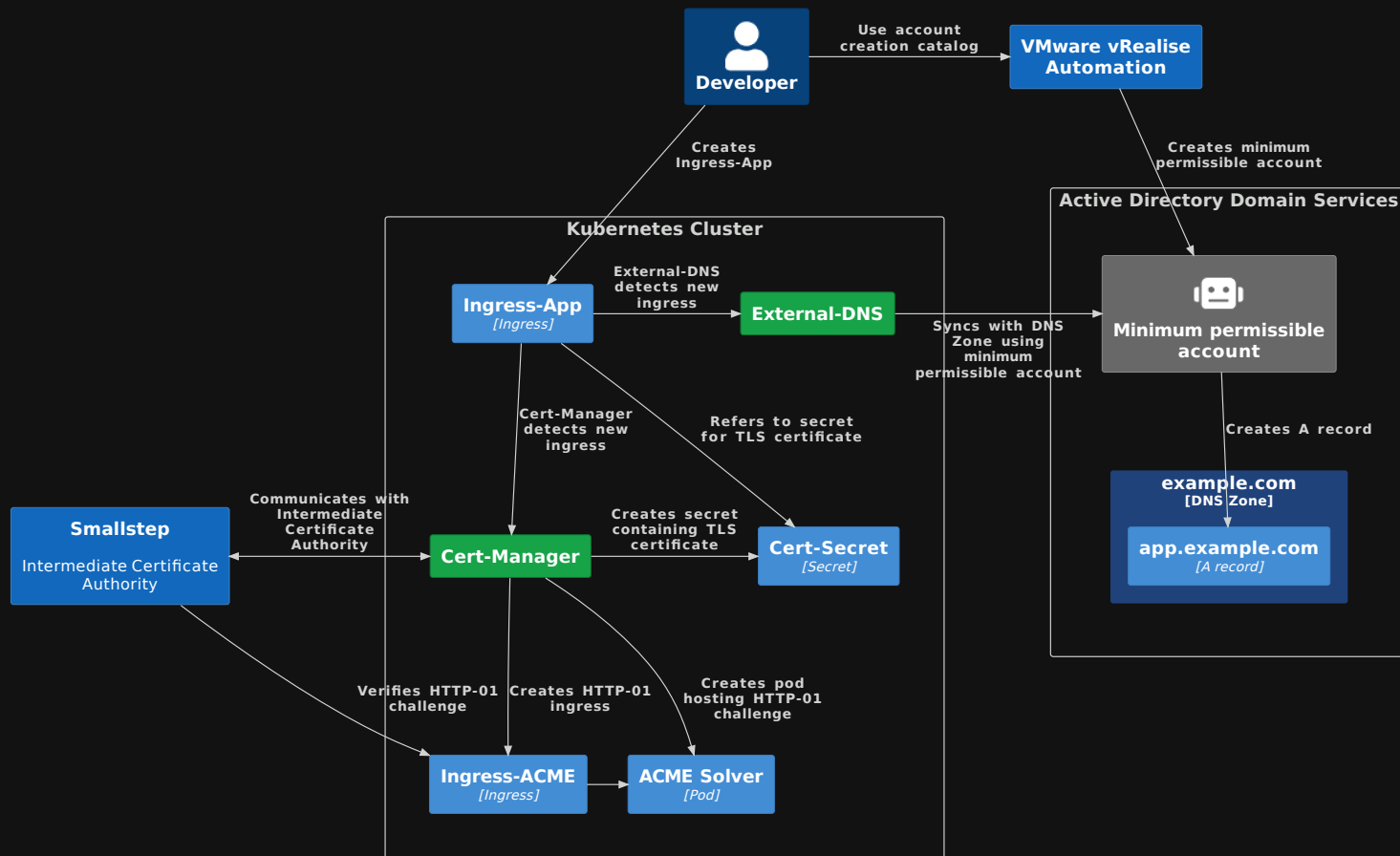
Manual TLS Certificate Creation



Let's automate it!



Architecture



No native multi-cluster support

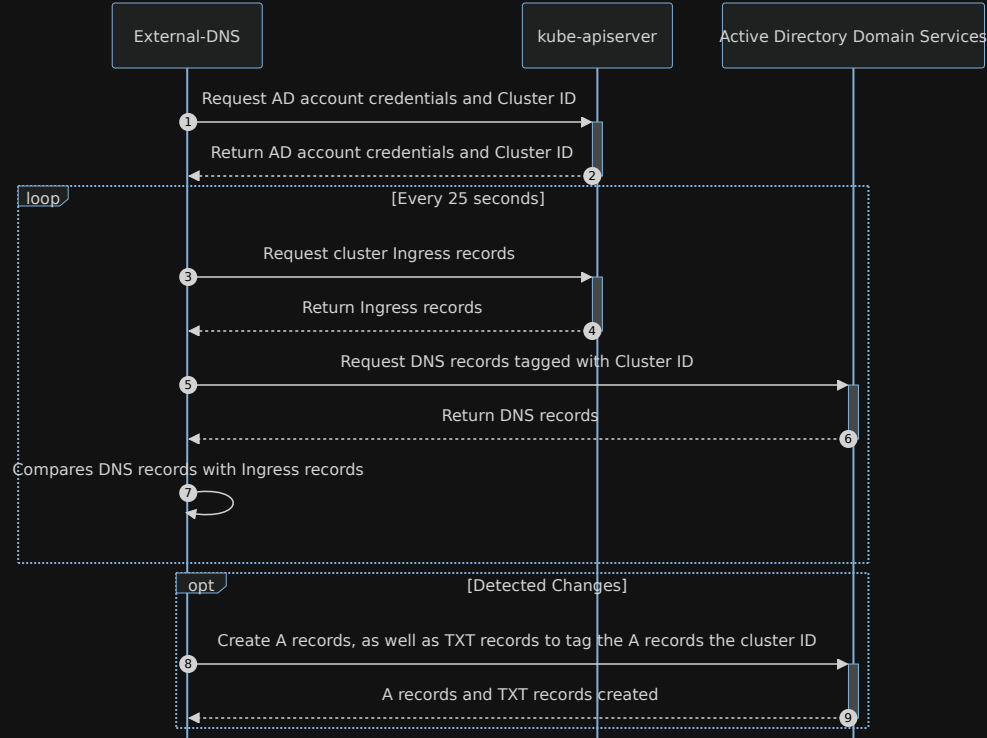
External-DNS is built for single-cluster use-cases

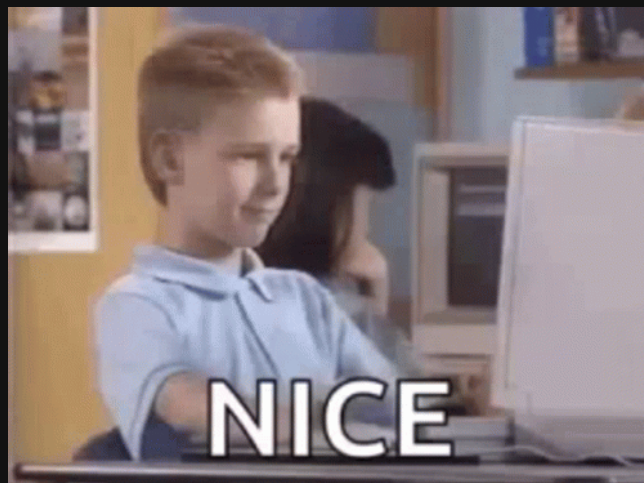
Multi-cluster External-DNS

We control External-DNS's access to Active Directory on 2 levels

1. Cluster ID — A unique text tagged to DNS records created, to identify the owner of the DNS record
 - Automatically created in the format ``supervisor_namespace`-`cluster_name`` when cluster is onboarded to Rancher Dashboard
2. AD account credentials — Required for External-DNS to be able to create and modify DNS records
 - Minimum permissible account created through VMware vRealize Automation

Automated multi-cluster DNS Creation





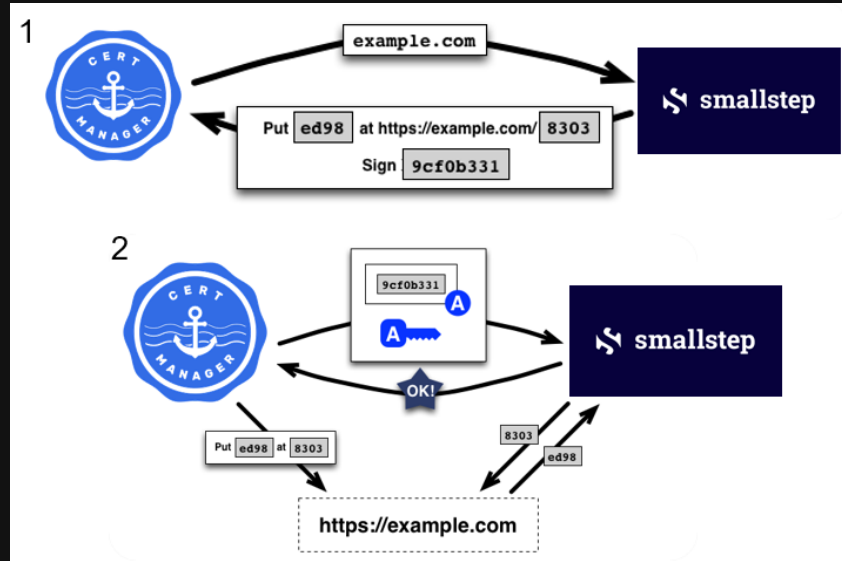
What is ACME?

- Automated Certificate Management Environment
- Protocol for automatic validation and issuance of certificates from a Certificate Authority
- No human interaction required

Summarized steps:

1. The agent proves to the Certificate Authority that the webserver controls a domain
2. The agent then can proceed to request, renew, and revoke certificates for that domain

HTTP-01 Example



Possible choices

ACME-ACDS-Server

- Enables installing ACME-ACDS as a website in Windows Server Active Directory to enable ACME certificate requests from Windows Server Active Directory Certificate Services
- Hobby project with no enterprise level support
- Installing custom components in Active Directory may lead to downstream issues with patching/upgrading

Vault

- Generic secrets management product
- Does not have ACME support
- Need to solve the bottom turtle problem ("Secret Zero")

What we chose

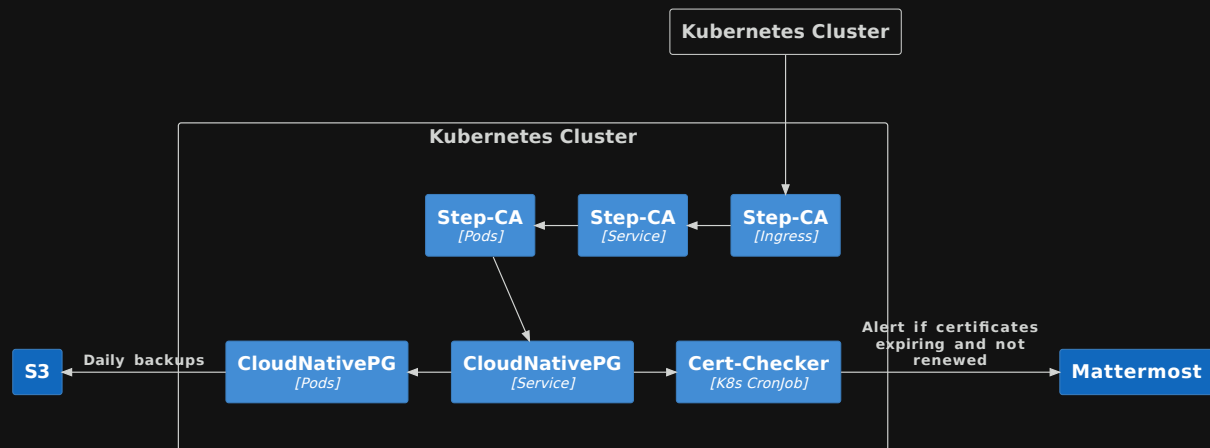
Smallstep

- Specialised Intermediate Certificate Authority to issue certificates
- Supports ACME protocol HTTP-01 challenge
- Templates to customise certificate fields for Subject Alternative Names
- Plays well with Cert-Manager
- No sensitive data stored in the database
- Certificate Authority signing key is encrypted at disk

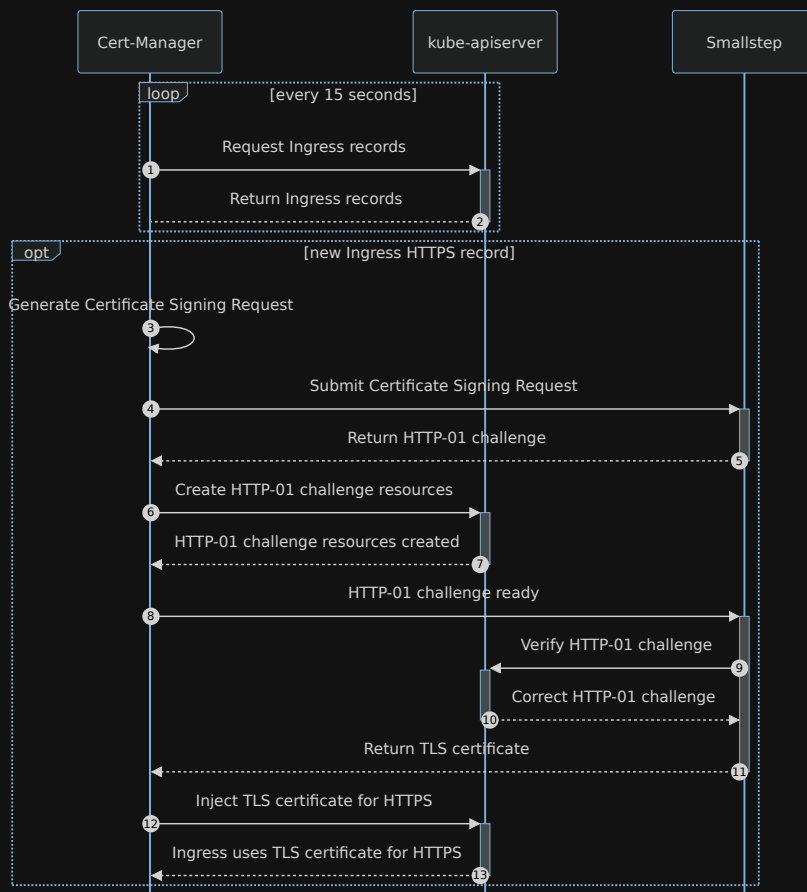
Certificate Lifetime

- Certificates should be short-lived
- Reduce ecosystem reliance on "broken" revocation checking solutions that cannot fail-closed
 - If revocation check response does not come back, the browser simply forgets about it
 - Chrome doesn't even do revocation checks
- 90-days validity follows best practices from Lets Encrypt and Google

Smallstep deployment



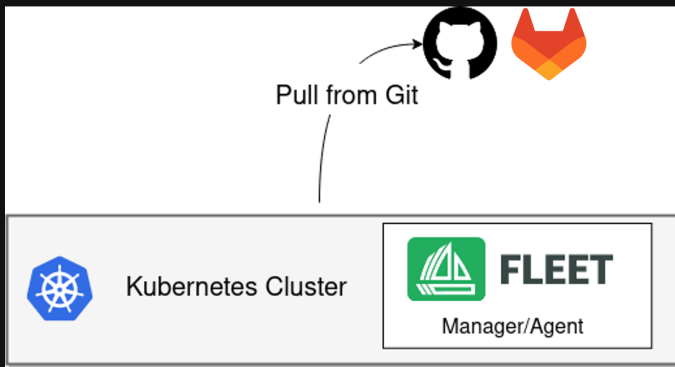
Automated TLS Certificate Creation





GitOps for Configuration Management at Scale

- Git as the single source of truth
- Pull-based approach — don't need to expose kubeconfig secrets
- Distributed initialisation system that makes it easy to customize applications and manage clusters from a single point



Thank you



Slides available at sachua.github.io/tgif-slides/