Niagara MQTT Technical Notes

TLS Security - Mosquitto Broker Configuration

This wiki is a guide to setup TLS/SSL communication between the Mosquitto Broker (MQTT broker) and the Niagara MQTT client.

Client Requirements

- Client certificate (signed by the CA) is used to sign the server or the broker (Mosquitto) certificate.

Broker Requirements

- CA Certificate
- Server or the broker certificate
- Server or the broker private key for decryption

Create the private key, CA certificate, server certificate and the client certificate using the openssl tool as follows. For details, see Mosquitto TLS configuration.

Step 1: Use the below command to create a Key pair for CA.

- **Command:** openssl genrsa -des3 -out ca.key 2048

Step 2: Use the below command to create a certificate for the CA using the CA key.

- **Command:** openssl req -new -x509 -days 1826 -key ca.key -out ca.crt

Step 3: Use the below command to create a server key pair for the broker.

- **Command:** openssl genrsa -out server.key 2048

Step 4: Use the below command to create a certificate request .csr.

- **Command:** openssl req -new -out server.csr -key server.key

When filling out the form the common name is important and is usually the domain name of the server. In our testing environment we had Windows machines on an isolated network, we used Windows name (Host Name) for the computer that is running the Mosquitto broker.

Step 5: Use the CA key to verify and sign the server certificate. This will create the server.crt file.

- **Command:** openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 360

Step 6: Configure the certificates in the broker.

- Create a folder under the mosquitto folder (ex. /certs/).
- Copy the files ca.crt, serever.crt and the server.key to the added folder.
- Edit the mosquitto.conf file as given below:

```
cafile c:\mosquitto\certs\ca.crt
keyfile c:\mosquitto\certs\server.key
certfile c:\mosquitto\certs\server.crt
tls_version tlsv1
```

- In the bind_address configuration, make sure you either configure the specific hostnames or ip address of the client, or comment it as shown below. Broker will accept connections only from the specified bind_address, if it is not commented/removed.

```
# ================================================================
# Default listener
# ================================================================

# IP address/hostname to bind the default listener to. If not
# given, the default listener will not be bound to a specific
# address and so will be accessible to all network interfaces.
# bind_address ip-address/host name
# bind_address 127.0.0.1


# Port to use for the default listener.
port 8883
```

Step 7: Configure the Client. For details, see Abstract MQTT Driver Guide.

- Make sure that you accept the host in your certificate manger. The certificate pops up automatically in the **Host Name** tab during the initial configuration of client . Client can establish a connection with the browser, if the host is accepted or approved.

Mosquitto Broker Configuration

- The default max_inflight_messages count for mosquitto broker is 20. If the incoming and outgoing messages are larger than default numbers, update the messages count as per the requirement. The maximun limit of the max_inflight_messages count is 65000.
- The default max_queued_messages for mosquitto broker is 100. If you have client configured with the more number of messages with QoS 1 or 2, change the configuration as per the broker recommendations.