Configure and Verify gRPC/gNMI on Nexus 9000

Contents

Introduction

This document describes how to setup gNMI for dial-in subscription to telemetry applications running on the Cisco Nexus 9000 Series switches.

Prerequisites

Requirements

General recommendations that you have knowledge of these topics:

- gRPC (Google remote-procedure-call)
- gNMI (Google RPC - Network Management Interface)
- CA certificates (Certificate Authority)
- TLS (Transport Layer Security)
- Nexus 9000 command line

Components Used

- The information in this document is based on these software and hardware versions:

Server (SW1)	N9K-C93180YC-FX	version 9.3(9)

Collector (Client)	Mac/ Ubuntu	13.4.1 / 5.19.0-46
TLS	Service running on Ubuntu	3.3.6
gNMI	Service running on Ubuntu	0.5.0

- The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

What is gRPC?

- gRPC (developed by Google) is an RPC framework to create distributed systems.
- In gRPC protocol a client running on one system can call the services defined in a remote server as if it were a local object.
- An endpoint (or a server) is a running process which is able to communicate with other endpoints with the gRPC protocol. An endpoint can host multiple services.

What is gNMI (Dail-in)?

- gNMI is Google RPC based Network Management Interface to configure network devices.

Supported gNMI RPCs

gNMI RPC	Supported
Capabilities	Yes
Get	Yes
Set	Yes
Subscribe	Yes

Supported Methods of gNMI

Server side authentication (TLS) / With Password

Configure gNMI on Nexus 9k

- Enable gRPC feature

Configure Client Machine

Install gNMI service:

```
bash -c "$(curl -sL https://get-gnmic.openconfig.net)"
```

Verify Nexus 9k

```
# show run grpc
feature grpc

#show grpc gnmi transactions
=============
gRPC Endpoint
=============
Vrf            : management
Server address : [::]:50051
Cert notBefore : Jul 19 13:16:53 2023 GMT  <- Default switch certificates used for one day
Cert notAfter  : Jul 20 13:16:53 2023 GMT
RPC          DataType   Session         Time In              Duration(ms) Status
------------ ---------- --------------- -------------------- ------------ ------
Get          ALL        3538957304      07/19 14:21:14       1            0
subtype: dtx:  st: path:
-        -     OK  /System/bgp-items/inst-items/dom-items/Dom-list/rtrId

Get          ALL        3536859976      07/19 14:20:30       1101         0
subtype: dtx:  st: path:
-        -     OK  /System/intf-items
```

Verify Client Collector

```
 % gnmic -a 10.88.146.112:50051 -u (username) -p (password) --skip-verify  get --path /System/bgp-items/
[
  {
    "source": "10.88.146.112:50051",
    "timestamp": 1689773883108293792,
    "time": "2023-07-19T19:08:03.108293792+05:30",
    "updates": [
      {
        "Path": "System/bgp-items/inst-items/dom-items/Dom-list/rtrId",
```

```
        "values": {
          "System/bgp-items/inst-items/dom-items/Dom-list/rtrId": null
        }
      }
    ]
  }
]
```

```
 % gnmic -a 10.88.146.112:50051 -u (username) -p (password) --skip-verify  capabilities
gNMI version: 0.5.0
supported models:
  - Cisco-NX-OS-device, Cisco Systems, Inc., 2022-02-04
  - DME, Cisco Systems, Inc.,
  - Cisco-NX-OS-Syslog-oper, Cisco Systems, Inc., 2019-08-15
supported encodings:
  - JSON
  - PROTO
```

Note: Data is encrypted with switch default certificates installed with password authentication.

Server Side Authentication (TLS) with Root CA Certificates and Password

Configure Client

- Generate Self-Signed Certificate (or create certificate from Certification Server).
- You can use Nexus 9k bash shell to generate self-signed certificates or Certificate server (Root CA).
- The certificate signed by Root CA can be used on the Switch or Collector.
- Use the Certificate on crypto with the password.
- Implement the crypto to the gRPC.

Become Local Root CA

These are the steps to become root and generate certificates:

1. Generate key:

```
bash-4.3# openssl genrsa -des3 -out myCA.key 2048    <<< Generate key for Root CA
Generating RSA private key, 2048 bit long modulus
..........
................
e is 65537 (0x10001)
Enter pass phrase for myCA.key:
Verifying - Enter pass phrase for myCA.key:
```

2. Generate a root certificate:

```
bash-4.3# openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1000 -out myCA.pem
Enter pass phrase for myCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:IN
Locality Name (eg, city) []:IN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IN
Organizational Unit Name (eg, section) []:IN
Common Name (e.g. server FQDN or YOUR name) []:IN
Email Address []:IN

bash-4.3# pwd
/bootflash/home/admin/certs

bash-4.3# ls -ll
total 8
-rw-r--r-- 1 root root 1743 Jul 19 14:24 myCA.key
-rw-r--r-- 1 root root 1302 Jul 19 14:25 myCA.pem
```

3. Create server certificate singed by root server:

```
1. openssl genrsa -out Server.test.key 2048. << create server private key

2. openssl req -new -key Server.test.key -out Server.test.csr << Create server csr

3. Need to create an X509 V3 certificate extension config file, which is used to define the Subject Alte

bash-4.3# cat Server.test.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
IP.1 = 10.88.x.x.   << Server IP address

4. Creating Server certificates singed by Root CA (myCA.pem)
openssl x509 -req -in Server.test.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out Server.test.crt

5. At last, we need to create .PFX file to use on switch.

 openssl pkcs12 -export -out Server.test.pfx -inkey Server.test.key -in Server.test.crt -certfile myCA.p


6. All created files

bash-4.3# ls -l
total 32
```

```
-rw-r--r-- 1 root root 1743 Jul 19 14:24 myCA.key
-rw-r--r-- 1 root root 1302 Jul 19 14:25 myCA.pem <-- .pem will be used on client machine for server aut
-rw-r--r-- 1 root root   17 Jul 19 14:40 myCA.srl
-rw-r--r-- 1 root root 1298 Jul 19 14:40 Server.test.crt
-rw-r--r-- 1 root root 1054 Jul 19 14:38 Server.test.csr
-rw-r--r-- 1 root root  203 Jul 19 14:40 Server.test.ext
-rw-r--r-- 1 root root 1679 Jul 19 14:36 Server.test.key
-rw-r--r-- 1 root root 3485 Jul 19 14:43 Server.test.pfx. <-- Copy file to Switch and import certificate
bash-4.3#
```

Configure the gRPC Nexus 9k

```
Feature grpc
crypto ca trustpoint trust_my                                          <-- trust point created
crypto ca import trust_my pkcs12 bootflash:Server.test.pfx cisco       <-- pfx file used to import
grpc certificate trust_my                                              <-- trust point added to grp
```

Verify the Switch

```
show grpc gnmi service statistics
=============
gRPC Endpoint
=============
Vrf            : management
Server address : [::]:50051
Cert notBefore : Jul 19 14:40:57 2023 GMT                          <-- Certificates installed by Ac
Cert notAfter : Oct 21 14:40:57 2025 GMT
Max concurrent calls            :  8
Listen calls                    :  1
Active calls                    :  0
Number of created calls         :  29
Number of bad calls             :  28
Subscription stream/once/poll   :  0/0/0
Max gNMI::Get concurrent        :  5
Max grpc message size           :  8388608
gNMI Synchronous calls          :  34
gNMI Synchronous errors         :  19
gNMI Adapter errors             :  18
gNMI Dtx errors                 :  0

show crypto ca certificates trust_my

Trustpoint: trust_my
certificate:
subject= /C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN/emailAddress=IN
issuer= /C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN/emailAddress=IN
serial=AC6E9591F0919488
notBefore=Jul 19 14:40:57 2023 GMT
notAfter=Oct 21 14:40:57 2025 GMT
SHA1 Fingerprint=7D:F1:7E:CD:C7:32:7E:B9:68:16:D4:D8:9A:48:C0:4A:7E:72:15:33
purposes: sslserver sslclient
```

```
CA certificate 0:
subject= /C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN/emailAddress=IN
issuer= /C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN/emailAddress=IN
serial=EE18094A2EC65F7D
notBefore=Jul 19 14:25:49 2023 GMT
notAfter=Apr 14 14:25:49 2026 GMT
SHA1 Fingerprint=A4:06:6A:80:A0:2A:D5:E1:15:92:F4:2B:50:89:BF:23:A0:52:D5:54
purposes: sslserver sslclient

show grpc gnmi transactions

=============
gRPC Endpoint
=============

Vrf : management
Server address : [::]:50051

Cert notBefore : Jul 19 14:40:57 2023 GMT
Cert notAfter : Oct 21 14:40:57 2025 GMT
Client Root Cert notBefore : n/a
Client Root Cert notAfter : n/a

RPC DataType Session Time In Duration(ms) Status
------------ ---------- --------------- ------------------- ------------ ------
Set - 3458208880 07/26 07:46:09 98 0
subtype: dtx: st: path:
Update - OK /interfaces/interface[name=mgmt0]/config/description


show run grpc
feature grpc
grpc certificate trust_my
```

Verify the client

```
1: Get

% gnmic -a 10.88.146.112:50051 -u (username) -p (Password)  --tls-ca myCA.pem get --path /System/bgp-ite
[
  {
    "source": "10.88.146.112:50051",
    "timestamp": 1689779603147750570,
    "time": "2023-07-19T20:43:23.14775057+05:30",
    "updates": [
      {
        "Path": "System/bgp-items/inst-items/dom-items/Dom-list/rtrId",
        "values": {
          "System/bgp-items/inst-items/dom-items/Dom-list/rtrId": null
        }
      }
    ]
  }
]

2: Capabilities

 % gnmic -a 10.88.146.112:50051 -u (username)  --tls-ca myCA.pem capabilities
```

```
gNMI version: 0.5.0
supported models:
  - Cisco-NX-OS-device, Cisco Systems, Inc., 2022-02-04
  - DME, Cisco Systems, Inc.,
  - Cisco-NX-OS-Syslog-oper, Cisco Systems, Inc., 2019-08-15
supported encodings:
  - JSON
  - PROTO

 % gnmic -a 10.88.146.112:50051 -u (username) -p (password)  --tls-ca myCA.pem capabilities
gNMI version: 0.5.0
supported models:
  - Cisco-NX-OS-device, Cisco Systems, Inc., 2022-02-04
  - DME, Cisco Systems, Inc.,
  - Cisco-NX-OS-Syslog-oper, Cisco Systems, Inc., 2019-08-15
supported encodings:
  - JSON
  - PROTO


3: Set

interface mgmt0      <-- No Description on interface
vrf member management
ip address x.x.x.x/x

% gnmic -a 10.88.146.112:50051 -u (username) -p (password) --tls-ca myCA.pem set --update-path "interfac
{
"source": "10.88.146.112:50051",
"timestamp": 1690357569933044933,
"time": "2023-07-26T13:16:09.933044933+05:30",
"results": [
{
"operation": "UPDATE",
"path": "interfaces/interface[name=mgmt0]/config/description"
}
]
}

interface mgmt0
description gnmic                                    <--   Description added with set RPC
vrf member management
ip address x.x.x.x/x
```

Summary

1. Check config guide for Nexus 9000 regarding further details and Guidelines/Limitations for gNMI.
2. Find link to check Openconfig path for get and set RPC.
3. You need to install RPM for Openconfig supported paths on 9.3(x) release and enable feature Openconfig starting 10.2.(2).

Related Information

- **Cisco Technical Support & Downloads**