Don't *-k* your services on k8s

Our journey of rolling out TLS for microservices on our Kubernetes clusters

Akshay Chitneni
Tilottama Gaat
VMware

vmware® | ©2019 VMware, Inc.

whoami

Production Engineers

VMware CMBU

vRA Cloud - Provides single pane of glass for users to automate their workflows across environments

K8s 1.9 (1.5 - 1.13)

AWS EC2

40 microservices in Prod

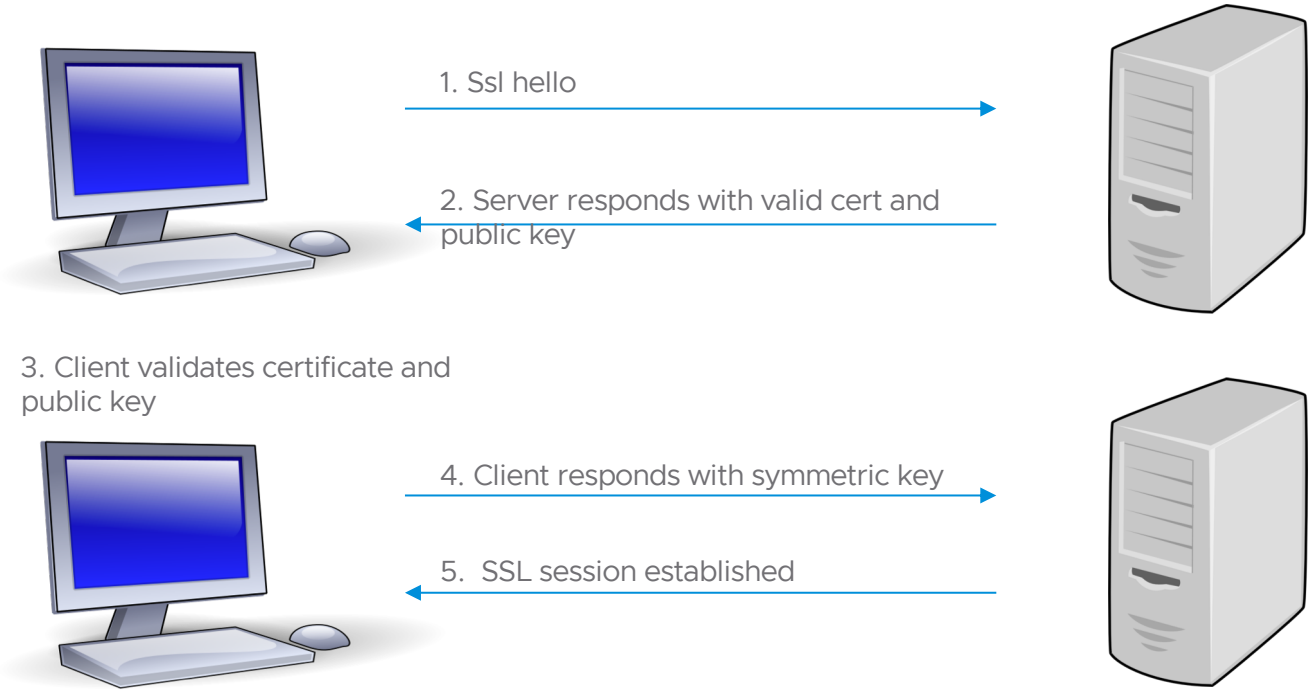
~700 pipeline runs in a day

300 dev/sre across 3 geos USA, Bulgaria, India



vmware | ©2019 VMware, Inc.

What is TLS?



vmware | ©2019 VMware, Inc.

What is TLS? Contd.

Identification:

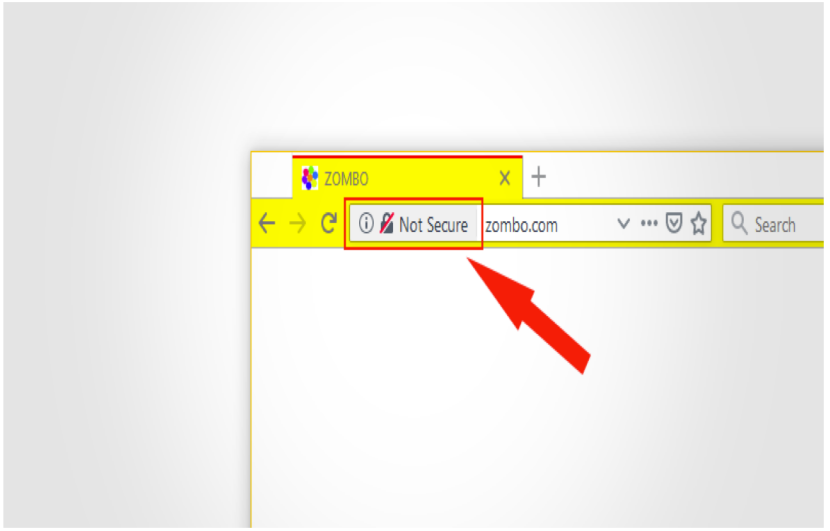
1. Company asks CA for root certificate

2. CA creates ROOT CA certificate and signs it

3. This Root CA will be installed in the webserver

4. Intermediate CA certificates used along with Root CA to create a chain of trust

5. Browser can now trust the certificates issued by the server



vmware | ©2019 VMware, Inc.

Kubernetes TLS challenges

Microservices –> more endpoints

Many environments

Custom Certificate Authorities and certificate signing processes.

Certificate Renewal is a calendar event.

vmware® | ©2019 VMware, Inc.

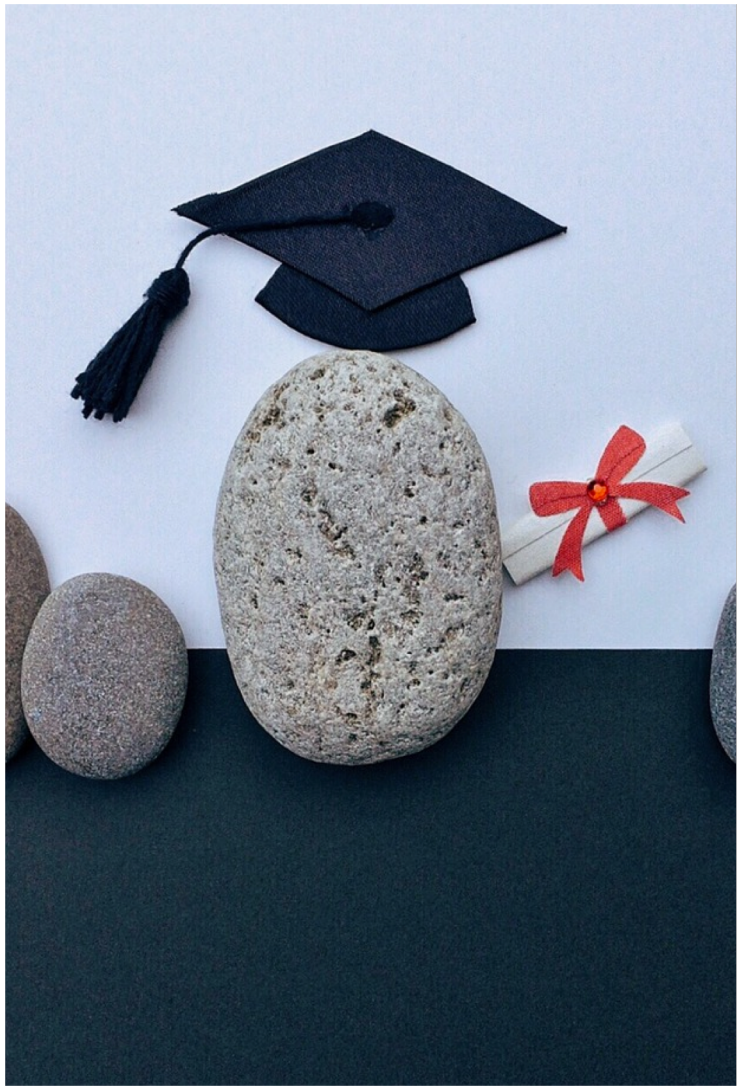
Problem statement 1.0

Encrypted communication between microservices using TLS

Distribute and Manage TLS certs

Applicable for service environments running in containers (k8s)

Highly available and fault tolerant



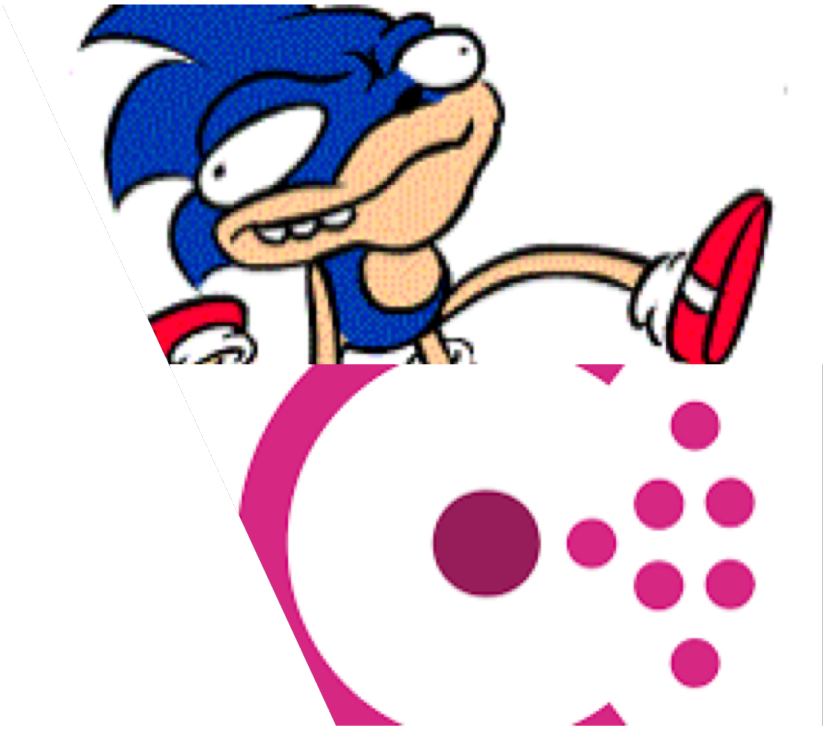
vmware | ©2019 VMware, Inc.

TLS Attempt 1.0



Provisioning Certificates 1.0

- **Diplomav1** - generates Certificates and CA certificates
- Uses Rest API (sanic)
- Vault and Consul

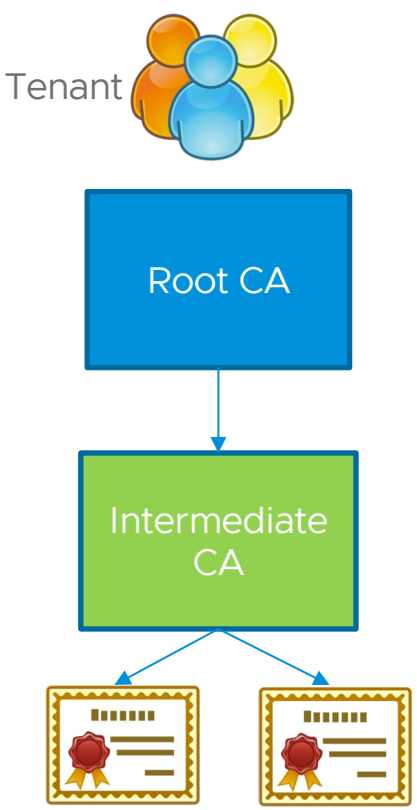


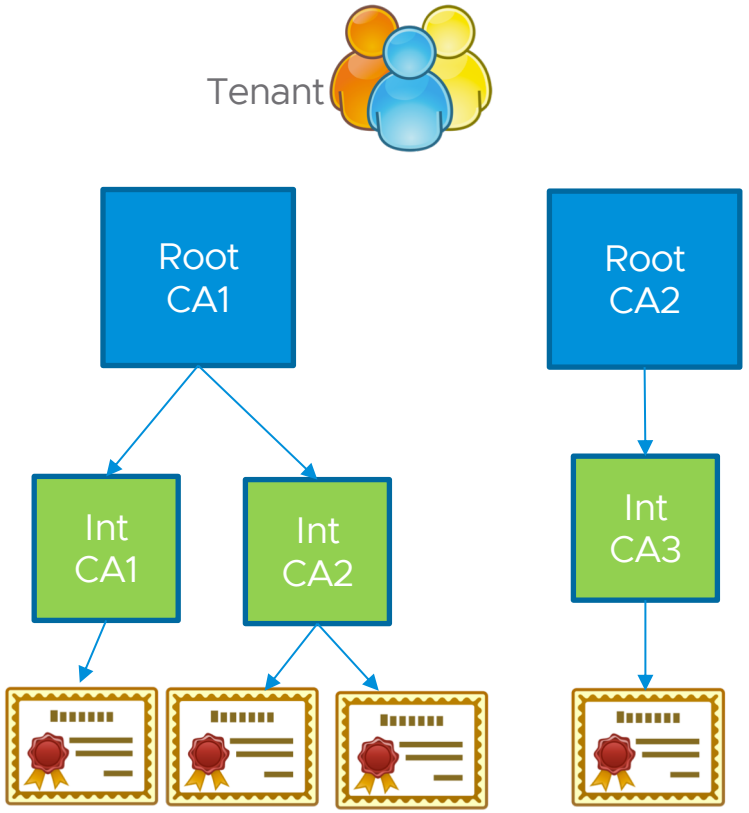
Distributing Certificates 1.0

- Deploy scripts of all services invoke diploma api

©2019 VMware, Inc.

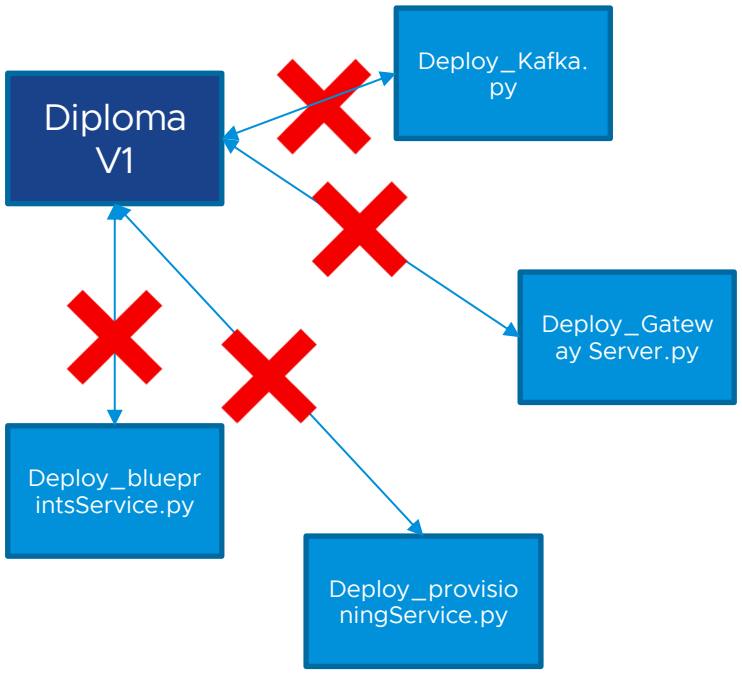
Diploma v1 vs Diplomav2

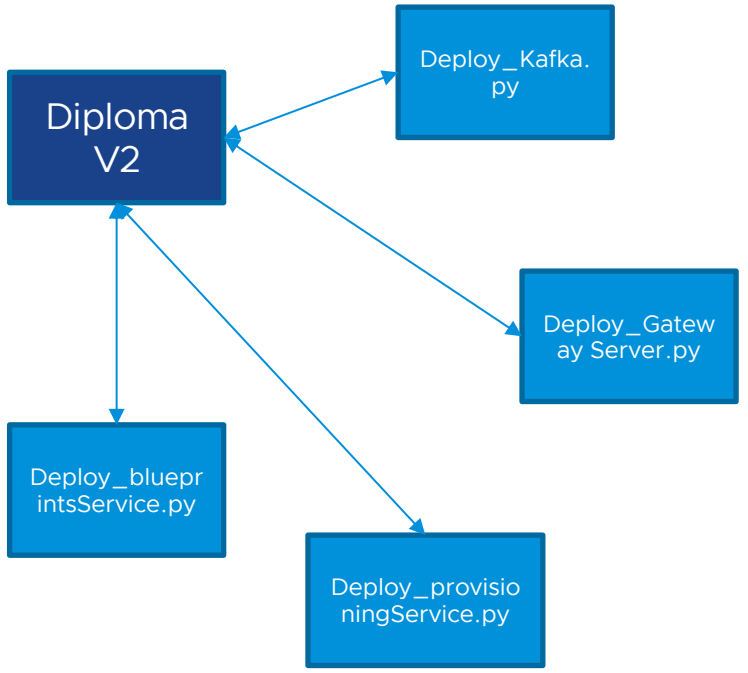




vmware | ©2019 VMware, Inc.

Migration to Diplomav2





vmware | ©2019 VMware, Inc.

Problems in Attempt 1.0

Provisioning Certificates 1.0 Problems

- Problems in diplomav1 design
- Not on k8s
- Want to move to diplomav2 but too many hurdles

Distributing Certificates 1.0 Problems

- Each service has deployment code touching diploma
- Want to move towards helm but cannot
- Renewing certs – onus on services



vmware | ©2019 VMware, Inc.

Problem statement 2.0

- Services will need to move to Diploma v2
  - New API for certs
  - Diff auth mechanism
- 40+ services in production
  - Multiple clusters
  - Multiple regions
  - Service specific Cert Config, varies per env
  - Service specific SLA, Release cycle
  - mtls
- Seamless migration without causing any downtime
- Minimal changes to existing deploy scripts.

vmware | ©2019 VMware, Inc.

Where to begin?

- Services use Diploma V1 API
  - Auth tokens
  - Certificate as Kubernetes secret
  - Jenkins jobs for certificate renewal

- Standardize
  - Service access to diploma
  - Auth tokens
  - Labels on secrets
  - Centralized CA config

vmware® | ©2019 VMware, Inc.

Chancellor

- K8s controller
- Watches deployments/statefulsets/daemonsets
- Cert config in the annotation
  - CA to use
  - Common name for cert

```
annotations:
    cert-request.diploma.vmware.com: '[{"caSecretName":"ops-kafka-ca","baseCommonName":"ops-ingest", }]'
```

- Retrieves Cert and creates k8s secret

vmware | ©2019 VMware, Inc.

Interfaces

- CA interface

```
apiVersion: v1
kind: Secret
data:
  ca0.email: xxxxx
  ca0.expirationTimeEpoch: xxx
  ca0.name: xxxxxxx
  ca0.root: xxxxxxx
  ca0.secret: xxxxxx
  ca0.token: xxxxxxx
```

- Secret Interface

```
apiVersion: v1
kind: Secret
data:
  chain.pem: xxxxx
  key.pem: xxxxx
  root0.pem: xxxxxx
```

vmware® | ©2019 VMware, Inc.

Migration

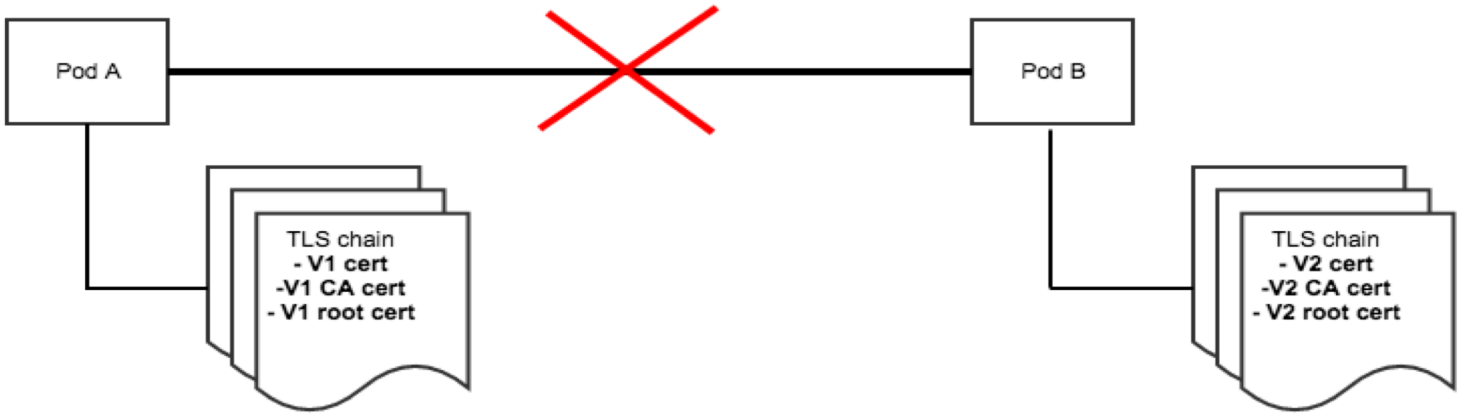
- Services need to use v2 CA

- Diploma V2
  - New Root CA
  - Not trusted by the services using v1 certs

vmware® | ©2019 VMware, Inc.

Migration

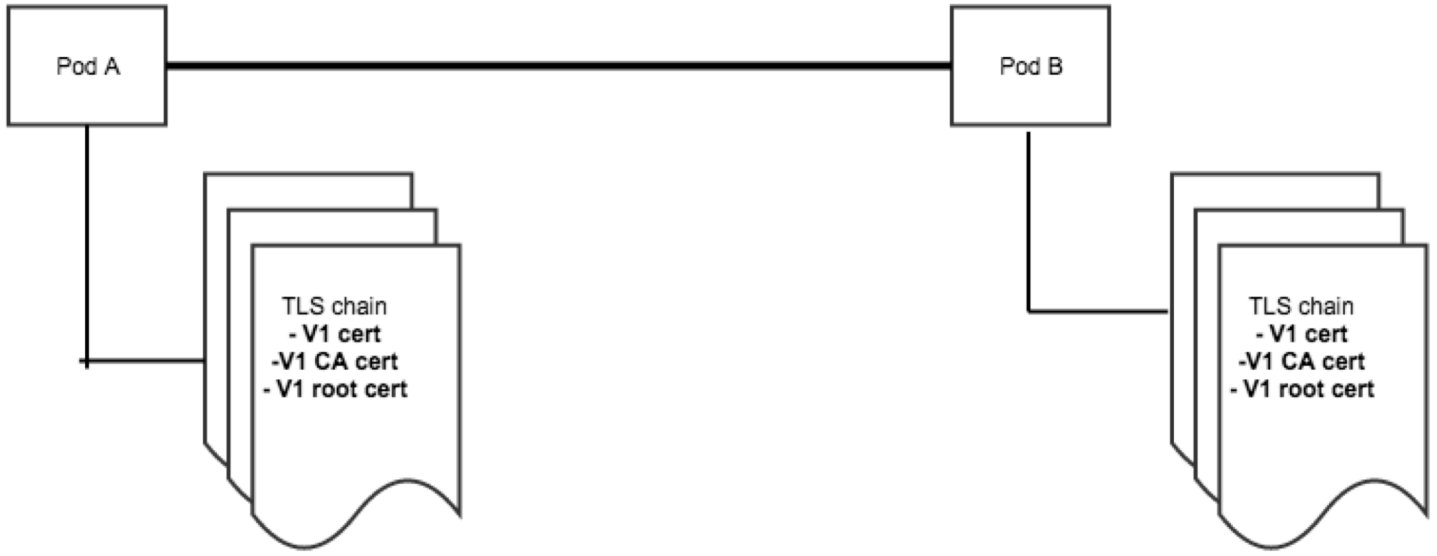
- Avoid bad state
  - Services on different CAs that are not trusted by each other.



vmware | ©2019 VMware, Inc.

Expand - Contract

- Onboard to use certs from chancellor
- Services still use V1 CA



vmware | ©2019 VMware, Inc.

Expand - Contract

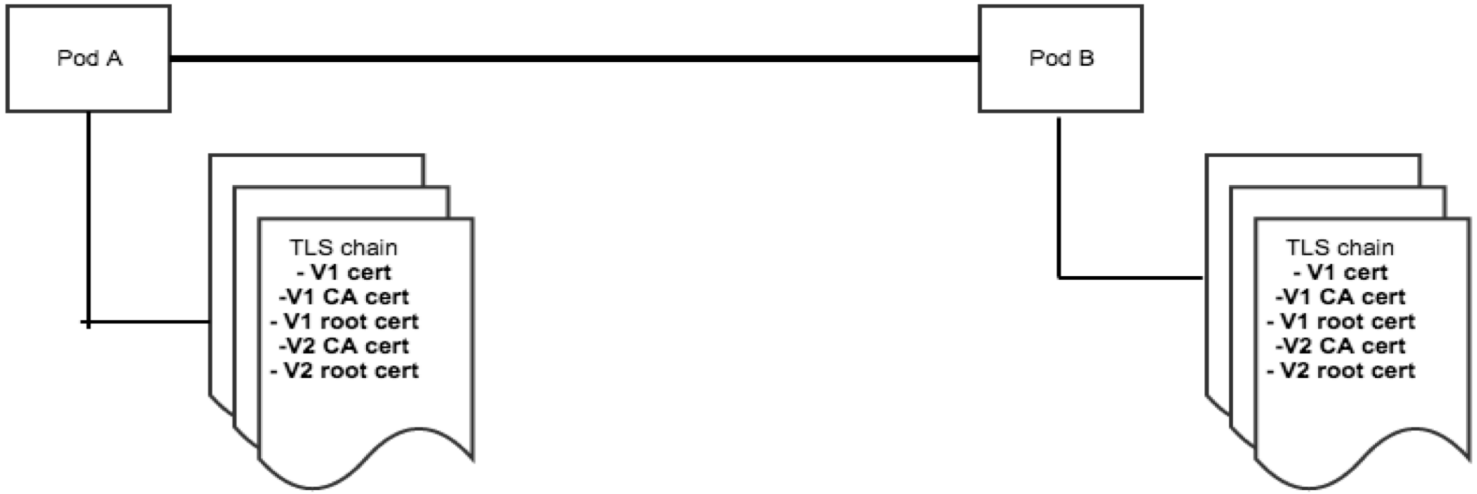
- Multiple CA config

```
apiVersion: v1
kind: Secret
data:
  ca0.email: xxxxx
  ca0.expirationTimeEpoch: xxx
  ca0.name: kafka-ca
  ca0.root: xxxxxxx
  ca0.secret: xxxxxx
  ca0.token: xxxxxxx
  ca1.email: xxxxx
  ca1.expirationTimeEpoch: xxx
  ca1.name: kafka-ca
  ca1.root: xxxxxxx
  ca1.token: xxxxxxx
```

vmware | ©2019 VMware, Inc.

Expand - Contract

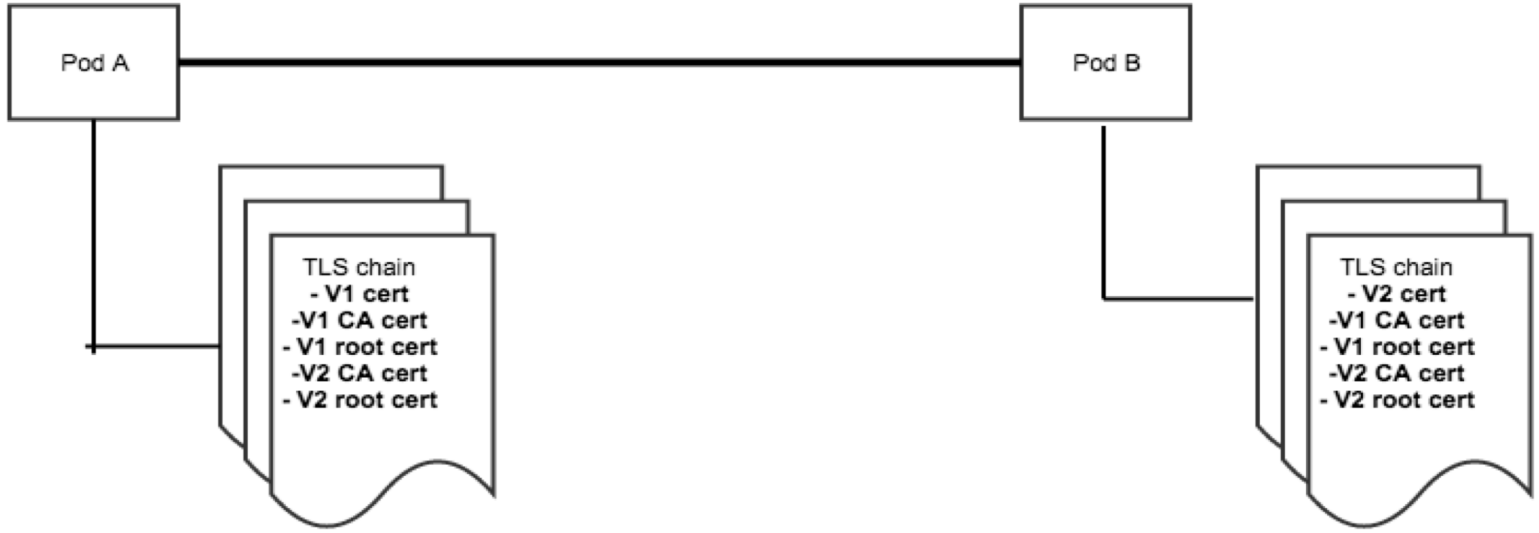
- Move all services to use expanded CA config



vmware | ©2019 VMware, Inc.

Expand - Contract

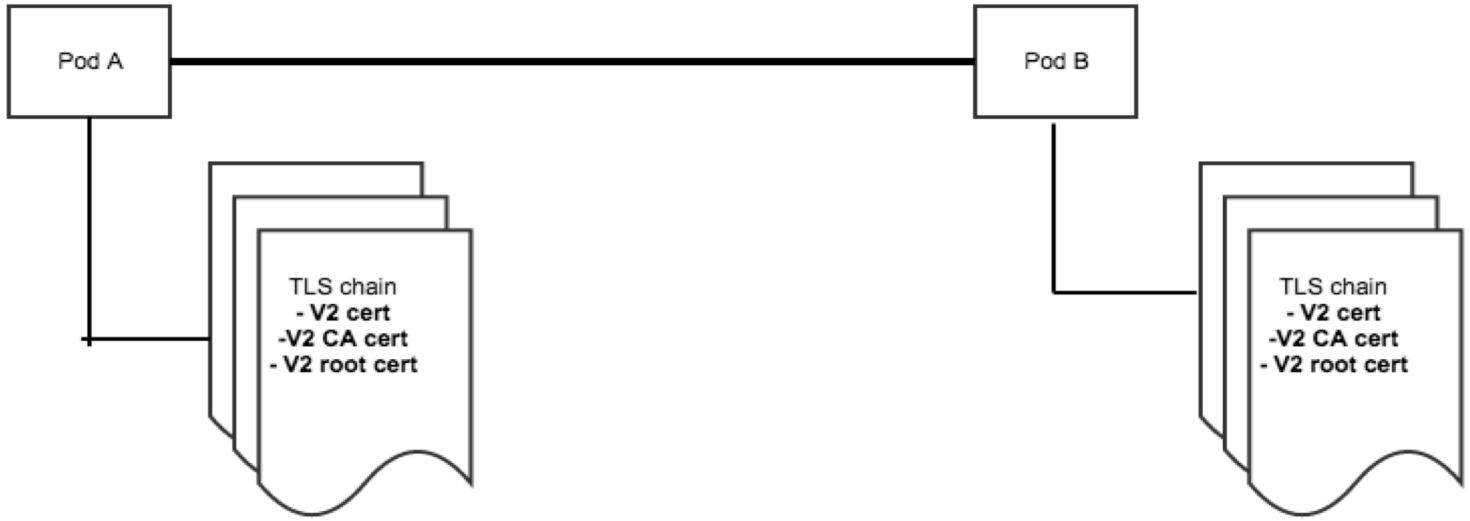
- Update CA config in chancellor to prioritize v2 CA over v1 CA for private cert generation.



vmware | ©2019 VMware, Inc.

Expand - Contract

- Delete v1 CA config in chancellor.



vmware | ©2019 VMware, Inc.

Other features

- Cert renewal
  - Better control to renew
- Debugging
  - K8s events on create/renew of certs
  - Observability metrics

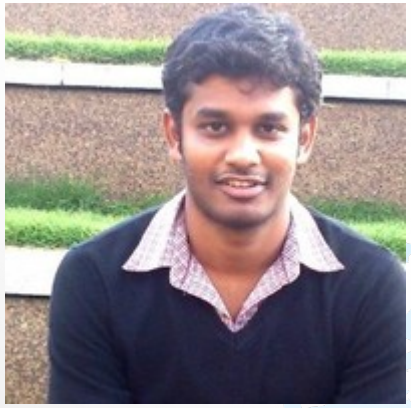
vmware® | ©2019 VMware, Inc.

Other Solutions

- Cert-Manager
  - Vault integration
  - Multiple CA support
- Istio
  - Sidecar approach
  - Service account based identity

vmware® | ©2019 VMware, Inc.

Thank you



Akshay Chitneni

https://www.linkedin.com/in/akshayadatta/

@akshayadatta



Tilottama Gaat

https://www.linkedin.com/in/tgaat/

vmware | ©2019 VMware, Inc.