SSL

The CA certificate bundle is automatically mounted into pods using the default service account at the path

/var/run/secrets/kubernetes.io/serviceaccount/ca.crt

Test Commands

> curl -vs --user test:testpw https://registry:5000/v2/_catalog

```
*   Trying 10.100.117.234...
* TCP_NODELAY set
* Connected to registry (10.100.117.234) port 5000 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS alert, Server hello (2):
* SSL certificate problem: unable to get local issuer certificate
* stopped the pause stream!
* Closing connection 0
```

> curl -vs --cacert /var/run/secrets/kubernetes.io/serviceaccount/ca.crt --user test:testpw https://registry:5000/v2/_catalog

```
*   Trying 10.100.117.234...
* TCP_NODELAY set
* Connected to registry (10.100.117.234) port 5000 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
  CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-ECDSA-AES128-GCM-SHA256
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=registry
*  start date: Apr 11 14:17:00 2019 GMT
*  expire date: Apr 10 14:17:00 2020 GMT
*  common name: registry (matched)
*  issuer: CN=kubernetes
*  SSL certificate verify ok.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* Server auth using Basic with user 'test'
* Using Stream ID: 1 (easy handle 0x55f9ad4398e0)
> GET /v2/_catalog HTTP/2
> Host: registry:5000
> Authorization: Basic dGVzdDp0ZXN0cHc=
> User-Agent: curl/7.58.0
> Accept: */*
>
* Connection state changed (MAX_CONCURRENT_STREAMS updated)!
< HTTP/2 200
< content-type: application/json; charset=utf-8
< docker-distribution-api-version: registry/2.0
< x-content-type-options: nosniff
< content-length: 34
< date: Thu, 11 Apr 2019 20:37:58 GMT
<
{"repositories":["nginx-jmehan"]}
* Connection #0 to host registry left intact
```

> echo | openssl s_client -connect registry:5000

```
depth=0 CN = registry
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = registry
verify error:num=21:unable to verify the first certificate
verify return:1
CONNECTED(00000003)
---
Certificate chain
 0 s:/CN=registry
   i:/CN=kubernetes
---
Server certificate
```

```
-----BEGIN CERTIFICATE-----
MIICPzCCASegAwIBAgIUZinreoUbOAubSHgg2SVHvSDSO9wwDQYJKoZIhvcNAQEL
BQAwFTETMBEGA1UEAxMKa3ViZXJuZXRlczAeFw0xOTA0MTExNDE3MDBaFw0yMDA0
MTAxNDE3MDBaMBMxETAPBgNVBAMTCHJlZ2lzdHJ5MFkwEwYHKoZIzj0CAQYIKoZI
zj0DAQcDQgAEepRoRVRGluazfPpwRT5dFs7oaB8LYQGd7wBxyQ84K6DFz4CuQVBf
3Sdz2pqnDfcNdpFQQpF+KdFSwWtQmGHZt6NUMFIwDgYDVR0PAQH/BAQDAgWgMBMG
DONE
A1UdJQQMMAoGCCsGAQUFBwMBMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFCfZjNms
NGcH6UTuzOUltNWsBbyKMA0GCSqGSIb3DQEBCwUAA4IBAQArMnn6eLiS/ZUwtLZg
s8LvHqe5OVJ2w+xDLaP6XwpY9F8yX8Cgzw+3haBPNObBB3KX9J79gFpgOsY0VVyC
iGjjEJ2sgyJ70GqdFsPaIIKpIIJqY/1xbz5IrHdouP6zcceaGwZVJjV7KRTK/T5a
ZR4tBn1ulawtswU4FS5J4KiBvphoqcvLB78bmxzTkz2fJ7fKlQCSC6CdgTazMyOy
VSE9o3wLPFpPojFBCKS27YU9t5Ctk8LHAboshBFOxQZfftSiVFAO/hZmhMZjg6EH
DjHCeYb7xGw51iHenmFw4q+xjvygE1gkBxlMOjSYIVwY3nxibd0e03MKsROY6m2o
hTc8
-----END CERTIFICATE-----
subject=/CN=registry
issuer=/CN=kubernetes
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 968 bytes and written 269 bytes
Verification error: unable to verify the first certificate
---
New, TLSv1.2, Cipher is ECDHE-ECDSA-AES128-GCM-SHA256
Server public key is 256 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-ECDSA-AES128-GCM-SHA256
    Session-ID: 397AD3D2AC801DC06FA5C51D94D9A21E4601DDA9C4EF1A7721E22F8A7F4FE0F4
    Session-ID-ctx:
    Master-Key: 76AD7A659F8A7C20371D33F57220ABC88AB241AF98D7383573DAF2B7D385EDE11A2166FEAA5945C8757C
0A9692944204
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket:
    0000 - ec 6d dd 31 99 d5 88 0c-57 bf d3 8a 54 30 f4 3b   .m.1....W...T0.;
    0010 - 23 07 a4 5a 03 29 6a 4f-bd 10 22 05 51 92 67 62   #..Z.)jO.."Q.gb
    0020 - db 8c 20 fc 8f 98 10 27-24 b3 f5 19 35 24 40 cb   .. ....'$...5$@.
    0030 - 4b 2a 04 1d 65 33 67 04-15 fa 47 70 bf 53 2c 39   K*..e3g...Gp.S,9
    0040 - 2f cb e0 2c d3 8a 3e 24-e3 c5 85 a8 3a 9b 57 b2   /..,..>$....:.W.
    0050 - e6 2e 6b 59 56 cd 9a ae-ca 38 f5 cc ab c2 e4 42   ..kYV....8.....B
    0060 - eb e4 1f 77 93 3a de 92-49 e6 ae 70 20 33 93 2a   ...w.:..I..p 3.*
    0070 - 16 eb b5 45 6c 1c 1f 2c-                          ...El..,

    Start Time: 1555013937
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
    Extended master secret: no
---
```

References

Reference	URL
Kiam	https://github.com/uswitch/kiam/blob/master/docs/TLS.md
Kiam Helm Chart	https://github.com/helm/charts/tree/master/stable/kiam

Istio service mesh	https://istio.io/