Secure and High-available Cloud Optical Network Data Collecting and Analysis System

Jian Kong, Ryan Morgan, Chuan Qin, Binbin Guan, Yawei Yin, Hui Ma, Jamie Gaudette
Azure Networking, Microsoft Corporation, Redmond, WA, USA
{jiankong, rymorgan, binbin.guan, qinchuan, yawei.yin, huima, jagaudet}@microsoft.com

Abstract: We implement a secure and high-available optical network data collecting framework with certificate validation and rotation to enhance the security, and high-available distributed data collector to pull the optical network data for monitoring and analysis. © The Author(s).

1. Introduction

To guarantee the customer's service quality, it is important for cloud providers to quickly detect, troubleshoot and fix the issues, especially for the issues in cloud optical network. Compared to the traditional vendor-locked monitoring system, the recent advancement in optical layer network disaggregation makes it feasible to configure and monitor the optical devices from different vendors via a common model[1, 2]. Optical network telemetry allows service providers to monitor many key optical parameters, e.g., Optical Signal to Noise Ratio (OSNR), Bit Error Ratio (BER), so optical network operators can detect, fix, and even predicate the failures in time. Aim to guarantee the customer's service quality, in this paper, we illustrate a secure and high-available cloud optical network data collecting and analysis system deployed in Azure optical network. It consists of certificate management service to guarantee the optical network devices' data security by periodically validating and rotating the certificate, as well as a resilient distributed data collector framework via a lightweight streaming data protocol, gRPC, to improve the data pulling efficiency and accuracy. The configuration and PM data are exported to various data lakes, and are widely used for monitoring dashboard tools, alerts system, optical network performance analysis, as well as future failure/defects prediction.

2. Secure and High Available Data Collecting Framework

We aim to provide a secure and highly available data collecting framework in Azure optical network to guarantee the customers service quality. As shown in Fig. 1, the secure and high-available data collecting system in Azure optical network has three main components, 1). certificate management service, 2). distributed data collector, and 3). data consumer. Security is one of the top considerations when we provide cloud services to the customers. The certificate management service performs a certificate validation and rotation to enhance the network devices data security by periodically validating the devices certificate integration and compatibility and updating the device with the latest certificate if needed. We also deploy a highly available and resilient distributed data collector to pull the configuration and periodical PM data. To prevent the possible outage of the backend service and guarantee the data's availability, The distributed data collector supports various protocols, including *streaming telemetry*, *Rest API*, *SNMP(x)*, and *command-line interface (CLI)* via *ssh*. Compared to the other approaches, streaming telemetry can quickly capture the configuration changes, collect high-volume and high-resolution performance data, and sends data at a higher rate and with lower impact on the optical network devices. Those data are exported to various data lakes flexibly, e.g., different databases, and message queues. In this paper, we illustrate the streaming telemetry-based data collector pipeline via gRPC.

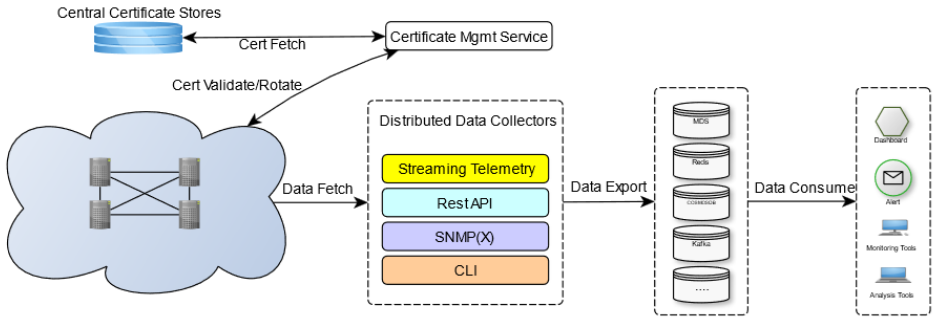


Fig. 1. Secure and high-available data collecting framework.

2.1. *Secure Data via Certificate Validation and Rotation*

Customer service security and quality are the top considerations of Azure networking. In the streaming telemetry-based data collector pipeline, we consider a lightweight streaming data protocol, gPRC, where we enable SSL/TLS mutual authentication to encrypt all the data exchanged between the client and the server. To further enhance the data and service security, the certificate management service performs a periodical validation and rotation to check the integrity and compatibility of the optical devices and rotate the certificate on devices if needed.

As shown in Fig. 2, in the certificate validation and rotation mechanism, we firstly check whether the certificate files are present on the optical devices, and whether the installed certificate is corrupt or broken. Then we check whether the certificate is expired or not based on the device's certificate information. If the certificate is valid, we then check the compatibility of certificate and the private key. After that, we compare the certificate details, e.g., cert CA, subject name, with the information retrieved from the latest certificate provided by our central certificate management service. If any validation result gets failed, we will pull the latest certificate from our centralized certificate management service and re-deploy the certificate to those devices to avoid security risk. If all validations pass, which means that the current certificate on the device is valid, this pipeline performs the certification validation every 12 hours.

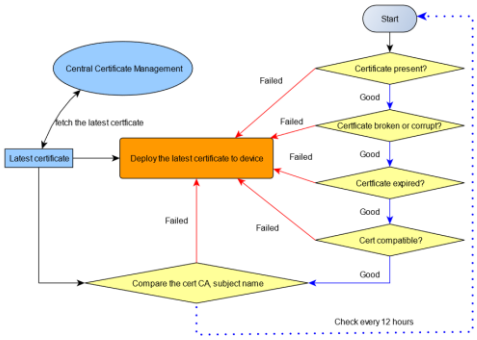


Fig. 2. Secure certificate validation and rotation.

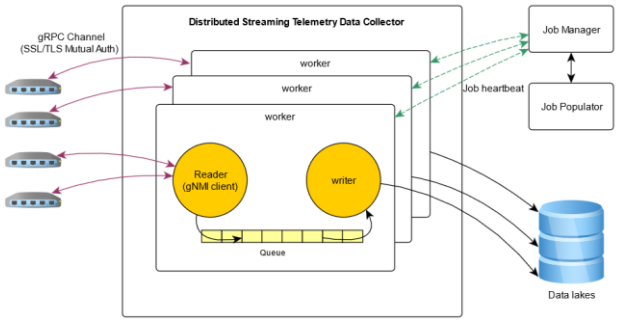


Fig. 3. High available ST data collecting pipeline.

2.2. *High-available and Real-time Data Collection Pipeline via Streaming Telemetry*

In this section, we illustrate more details on the high available streaming telemetry collection pipeline for Azure optical network to pull the data accurately and efficiently. As shown in Fig. 3., The pipeline consists of three main components, the job populator, the job manager, and the distributed streaming telemetry data collector. The job populator creates streaming telemetry pulling job for each device, continuously monitor device status, and update the jobs accordingly. After the job populator creates the job, the job manager will maintain the job lifecycle for each device, as well as the job's heartbeat session. The distributed streaming telemetry data collector mainly focuses on retrieving data from device, processing the data, and exporting the data to various data lake efficiently. It consists of two sub-compenents, the reader and writer, where reader establish persistent gRPC channel with optical devices via encrypt ed SSL/TLS, relay the data to an internal message queue, and the writer periodically read and process the data from the the message queue, and finally export the data to various data sources depends on the need. The collector pipeline is deployed in different regional clusters to improve efficiency, fault torlerance and availability.

2.3. *Data Model and Subscription Paths*

As an extensible data modeling language, YANG is widely used by numerous network standardization communities, vendors, and service providers. Compared with other YANG models[3,4,5], We adopt the OpenConfig YANG data models for the optical device configuration change and PM data. OpenConfig YANG data model is vendor-neutral, consistent, and cohesive [6], where we can avoid the extra data process. OpenConfig models also cover both configuration and monitoring data in the same model for IP devices and optical devices, so we can easily handle all the routers/switches/optical devices configuration and PM data in a consistent data collecting framework. Fig. 5. a) shows some path samples we use for optical device configuration and PM data. Generally, for PM data paths, we deploy a *Sample* mode with the sample interval 10 seconds (we can also specify different sample interval for different paths), while for other configuration/status related data paths, we use an *OnChange* mode to get the data only when there are changes to improve the efficiency. Fig. 5. b) is the

configuration template we use in the data collector for the optical amplifier data of optical long-haul devices. To be noted that due to the high-volume of the streaming telemetry data, there is a tradeoff between the metric importance, streaming telemetry mode, sample interval if it is in *Sample* mode, the device performance, as well as the backend data collector service scalability.

Table 1. a) optical device subscription paths

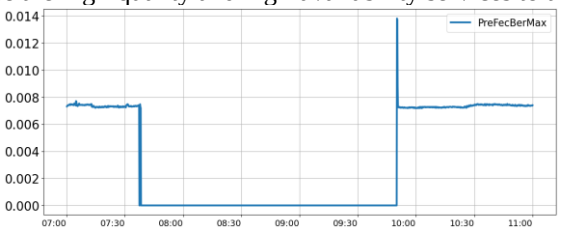
Subscription Path	Stream Mode	Interval (seconds)
openconfig-system:system/alarms/alarm/state	OnChange	N/A
openconfig-platform:components/component/state	OnChange	N/A
openconfig-optical-attenuator:optical-attenuator/attenuators/attenuator/state	SAMPLE	10
openconfig-optical-amplifier:optical-amplifier/amplifiers/amplifier/state	SAMPLE	10
openconfig-terminal-device:terminal-device/logical-channels/channel/otn/state	SAMPLE	10
openconfig-terminal-device:terminal-device/logical-channels/channel/ethernet/state	SAMPLE	10
openconfig-platform:components/component/transceiver/physical-channels/channel/state	SAMPLE	10
openconfig-terminal-device:terminal-device/logical-channels/channel/ logical-channel-assignments/assignment/state	OnChange	N/A

b) config template for optical amplifier

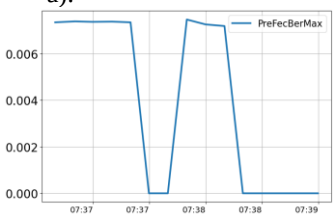
```
{
  "StreamingAgentType": "Optical Vendor A",
  "SubscriptionMode": "Sample",
  "SamplingFrequency": 10,
  "Path": "openconfig-optical-amplifier:optical-amplifier/amplifiers/amplifier/state",
  "OsVersionRegex": ".*",
  "CounterType": "OpticalAmplifiers",
  "Comment": "Optical Amplifier State "
},
```

3. Real Case – Fast Issues Detection and Fix

We deployed this efficient and resilient data collecting pipeline in Azure optical network. Compared to the other data collectors via CLI, SNMP, and Rest API, the streaming telemetry pipeline can pull the data in a more secure and efficient way, and significantly reduces the time to detect and fix the optical network issues. We use a real case of a fiber cut issue as an example. As shown in Fig. 5 c), we got several critical alarms of the transponder, which indicated that there may be a fiber cut. The ticketing system will create a new ticket based on such alarms, and network engineers can respond quickly to this issue. Fig. 5 a, b) shows the monitoring data of the metric pre-Forwarding Error Correction Bit Error Rate (preFecBer). We can find that there was flap initially, and then the network got hard down in short time. After confirming the issue, the network engineers acted immediately to involve fiber provider to troubleshoot and fix the issue. By taking advantage of the resilient, accurate and almost real-time data collected by the streaming telemetry pipeline, we can quickly respond to the network issues and restore the services and guarantee the high-quality and high-availability services to the customers.



a).



b).

TIMESTEMP	deviceHostName	Id	Resource	Severity	Text
07:38:04.4521598	Transponder_1	1	PTP-7/1	CRITICAL	Rx Loss of Clock
07:38:04.4521722	Transponder_1	2	PTP-7/2	CRITICAL	Rx Loss of Clock
07:38:04.4523446	Transponder_1	3	Port-7/3	CRITICAL	Rx Remote Fault
07:38:04.4523487	Transponder_1	13	Port-3/3	CRITICAL	Rx Remote Fault
07:38:04.4524053	Transponder_1	8	Port-7/12	CRITICAL	Rx Remote Fault
07:38:04.4524093	Transponder_1	12	PTP-3/2	CRITICAL	Rx Loss of Clock
07:38:04.4524293	Transponder_1	9	Port-7/13	CRITICAL	Rx Remote Fault
07:38:04.4525132	Transponder_1	7	Port-7/11	CRITICAL	Rx Remote Fault
07:38:04.4525191	Transponder_1	17	Port-3/11	CRITICAL	Rx Remote Fault
07:38:04.4525312	Transponder_1	19	Port-3/13	CRITICAL	Rx Remote Fault
07:38:04.4525398	Transponder_1	5	Port-7/5	CRITICAL	Rx Remote Fault
07:38:04.4525454	Transponder_1	15	Port-3/5	CRITICAL	Rx Remote Fault
07:38:04.4525535	Transponder_1	20	Port-3/14	CRITICAL	Rx Remote Fault
07:38:04.4526472	Transponder_1	18	Port-3/12	CRITICAL	Rx Remote Fault

c).

Fig. 5. Potential fiber cut detection and fast fix. a). PreFecBerMax monitoring data of transponder, b). PreFecBerMax monitoring data around fiber issue happened, c). System alarms collected

4. Conclusion

In this paper, we provide a secure and high-available distributed data collector framework for Azure optical network, including a certificate validation and rotation mechanism to enhance the network data security, and a high-available data collector pipeline to collect the data accurately and efficiently. Based on the accurate and real-time configuration and PM data, we can quickly detect and fix the potential issues in optical network, and thus guarantee the customer's service quality.

5. References

[1] A. Sadasivarao, "Demonstration of extensible threshold-based streaming telemetry for open DWDM analytics and verification," OFC 2020
[2] F. Paolucci, et al. "Telemetry Solutions in Disaggregated Optical Networks: an Experimental View", OFC 2021
[3] O. Jung-Yeol, "YANG model based optical access SDN control architecture for … multi-vendor PON systems." ECOC, 2017
[4] V. Ricard, et al. "Optical network telemetry with streaming mechanisms using transport API and Kafka." ECOC 2021
[5] OpenROADM, "http://openroadm.org/home.html"
[6] OpenConfig, "https://www.openconfig.net/projects/models/"