Cisco Telemetry Broker

The bridge to possible

Contents

Solution overview

Cisco Telemetry Broker is a foundational component for the intelligent telemetry plane, which makes telemetry architecture future proof. It provides context and visibility into the telemetry that powers products that need it, enabling telemetry brokering, filtering, and sharing.

Telemetry broker is the result of years of management, troubleshooting, transforming and sharing telemetry to power Security and Network Analytics products.

When we talk about telemetry we're referring to any data that has the potential to power a specific function. Cisco Telemetry Broker, in particular, can understand and act on all types of flow-based telemetry, such as Netflow v5, v9, IPFIX, VPC Flow Logs, NSG Flow Logs, and so on. It can also understand and act on Syslog-based telemetry, and more types of telemetry are being added with each release.

The solution comes as a hardware or virtual deployment.

Primary use cases

Telemetry architecture

When it comes to modern networks, telemetry becomes a vague concept. What does it mean, really? It's about powering DevOps, NetOps and business tools to function. It means that without that, most enterprises couldn't function. And the amount of telemetry and types of telemetry is exploding. So, why not create a dedicated network, with specific controls that don't mix up with the normal data plane? That's the objective of a modern telemetry architecture.

Telemetry brokering

How much information can we glean from the same telemetry, and how do we quantify it? One approach is to ensure that telemetry is generated once and shared multiple times. This is the best method for turning on the light in the right place with the right tools.

Telemetry filtering

One common issue to address is an overabundance of telemetry generation tools. In this scenario, you might ask:

- Should tool A send data to tools B, C, and D? Or should we only send telemetry to C and D?

- Should tools A, B, and C send data to tool D? Or should A and C only send telemetry to D?

Telemetry security

Telemetry sharing can be dangerous and costly. Sharing telemetry with the wrong tools could result in a large bill or, worse, -- enable attackers and provide them with visibility into the network's topology.

Components of the system

Manager node

The Manager node is a virtual machine that manages broker nodes. It allows admins to gain visibility into telemetry and how it is shared across consumers. Rules on input and destinations allow full control of the flow of telemetry, bringing peace of mind and maximizing ROI.

Broker node

The Broker node can be physical or virtual. Broker nodes can be clustered in a high-availability configuration to avoid disruptions on telemetry flows. All broker nodes have at least 2 network interfaces:

- Management plane for connectivity to the manager

- Telemetry plane for a dedicated telemetry architecture

Telemetry is received and forwarded on the telemetry plane for most cases.

Broker node SKU: ST-TB2300-K9. For the latest spec sheet please go to https://www.cisco.com/c/en/us/support/security/telemetry-broker/series.html.

Deployment requirements for virtual edition

The following lists the prerequisites for deploying Cisco Telemetry Broker to your network:

	Management Server	Brokering Node
CPU	4 CPUs	1 Gbit/s: 2 CPUs 10 Gbit/s: 5 CPUs Transformation Capable: 8 CPU
Memory	8 GB	1 Gbit/s: 4 GB 10 Gbit/s: 8 GB Transformation Capable: 12 GB
Storage	80 GB	70 GB

To deploy a manager to a hypervisor, you must download the OVA file from https://software.cisco.com. The Cisco Telemetry Broker Virtual Machine will synchronize its system time with the hypervisor. To ensure that features like TLS work correctly, hypervisor time needs to be accurate. To learn how to run NTP on the ESXI hypervisor, please refer to this VMWare knowledgebase article.

The node virtual appliance requires deployment on a VMware vSphere Hypervisor ESX version 6.7.

Concepts and Architecture

Cisco Telemetry Broker allows you to ingest network telemetry from many sources, replicate it, and broker that data to multiple sources. For example, you can ingest any of the following:

- On-premises network telemetry, including NetFlow, syslog, and IPFIX
- Cloud-based telemetry sources, including AWS

And consume that telemetry with a variety of tools including Cisco Secure Network Analytics and Splunk.

Cisco Telemetry Broker can also detect protocols on ingress. These protocols include

- IPFIX
- NetFlow (all versions)
- sFlow
- Syslog
- SNMP

All this functionality will come standard with the Cisco Telemetry Broker base license, which allows you to deploy as many nodes as you want. See the ordering guide for details.

FRU: Field Replacement Units

Only the following SKUs are available for replacement:

- UCSC-PSU1-1050W=
- UCS-HD600G10K12N=
- UCSC-RAIL-M6=
- UCSC-PSUV2-1050DC=

Printed in USA

C78-3837859-01   03/24