MQTT Distributor Access Control Lists

Abstract

Access Control Lists (ACLs) control what topics a given username/password pair is allowed to publish and subscribe on. ACLs should be designed with a 'principal of least privilege' model while also considering device management and maintenance. For example gateways and devices in the field should be limited to publishing and subscribing only on the topics for which they should be expected to. The same should be true of 'consumer' applications that will be either sending commands to devices in the field or consuming data coming from those devices.

It is important to note that a username is not limited to a single MQTT client. You will need to create separate users for each publishing and/or subscribing client, such as MQTT Transmission and MQTT Engine, if each one has a different Read/Write requirement.

If you are new to MQTT topics, the Eclipse Foundation's Paho project provides good information here on the basics of wildcards.

For subscriptions, two wildcard characters are supported:

- A '#' character represents a complete sub-tree of the hierarchy and thus must be the last character in a subscription topic string, such as SENSOR/#. This will match any topic starting with SENSOR/, such as SENSOR/1/TEMP and SENSOR/2/HUMIDITY.
- A '+' character represents a single level of the hierarchy and is used between delimiters. For example, SENSOR/+/TEMP will match SENSOR/1/TEMP and SENSOR/2/TEMP.

Definition

ACLs are defined by the following format: ***[R|W|RW] topic*** where:

R = Read or 'subscribe' privileges

W = Write or 'publish' privileges

RW = Read and Write (subscribe and publish) privileges

topic = The topic or wildcard topic representing the scope of the privilege

RW #

- This allows clients connecting using this username/password to publish and subscribe on any topic

R #

- This allows clients connecting using this username/password to subscribe on any topic but not publish on any topics

W #

- This allows clients connecting using this username/password to publish on any topic but not subscribe on any topics

ACLs are case sensitive. This means that setting a users ACL to *R spbv1.0* will **not** allow a user to subscribe to *spBv1.0/#* topics

Examples for MQTT Transmission ACLs

W spBv1.0/GroupID/+/EdgeNodeID/#

- This allows clients connecting using this username/password to publish on spBv1.0/GroupID/+/EdgeNodeID/# topic

R STATE/PrimaryHostID, R spBv1.0/STATE/PrimaryHostID, R spBv1.0/GroupID/#

- This allows clients connecting using this username/password to subscribe on both the legacy Sparkplug STATE, Sparkplug STATE and spBv1.0/GroupID# topics

W device_one/temp/#, R state/#

- This allows clients connecting using this username/password to publish on device_one/temp/# and subscribe on legacy STATE topics

When creating an Access Control List (ACL) for an MQTT Transmission client:

- There must be R privilege's for the Sparkplug NCMD message
  - This is used by MQTT Transmission to subscribe to the Sparkplug Rebirth request
- There must be R privilege's for the Sparkplug NDEATH message
  - This is used by MQTT Transmission to subscribe to its own STATE message

Examples For MQTT Engine ACLs

RW spBv1.0/GroupID/+/EdgeNodeID/#, RW spBv1.0/STATE/PrimaryHostID

- This allows Engine clients connecting using this username/password to subscribe and publish on the Sparkplug STATE and spBv1.0/GroupID/+/EdgeNodeID/# topics

RW STATE/PrimaryHostID, RW spBv1.0/STATE/PrimaryHostID, R spBv1.0/GroupID/#

- This allows clients connecting using this username/password to subscribe on both the legacy Sparkplug STATE and Sparkplug STATE topics and subscribe on the spBv1.0/GroupID/# topic

RW spBv1.0/STATE/PrimaryHostID, W spBv1.0/GroupID/NCMD/#, R spBv1.0/GroupID/#

- This allows clients connecting using this username/password to subscribe on both the Sparkplug STATE and spBv1.0/GroupID/# topics and publish on the spBv1.0/GroupID/NCMD/#

When creating an Access Control List (ACL) for an MQTT Engine client:

- There must be RW privilege's for the MQTT Sparkplug™ B STATE message
  - Sparkplug v3.0.0 state message topic: spBv1.0/STATE/primary_host_id
  - Legacy Sparkplug state message topic: STATE/PrimaryHostID
  - Review Changes to the STATE message in the Sparkplug v3.0.0 Specification for details on the legacy STATE client topic
- There must be W privilege's for the Sparkplug NCMD message
  - This is used by MQTT Engine to publish the Sparkplug Rebirth request
- The MQTT Engine SparkplugB Namespace Filter must be configured for the same Group or Group/EdgeNode combination used in the ACL entry

Client Connection Issues

Subscribe on topic not allowed by the ACL

If MQTT Engine or MQTT Transmission client attempts to subscribe on a topic that is not allowed by the ACL for that client, the connection will fail and the client will not attempt to reconnect.

With the following ACL, the Transmission client is not able to subscribe to the NCMD and DCMD topics

```
R spBv1.0/My MQTT Group/NDEATH/PLC 1, W #
```

E	TransmissionClient	17Apr2024 15:45:45	Failed to subscribe to TARGET elements +
W	PacketHandler	17Apr2024 15:45:45	SUBSCRIBE - [00ec923c-7d33-4180-a2f8-0f8f5ed726e1, MT-18ac06d8-60c1-44a8, /127.0.0.1] Failed: Not authorized for username admin on topic 'spBv1.0/My MQTT Group/DCMD/PLC 1/#' with QoS 0
W	PacketHandler	17Apr2024 15:45:45	SUBSCRIBE - [00ec923c-7d33-4180-a2f8-0f8f5ed726e1, MT-18ac06d8-60c1-44a8, /127.0.0.1] Failed: Not authorized for username admin on topic 'spBv1.0/My MQTT Group/NCMD/PLC 1' with QoS 0
I	PacketHandler	17Apr2024 15:45:45	SUBSCRIBE - [00ec923c-7d33-4180-a2f8-0f8f5ed726e1, MT-18ac06d8-60c1-44a8, /127.0.0.1] on topic(s) [[spBv1.0/My MQTT Group/NCMD/PLC 1][0], [spBv1.0/My MQTT Group/DCMD/PLC 1/#][0], [spBv1.0/My MQTT Group/NDEATH/PLC 1][0]]
I	TransmissionClient	17Apr2024 15:45:45	[My MQTT Group/PLC 1][MT-18ac06d8-60c1-44a8] Connected to the MQTT Server
I	TransmissionMqttCallback	17Apr2024 15:45:44	Connect complete for to tcp://localhost:1883 for MT-18ac06d8-60c1-44a8 - waiting for transition to online based on primary host status
I	TahuClient	17Apr2024 15:45:44	MT-18ac06d8-60c1-44a8: Connected to tcp://localhost:1883
I	TahuClient	17Apr2024 15:45:44	MT-18ac06d8-60c1-44a8: connect succeeded

Publish on a topic not allowed by the ACL

If MQTT Engine or MQTT Transmission client attempts to publish on a topic that is not allowed by the ACL for that client, the connection will be forcefully closed and the client will attempt to reconnect.

With the following ACL, the Transmission client can publish the NBIRTH for PLC 1 but is not able to publish the DBIRTH for edge node device D1

```
R #, W spBv1.0/My MQTT Group/+/PLC 1
```

			ent=null, metaData=null, properties=null, value=219, isNull=false]], seq=null, uuid=null, body=null]
E	TransmissionMqttCallback	17Apr2024 13:44:26	Connection lost +
W	TransmissionMqttCallback	17Apr2024 13:44:26	MQTT connection lost for MT-01f6c22a-76e7-436c
W	PacketHandler	17Apr2024 13:44:26	PUBLISH - Failed authorization [client ID: MT-01f6c22a-76e7-436c, username: admin, topic: spBv1.0/My MQTT Group/DBIRTH/PLC 1/D1]
I	DefaultConnectionListener	17Apr2024 13:44:26	Forcefully closing SocketChannel for 719dee55-8977-40cc-8472-3af22e49e3b1
I	TransmissionClient	17Apr2024 13:44:26	History flush (in-order) completed successfully for My MQTT Group/PLC 1
D	SparkplugPayloadHandler	17Apr2024 13:44:26	Got Sparkplug message: spBv1.0/My MQTT Group/NBIRTH/PLC 1
T	SparkplugPayloadHandler	17Apr2024 13:44:26	On topic=spBv1.0/My MQTT Group/NBIRTH/PLC 1: Incoming payload: SparkplugBPayload [timestamp=1713379464882, metrics=[Metric [name=Node Control/Next Server, alias=null, timestamp=1713379464882, dataType=Boolean, isHistorical=null, isTransient=null, metaData=null, properties=null, value=false, isNull=false], Metric [name=Node Info/Transmission Version, alias=null, timestamp=1713379464882, dataType=String, isHistorical=null, isTransient=null, metaData=null, properties=null, value=4.0.21 (b2024012622), isNull=false], Metric [name=Node Control/Rebirth, alias=null, timestamp=1713379464882, dataType=Boolean, isHistorical=null, isTransient=null, metaData=null, properties=null, value=false, isNull=false], Metric [name=bdSeq, alias=null, timestamp=1713379466885, dataType=Int64, isHistorical=null, isTransient=null, metaData=null, properties=null, value=219, isNull=false]], seq=0, uuid=null, body=null]
I	TransmissionClient	17Apr2024 13:44:26	Bringing My MQTT Group/PLC 1 online with CACHED history store Birth certs
I	TransmissionClient	17Apr2024 13:44:26	[MAIN THREAD] Handling transition to online with globalInOrderFlushingActive=true, historyEnabled=true, inOrderHistory=true
I	PacketHandler	17Apr2024 13:44:26	SUBSCRIBE - [719dee55-8977-40cc-8472-3af22e49e3b1, MT-01f6c22a-76e7-436c, /127.0.0.1] on topic(s) [[spBv1.0/My MQTT Group/NCMD/PLC 1][0], [spBv1.0/My MQTT Group/DCMD/PLC 1/#][0], [spBv1.0/My MQTT Group/NDEATH/PLC 1][0]]
I	TransmissionClient	17Apr2024 13:44:26	[My MQTT Group/PLC 1][MT-01f6c22a-76e7-436c] Connected to the MQTT Server
I	TransmissionMqttCallback	17Apr2024 13:44:26	Connect complete for to tcp://localhost:1883 for MT-01f6c22a-76e7-436c - waiting for transition to online based on primary host status
I	TahuClient	17Apr2024 13:44:26	MT-01f6c22a-76e7-436c: Connected to tcp://localhost:1883
I	TahuClient	17Apr2024 13:44:26	MT-01f6c22a-76e7-436c: connect succeeded

With the following ACL, the MQTT Engine client is not able to send a rebirth request

```
R #, W spBv1.0/STATE/MyPrimaryHost
```

I	TahuClient	17Apr2024 16:03:16	ME-b8e3c40a-c8fc-4dca: MQTT Client connected to tcp://localhost:1883 on thread Thread-74182
I	PacketHandler	17Apr2024 16:03:15	SUBSCRIBE - [e594f446-1fca-49db-af98-c5b85975cda7, ME-b8e3c40a-c8fc-4dca, /127.0.0.1] on topic(s) [[spBv1.0/#][0]]
I	TahuClient	17Apr2024 16:03:15	ME-b8e3c40a-c8fc-4dca: Connected to tcp://localhost:1883
I	TahuClient	17Apr2024 16:03:15	ME-b8e3c40a-c8fc-4dca: connect with retry succeeded
I	PacketHandler	17Apr2024 16:03:15	CONNECT - [e594f446-1fca-49db-af98-c5b85975cda7, ME-b8e3c40a-c8fc-4dca, /127.0.0.1] [304] NEW Client Session
I	TahuClient	17Apr2024 16:03:15	ME-b8e3c40a-c8fc-4dca: Creating the MQTT Client to tcp://localhost:1883 on thread Thread-74182
E	EngineCallback	17Apr2024 16:03:14	Connection lost due to - Connection lost +
W	EngineCallback	17Apr2024 16:03:14	Connection Lost to - Chariot SCADA :: tcp://localhost:1883 :: ME-b8e3c40a-c8fc-4dca
W	PacketHandler	17Apr2024 16:03:14	PUBLISH - Failed authorization [client ID: ME-b8e3c40a-c8fc-4dca, username: admin, topic: spBv1.0/My MQTT Group/NCMD/PLC 1]
I	EdgeNodeManager	17Apr2024 16:03:14	Staling tags for PLC 1 via server Chariot SCADA
I	EdgeNodeManager	17Apr2024 16:03:14	Disconnecting any Nodes currently connected to this MQTT Server! 2
I	EngineCallback	17Apr2024 16:03:14	Clear out all connection counts to this MQTT Server
I	DefaultConnectionListener	17Apr2024 16:03:14	Forcefully closing SocketChannel for c4063af8-0823-4fe0-bc5e-36a72da1fb95
D	SparkplugPayloadHandler	17Apr2024 16:03:14	Sparkplug Cmd Topic: spBv1.0/My MQTT Group/NCMD/PLC 1
D	SparkplugPayloadHandler	17Apr2024 16:03:14	Publishing Command on MQTT Server: Chariot SCADA, Client ID: ME-b8e3c40a-c8fc-4dca with stripDataTypeBytes=false
I	TahuClient	17Apr2024 16:03:01	ME-b8e3c40a-c8fc-4dca: MQTT Client connected to tcp://localhost:1883 on thread Thread-74174

Connect using a LWT not allowed by the ACL

With the following ACL, the Transmission client My MQTT Group/PLC 1 is able to connect and subscribe but client My MQTT Group/PLC 2 is not authorized to connect with the LWT of spBv1.0/My MQTT Group/NDEATH/PLC 2.

```
R #, W spBv1.0/My MQTT Group/+/PLC 1/#
```

E	TransmissionClient	17Apr2024 16:46:32	[My MQTT Group/PLC 2][MT-59ad4f90-91b7-48ee] Failed to achieve connected state
I	TransmissionClient	17Apr2024 16:46:32	Attempting disconnect tcp://localhost:1883 :: MT-59ad4f90-91b7-48ee with sendDisconnect=false, publishLwt=true, waitForLwt=false, resetForceTagScan=false
I	TransmissionClient	17Apr2024 16:46:32	[My MQTT Group/PLC 2][MT-59ad4f90-91b7-48ee] No longer attempting to connect
W	TahuClient	17Apr2024 16:46:31	MT-59ad4f90-91b7-48ee: MQTT Client details: MQTT Server Name = Chariot SCADA :: MQTT Server URL = tcp://localhost:1883 :: MQTT Client ID = MT-59ad4f90-91b7-48ee :: Using Birth = false :: Using LWT = true
W	TahuClient	17Apr2024 16:46:31	MT-59ad4f90-91b7-48ee: connect failed due to Not authorized to connect +
I	DefaultConnectionListener	17Apr2024 16:46:31	Closing SocketChannel for 78d8dcc9-4b41-42e2-ae3a-b27073995c5b
W	PacketHandler	17Apr2024 16:46:31	CONNECT - Failed LWT authorization [client ID: MT-59ad4f90-91b7-48ee, username: admin, topic: spBv1.0/My MQTT Group/NDEATH/PLC 2]
I	PacketHandler	17Apr2024 16:46:31	CONNECT - [78d8dcc9-4b41-42e2-ae3a-b27073995c5b, MT-59ad4f90-91b7-48ee, /127.0.0.1] [305] NEW Client Session
I	TahuClient	17Apr2024 16:46:31	MT-59ad4f90-91b7-48ee: Creating the MQTT Client to tcp://localhost:1883 on thread Thread-74922
I	TransmissionClient	17Apr2024 16:46:31	[My MQTT Group/PLC 2][MT-59ad4f90-91b7-48ee] Attempting to connect
I	TransmissionClient	17Apr2024 16:46:31	[My MQTT Group/PLC 2][] Not connected - attempting connect with isStayRunning=true
I	TransmissionClient	17Apr2024 16:46:30	Successfully disconnected tcp://localhost:1883 :: MT-59ad4f90-91b7-48ee

Additional Resources

- Inductive Automation's Ignition download with free trial
  - Current Ignition Release
- Cirrus Link Solutions Modules for Ignition
  - Ignition Strategic Partner Modules
- Questions about this tutorial?
  - Check out the Cirrus Link Forum: https://forum.cirrus-link.com/
  - Contact support: support@cirrus-link.com
- Sales questions
  - Email: sales@cirrus-link.com
  - Phone: +1 (844) 924-7787
- About Cirrus Link
  - https://www.cirrus-link.com/about-us/