Custom Kyverno Configuration for Custom Kubernetes Certificates

---

1. Generate or Use CA-Signed Certificates

If you're using your organization's internal CA, you will need certificates for the following services:

- `kyverno-svc.kyverno.svc`
- `kyverno-cleanup-controller.kyverno.svc`

These certificates **must be signed by your internal CA**, not self-signed by Kyverno.

Note on Wildcard Certificates:

If you're using a wildcard certificate (e.g., `*.rancher-odc-poc.test.intranet`), ensure the Subject Alternative Names (SANs) include:

- `kyverno-svc.kyverno.svc`
- `kyverno-cleanup-controller.kyverno.svc`

This ensures the Kubernetes API server trusts and connects over TLS with the webhook servers correctly.

---

2. Verify Subject Alternative Names (SANs)

Ensure that the following SANs are present in your certificates **before** creating secrets:

For kyverno-svc:

- `kyverno-svc`
- `kyverno-svc.kyverno`
- `kyverno-svc.kyverno.svc`

For kyverno-cleanup-controller:

- `kyverno-cleanup-controller`
- `kyverno-cleanup-controller.kyverno`
- `kyverno-cleanup-controller.kyverno.svc`

To verify the SANs and inspect your certificates, you can use the **Step CLI tool**. For more information on the tool and how to use it, refer to the official documentation here: [Step CLI Documentation]

Unset

```
step certificate inspect your-admission-cert.crt --short
```

---

3. Create Kubernetes Secrets for Your Certificates

Use the following commands to create the required secrets in the Kyverno namespace (replace `<namespace>` appropriately):

Admission Controller Secrets

Unset

```
# Certificate and key pair
kubectl create secret tls
kyverno-svc.kyverno.svc.kyverno-tls-pair \
  --cert=your-admission-cert.crt \
  --key=your-admission-key.key \
  -n <namespace>

# CA certificate
kubectl create secret generic
kyverno-svc.kyverno.svc.kyverno-tls-ca \
  --from-file=rootCA.crt=your-ca.crt \
  -n <namespace>
```

Cleanup Controller Secrets

Unset

```
# Certificate and key pair
kubectl create secret tls
kyverno-cleanup-controller.kyverno.svc.kyverno-tls-pair \
  --cert=your-cleanup-cert.crt \
  --key=your-cleanup-key.key \
  -n <namespace>

# CA certificate
kubectl create secret generic
kyverno-cleanup-controller.kyverno.svc.kyverno-tls-ca \
  --from-file=rootCA.crt=your-ca.crt \
  -n <namespace>
```

Important: Do not rename these secrets. Kyverno expects these exact secret names.

4. Reference

For additional details, refer to the official Kyverno documentation:
https://kyverno.io/docs/installation/customization/#custom-certificates