TLS Transport Support

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF supports HTTP2 over a TLS secure channel for all SBA interfaces towards NRF, NSSF, AUSF, UDM, PCF, SMF, and so on.

This feature supports the server and client certificate management. It stores the certificates as k8 secrets.

Note You must generate and configure ca-certificates, and certificates for the server and client.

Feature Configuration

Configuring this feature involves the following steps:

- Client Certificates Configuration—This configuration provides the commands to configure the client certificates. For more information, refer to Configuring the Client Certificates, on page 2.
- Server Certificates configuration—This configuration provides the commands to configure the server certificates. For more information, refer to Configuring the Server Certificates, on page 2.
- TLS Enable Configuration—This configuration enables the TLS. For more information, refer to Enabling the TLS, on page 3.

Configuring the Client Certificates

To configure the Client certificates, use the following configuration:

```
config
   nf-tls ca-certificates certificate_name
      cert-data certificate_data
      end
```

NOTES:

- **ca-certificates** *certificate_name*—Specify the certificate name and data.
- **cert-data** *certificate_data*—Specify the certificate data in PEM format.

Configuring the Server Certificates

To configure the Server certificates, use the following configuration:

```
config
   nf-tls certificates certificate_name
      cert-data certificate_data
      private-key private_key_data
      end
```

NOTES:

- **nf-tls certificates** *certificate_name*—Specify the certificate name, data, and key.
- **cert-data** *certificate_data*—Specify the certificate data in PEM format.
- **private-key** *private_key_data*—Specify the certificate private key in PEM format.

Enabling the TLS

To configure the TLS enable, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint sbi
         uri-scheme { http | https }
         certificate-name certificate_name
         end
```

NOTES:

- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint sbi**—Specify the endpoint as sbi.
- **uri-scheme { http | https }**—Specify the uri scheme either http or https.
- **certificate-name** *certificate_name*—Specify the certificate name.

Configuration Verification

To verify the configuration:

```
show running-config instance instance-id 1 endpoint
instance instance-id 1
endpoint sbi
replicas     2
loopbackPort 8091
instancetype IPv4
vip-ip 209.165.200.224 vip-port 1000
exit
endpoint sctp
replicas 2
nodes    2
vip-ipv6 1000:1003::10:100 vip-ipv6-port 1001
exit
endpoint nodemgr
replicas 1
```

```
show nf-tls certificate-status days
CERTIFICATE NAME POD INSTANCE DAYS
-------------------------------------------
octrel-amf-server amf-amf-rest-ep-0 3632
octrel-lfs-server amf-amf-rest-ep-0 3632
```

Troubleshooting Information

This section describes troubleshooting information for this feature.

Trouble Ticket Data Collection

To debug the content data collection issues, use the following commands.

If the commands don’t assist you in resolving the issue, analyze the diagnostic data that is available in the form of logs.

- **helm list -n** *namespace*
- **kubectl get pods -n** *namespace*
- **kubectl get pod -o yaml -n** *namespace*
- **kubectl get pod -o yaml -n** *namespace pod_name*