gRPC Ports & Certificate Management

P4 Control Plane is moving to a *secure-by-default* model. gRPC communication will secure open ports by default. A user may choose to open insecure ports if needed, but this will be a conscious decision taken by the user at process launch time.

This document captures all the details related to gRPC ports and secure/insecure modes and certificate management.

Secure-by-default (TLS-mode)

infrap4d is launched only with secure gRPC ports open. The port numbers are:

- 9339 - an IANA-registered port for gNMI and gNOI
- 9559 - an IANA-registered port for P4RT

Generating TLS Certificates & installing with script

A script is available to generate and install the certificates in order to establish gRPC secure-mode communication. This setup script uses a pre-configured options and uses OpenSSL to generate the certificate and key files.

To run the script, which generates certificate and key files and installs to default location:

```
$IPDK_RECIPE/scripts/security/setup_certs_tls_mode.sh
```

Generating TLS certificates & installing manually

The gRPC ports are secured using TLS certificates. A Stratum script and reference configuration files are available to assist in generating the certificates. The reference file uses OpenSSL to generate the keys & certificates. However, users may choose other tools.

The reference file uses a simple PKI where a self-signed RootCA is generated and the same RootCA is used to generate server key & cert and client key & cert. This results in a 1-depth level certificate chain, which will suffice for testing and confirmation, but production systems are encouraged to generate multiple depth levels in order to conform to higher security standards.

The Stratum reference files are available here: https://github.com/stratum/stratum/tree/main/tools/tls

All certificates are in PEM format.

To generate the TLS certificates:

1. Review the files to verify if configuration settings are as-desired
2. Run the generate-certs.sh script with following command:

```
COMMON_NAME=<IP> ./generate-certs.sh
or
COMMON_NAME=<FQDN> ./generate-certs.sh
or
COMMON_NAME=localhost ./generate-certs.sh
```

3. Copy the generated *ca.crt, stratum.crt and stratum.key* to the server running infrap4d
4. Copy the generated ca.crt, client.crt and client.key to the gRPC client machine

Certificate installation

infrap4d will check for certificate in the following default location:

> */usr/share/stratum/certs/*

If alternate location is desired, the location will need to be specified during runtime with the following flags

> *-ca_cert_file=[CA certificate file]*
> *-server_cert_file=[Server certificate file]*
> *-server_key_file=[Server private key file]*

For example:

```
# Files present in /tmp/certs/ directory

$IPDK_RECIPE/install/sbin/infrap4d  -ca_cert_file=/tmp/certs/ca.crt  -server_cert_file=/tmp/certs/stratum.crt  -
server_key_file=/tmp/certs/stratum.key
```

Client Certificate Verification

infrap4d requires connecting gRPC clients to send a valid certificate that can be verified. A flag is available to the users to tune the level of security required. The available values are:

> *NO_REQUEST_CLIENT_CERT*
> *REQUEST_CLIENT_CERT_NO_VERIFY*
> *REQUEST_CLIENT_CERT_AND_VERIFY*
> *REQUIRE_CLIENT_CERT_NO_VERIFY*
> *REQUIRE_CLIENT_CERT_AND_VERIFY (default)*

More info on these values can be found on [this gRPC library documentation page](https://grpc.github.io/grpc/cpp/grpc__security__constants_8h.html#a29ffe63a8bb3b4945ecab42d82758f09).

Running in Insecure Mode

Ports can be opened in insecure mode by user if needed. This is controlled by a flag that needs to be enabled during runtime. Change the `grpc_open_insecure_ports` value to `true` to open insecure ports.

Also, make sure `certs` directory is removed from default location or user desired location as mentioned above.

To launch infrap4d with insecure ports 9339 and 9559 open:

```
$IPDK_RECIPE/install/sbin/infrap4d  -grpc_open_insecure_mode=true
```

gRPC Clients

Under default conditions, the gRPC clients will require the TLS certificates to establish communication with infrap4d server. The clients will need to use the same ca.crt file and the client.key and client.crt files signed by the ca.crt (can copy the generated files from the server if client is not on the same system as server).

P4RT Client

The p4rt-ctl (P4RT client) will default to communicate over secure mode (port 9559). If certificates are not available or if there are certificate read errors, it will try the insecure port as a fallback mechanism. This may fail if insecure ports are not open on the server.

NOTE: If running infrap4d in insecure-mode, move certificates out of /usr/share/stratum/certs folder, else p4rt client will use secure-mode only. A future fix will address this issue

gNMI Client

The gnmi-ctl (gNMI client) requests should be directed to port 9339. If the user desires to run the gnmi-ctl in insecure mode, a flag is available. Note that the insecure mode may fail if insecure ports are not open on the server.

```
$IPDK_RECIPE/install//bin/gnmi-ctl set <COMMAND>  -grpc_use_insecure_mode=true
```

==

P4OVS (old arch) build and setup

Same system for build and test

Certificates are automatically generated and installed in the default location (/usr/share/stratum/certs) folder when building p4ovs.

A script in the main p4ovs repository called `setup_certs_tls_mode.sh` calls the `stratum/stratum/tools/tls/generate-certs.sh` script to generate certificates with COMMON_NAME=localhost (see above if certificates need to be generated against other COMMON_NAME). The generated certs folder is copied over to /usr/share/stratum.

Different systems for build and test

If build system and test system are different, it is up to the user to generate the certificates (user can choose the Stratum script provided or use other methods of certificate generation) and copy them to the test system's /usr/share/stratum/certs folder.