**Nginx special TCP/UDP configurations**

**ActiveMQ**

* Create TCP directory under /etc/nginx/conf.d/
* Create file activemq.conf and paste the following config block:

stream {

log\_format basic '$time\_iso8601 $remote\_addr '

'$protocol $status $bytes\_sent $bytes\_received '

'$session\_time $upstream\_addr '

'"$upstream\_bytes\_sent" "$upstream\_bytes\_received" "$upstream\_connect\_time"';

access\_log /var/log/nginx/activemq\_access.log basic buffer=1k flush=5s;

error\_log /var/log/nginx/activemq\_error.log debug;

server {

listen (nginx ip):61616; #for unsecured connection

#listen (nginx ip):61616 ssl; #for sucured connection

#ssl\_verify\_client on; #uncomment for MTLS

#ssl\_verify\_depth 2; #uncomment for MTLS

ssl\_certificate /etc/nginx/conf.d/ssl/<relevant certificate chain;

ssl\_certificate\_key /etc/nginx/conf.d/ssl/<relevant certificate key>;

#ssl\_client\_certificate /etc/nginx/conf.d/ssl/<relevant client cert>; #uncomment for MTLS

ssl\_protocols TLSv1.2 TLSv1 TLSv1.1;

ssl\_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSAAES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSAAES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK';

proxy\_pass <SWM\_IP>:61616;

}

* Add the following line at end of /etc/nginx/nginx.conf outside of the http block:

include /etc/nginx/conf.d/tcp/\*.conf;

**LWM2M**

* Create TCP directory under /etc/nginx/conf.d/
* If activemq.conf exist paste the following block inside if not create new conf file and paste the following

upstream <upstream name> {

zone backend 64k;

server <SWM\_IP):5684;

}

match coaps\_test {

send \x40\x00\x01\x01;

expect ~\* \x01\x01;

}

server {

listen [::]:5684 udp reuseport;

listen 0.0.0.0:5684 udp reuseport;

proxy\_pass leshan\_server\_coap;

health\_check interval=1 passes=2 fails=1 match=coaps\_test udp;

}

* If the below line does not exist in /etc/nginx/nginx.conf at end of /etc/nginx/nginx.conf file outside of the http block , append it to end of file:
* include /etc/nginx/conf.d/tcp/\*.conf;