AVI Networks®

Default Secret for TLS Routes

Avi Technical Reference (v21.1)

Default Secret for TLS Routes

view online

Overview

By default, AKO expects all routes with TLS termination to have key and cert to be specified in the route spec. Sometimes, users may want to apply a common key-cert for multiple routes.

To handle such use cases, AKO supports TLS routes without key/cert specified in the route spec.

Starting with AKO version 1.3.1, you can apply a common key-cert value for multiple routes using the default secret for TLS routes. For example, a wild card secret can be used for all host names in the same subdomain.

Using a Wild Card Secret

In such a scenario, a common key-cert value can be specified in a secret that can be used for TLS routes that do not have a key-cert value specified in the route spec.

To use the wild card secret,

1. Create a secret with name `router-certs-default` in the same namespace where the AKO pod is running (avi-system). Ensure that the secret has a `tls.crt` and `tls.key` fields in its data section.

   An example of the default secret is given below:

   ```
   apiVersion: v1
   kind: Secret
   metadata:
     name: router-certs-default
     namespace: avi-system
   type: kubernetes.io/tls
   data:
     tls.crt:
       -----BEGIN PRIVATE KEY-----
       [...]
       -----END PRIVATE KEY-----
     tls.key:
       -----BEGIN CERTIFICATE-----
       [...]
       -----END CERTIFICATE-----
   ```

2. After creating the secret, we can add a secure route without without key or cert in the spec.

   For example,

   ```
   apiVersion: v1
   kind: Route
   metadata:
   ```

```
  name: secure-route-no-cert
spec:
  host: secure-no-cert.avi.internal
  to:
    kind: Service
    name: avisvc
  tls:
    termination: edge
```

AKO uses the default secret to fetch the key and cert values for processing all such routes.

Notes: * For TLS routes with termination type re-encrypt, the value of the destination CA has to be specified in the route spec itself. * The CA certificate can not be specified as a part of the default secret. * The field`router-certs-default` present in the OpenShift-ingress namespace is not used by AKO. Create `router-certs-default` in the avi-system namespace.

Document Revision History

Date	Change Summary
December 18, 2020	Published the article for Default Secret for TLS Routes