CERT MANAGER

FREE SSL/TLS FOR KUBERNETES WITH CERT-MANAGER

WHAT IS CERT MANAGER

CERT-MANAGER IS A POWERFUL AND EXTENSIBLE X.509 CERTIFICATE CONTROLLER FOR KUBERNETES AND OPENSHIFT WORKLOADS. IT WILL OBTAIN CERTIFICATES FROM A VARIETY OF ISSUERS, BOTH POPULAR PUBLIC ISSUERS AS WELL AS PRIVATE ISSUERS, AND ENSURE THE CERTIFICATES ARE VALID AND UP-TO-DATE, AND WILL ATTEMPT TO RENEW CERTIFICATES AT A CONFIGURED TIME BEFORE EXPIRY.

- CNCF PROJECT
- ACCEPTED ON NOVEMBER 10, 2020
- ACCEPTED AS A CNCF **INCUBATING PROJECT** ON OCTOBER 19,2022
- IT PROVIDES A KUBERNETES ADD-ON TO AUTOMATICALLY PROVISION AND MANAGE TLS CERTIFICATES
- IS THE DE FACTO STANDARD FOR X.509 CERTIFICATES IN KUBERNETES ENVIRONMENTS

Notable Milestones:

- 9.4k GitHub Stars
- 2057 merged pull requests
- 2531 closed issues
- 300+ contributors
- 136 Releases
- 7k Slack members

WHY TO USE CERT MANAGER

CERTIFICATE ARE STORED IN SECRET WITHIN NAMESPACES AND ARE CONSUMED BY APPLICATION ON INGRESS COMPONENT

MANY PARAMETERS TO CONSIDER:

- THE NUMBER OF KUBERNETES CLUSTERS
- THE NUMBER OFF SSL/TLS CERTIFICATE IN A CLUSTER
- MANUALLY REPLACE EACH CERTIFICATE EACH TIME THE EXPIRE
  - HUMAN ERROR PRONE,
  - MISSING SOME CERTIFICATES, WHICH LEADS TO SYSTEM DOWNTIME
  - POSSIBILITY FOR CERTIFICATE LEAK, SECURITY ISSUES

MAIN CONCEPT

- **ISSUER**
- ACME ISSUER
- CERTIFICATE
- CERTIFICATE REQUEST
- ACME ORDERS AND CHALLENGES

- **ISSUERS/CLUSTERISSUERS:** ARE KUBERNETES RESOURCES THAT REPRESENT CERTIFICATE AUTHORITIES (CAS)
- CLUSTERISSUER IS CLUSTER SCOPED RESOURCE WHILE ISSUER IS A NAMESPACE SCOPE RESOURCE
- DIFFERENT ISSUERS:
  - BUILTIN:
    - SELFSIGNED, CA, VAULT, VENAFI, ACME
  - EXTERNAL: AMONG THEM
    - AWS-PRIVATECA-ISSUER: REQUESTS CERTIFICATES FROM ***AWS PRIVATE CERTIFICATE AUTHORITY FOR CLOUD NATIVE/HYBRID ENVIRONMENTS.***
    - GOOGLE-CAS-ISSUER: REQUESTS CERTIFICATES SIGNED BY ***PRIVATE CAS MANAGED BY THE GOOGLE CLOUD CERTIFICATE AUTHORITY SERVICE***

MAIN CONCEPT

- ISSUER
- **ACME ISSUER**
- CERTIFICATE
- CERTIFICATE REQUEST
- ACME ORDERS AND CHALLENGES

- ACME STANDS FOR: THE AUTOMATED CERTIFICATE MANAGEMENT ENVIRONMENT
- THE ACME ISSUER TYPE REPRESENTS A SINGLE ACCOUNT REGISTERED WITH ACME CERTIFICATE AUTHORITY SERVER. WHEN YOU CREATE A NEW ACME ISSUER, CERT-MANAGER WILL GENERATE A PRIVATE KEY WHICH IS USED TO IDENTIFY YOU WITH THE ACME SERVER.

```yaml
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: letsencrypt-staging
spec:
  acme:
    email: zoubir.ouarab@gmail.com
    server: https://acme-staging-v02.api.letsencrypt.org/directory
    privateKeySecretRef:
      name: letsencrypt-staging
    solvers:
    - http01:
        ingress:
          class: nginx
```

MAIN CONCEPT

- ISSUER
- ACME ISSUER
- **CERTIFICATE**
- CERTIFICATE REQUEST
- ACME ORDERS AND CHALLENGES

- A CERTIFICATE IS A NAMESPACED RESOURCE THAT REFERENCES AN ISSUER, AND IT IS INTENDED TO REPRESENT X.509 CERTIFICATE WHICH WILL BE RENEWED AND KEPT UP TO DATE. THE X.509 CERTIFICATE WILL BE STORED IN A KUBERNETES SECRET DEFINED IN THE CERTIFICATE RESOURCE.

```
6   apiVersion: cert-manager.io/v1
7   kind: Certificate
8   metadata:
9     name: myapp-secret-prod-tls
10    namespace: myapp-ns
11  spec:
12    secretName: myapp-secret-prod-tls
13    issuerRef:
14      name: letsencrypt-prod
15      kind: ClusterIssuer
16    commonName: nginx-service.ca
17    dnsNames:
18      - nginx-service.ca
```

MAIN CONCEPT

- ISSUER
- ACME ISSUER
- CERTIFICATE
- **CERTIFICATE REQUEST**
- ACME ORDERS AND CHALLENGES

- THE CERTIFICATEREQUEST IS A RESOURCE WITHIN A NAMESPACE IN CERT-MANAGER THAT IS USED TO REQUEST X.509 CERTIFICATES FROM AN ISSUER. THIS RESOURCE IS STRICTLY MANAGED BY THE CONTROLLERS

MAIN CONCEPT

- ISSUER
- ACME ISSUER
- CERTIFICATE
- CERTIFICATE REQUEST
- **ACME ORDERS AND CHALLENGES**

- FOR ACME CONFIGURATION ;
- CERT-MANAGER SHOULD SOLVE ACME CHALLENGES TO SUCCESSFULLY REQUEST A CERTIFICATE,
- ACME CHALLANGES ARE TO PROVE THAT THE CLIENT OWNS THE DNS ADDRESSES THAT ARE BEING REQUESTED.
- FOR THAT TWO CERTIFY MANAGER RESOURCE OF CUSTOMRESOURCE TYPES A RE CREATED: ORDERS AND CHALLENGES
- ORDER RESOURCE MAGES THE LIFECYCLE OF AN ACME ORDER AND IT IS A COLLECTION OF CHALLENGES
- CHALLENGES RESOURCES MANAGES THE LIFECYCLE OF ACME CHALLENGE
- TWO TYPE OF CHALLENGES SOLVER :
  - HTTP01
  - DNS01

CERT MANAGER MECHANISM

1. CERTIF MANAGER CHECKS IF A CERTIFICATE EXITS/VALIDE
2. IF NOT IT ISSUES A CERTIFICATE REQUEST
3. WHICH IN TURN ISSUES AN ORDER
4. WHICH, ALSO, ISSUES A ISSUER CHALLENGE(FOR LET'SENCRYPT IT EITHER A HTTP01OR DNS01 CHALLENGE)
5. WHEN THE CHALLENGE IS SUCCESSFUL THE ISSUER GENERATE A X.509 CERTIFICATE
6. THE CERTIF MANAGER STORE THE CERTIFICATE IN THE KUBERNETES SECRET USED BY INGRESS OR APPLICATION

Problem: GKE Autopilot does not allow modifications to the kube-system-namespace.

COMPATIBILITY ISSUE

- GKE AUTOPILOT MODE WITH KUBERNETES < 1.21
- **ISSUE:** GKE AUTOPILOT DOES NOT ALLOW MODIFICATIONS TO THE KUBE-SYSTEM-NAMESPACE
- THE NAMESPACE "KUBE-SYSTEM" IS MANAGED, AND CERT MANAGER CANNOT CREATE RESOURCE IN THAT NAMESPACE.
- SOLUTION : USE ANOTHER NAMESPACE FOR SOME CERT MANAGER OBJECTS

```
HELM INSTALL \
CERT-MANAGER JETSTACK/CERT-MANAGER \
--NAMESPACE CERT-MANAGER \
--CREATE-NAMESPACE \
--VERSION ${CERT_MANAGER_VERSION} \
--SET GLOBAL.LEADERELECTION.NAMESPACE=CERT-MANAGER
```

DEMO

GENERATE CERTIFICATE FOR A NGINX WEB SERVER APPLICATION USING CERT MANAGER AND LET'SENCRYPT

- GKE : V1.22.12-GKE.2300
- KUBECTL : V1.25
- HELM : V3.9.3
- LET'S ENCRYPT IS A FREE, AUTOMATED, AND OPEN CERTIFICATE AUTHORITY BROUGHT TO YOU BY THE NONPROFIT INTERNET SECURITY RESEARCH GROUP (ISRG)

QUESTION?

REFERENCES

HTTPS://CERT-MANAGER.IO/DOCS/

HTTPS://WWW.CNCF.IO/BLOG/2022/10/19/CERT-MANAGER-BECOMES-A-CNCF-INCUBATING-PROJECT/

HTTPS://LETSENCRYPT.ORG/HOW-IT-WORKS/