MantisNet

Real-time, network visibility and intelligence solutions

OVERVIEW OF THE MANTISNET/UNRYO INTEGRATION

5G MONITORING & ANALYTICS

Contents

Introduction

The MantisNet / Unryo integration enables teams to effectively monitor and visualize their 5G infrastructure, at scale.

In the cloud-native 5G world - network and packet constructs alone are no longer sufficient or relevant to provide the necessary visibility into the underlying infrastructure. Packets do not provide the appropriate context (container, process, link, machine, flow) and VM-based monitoring tools do not provide a sufficient depth and level of observability.

Additionally, new forms of analytics and visualization solutions are needed to collect, process, analyze and visualize these new data types(?) in order to address the operational and security needs of 5G systems

What is API Observability

API-Centric observability is a deep instrumentation and the ability to monitor events down to the lowest level. In many cases the deep visibility is derived using eBPF, which provides event monitoring down to the most basic level: links, namespace, processes, flows, containers, applications, and users. The metadata resulting from API observability tools which describes those low-level events and behaviors is then available for upstream analytics tools to exploit and derive insights.

The fundamental value of API-Centric observability is the ability to instrument and make inquiries into both system level events as well as the lowest level primitives: behaviors or interactions; sampled down to node/kernel communications, namespace, dataflows, and timestamps which can be transcoded into (JSON formatted) metadata from which to build abstractions as well as models to correlate, analyze, and understand complex behaviors.

Using foundational API metadata elements, one can apply the appropriate analytics workflows to generate a broad range of reports, alarms, KPIs, dashboards, and visualizations. Here are examples of high-level capabilities;

- Dynamic Discovery and Inventory
- Topology and Dependency Tracking
- Messaging / Payload monitoring (incl, encrypted payloads)
- Communications Flow and Tracing
- Performance, Latency, Throughput and Resource Utilization
- Resource Status and Protocol Conformance

The MantisNet – Unryo Solution

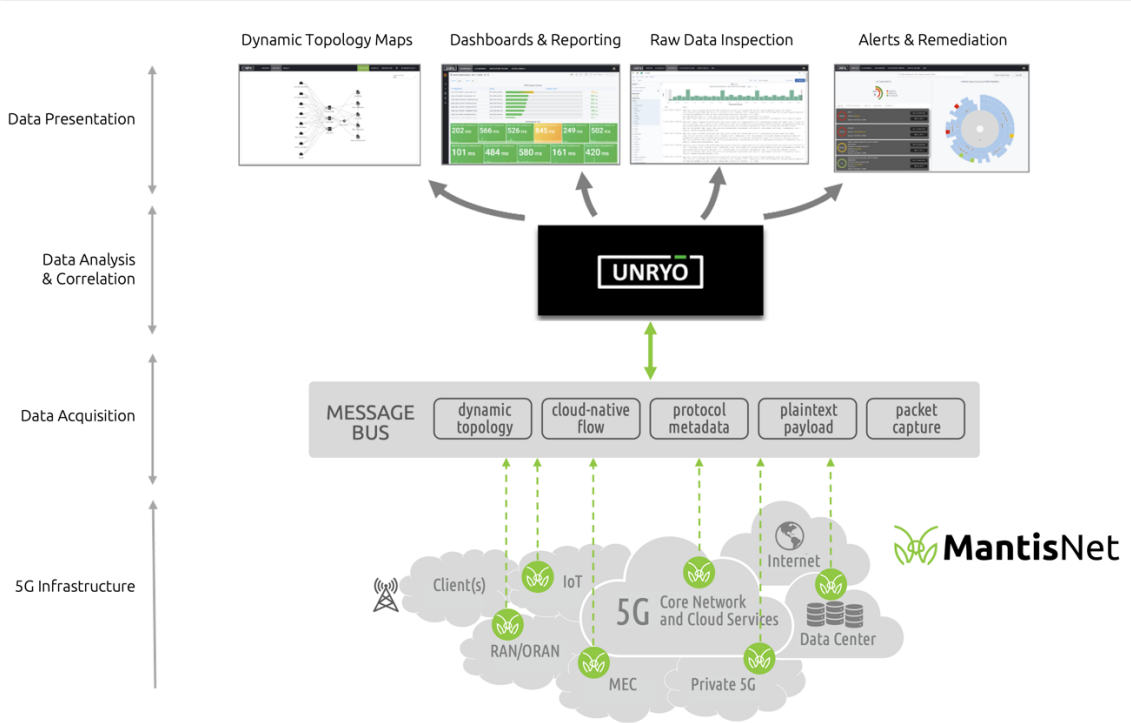


Figure 1: The Mantisnet/Unryo Platform

MantisNet and Unryo products are built using a container-based architecture, to enable state-of-the-art data collection, analytics, and visualization at scale. The solution ingests and consolidates data from distributed probes, as one unified, consistent, and ready-to-use system. This gives teams holistic visibility on the health of the 5G infrastructure, with global dashboards across all sites, down to edge-level statistics.

The MantisNet Probe

The MantisNet Containerized Visibility Fabric (CVF®) platform consists of e-BPF (extended Berkeley Packet Filter) agents that can be deployed anywhere from the core to the edge. The CVF is most typically deployed as a Helm Chart within k8s, with the agents acting as a daemonset. This deployment method allows the monitoring agents to scale directly alongside production resources, ensuring full visibility.

Once the agents are deployed, they begin monitoring the traffic where they are located and start generating what are called “data sets” for collection by Unryo. While the CVF can capture packets anywhere in the environment, it is more importantly focused on extracting JSON formatted metadata (data sets) from the environment. This metadata is streamed into an open message bus for collection by Unryo.

The CVF embraces pushing processing complexity to the edge- all processing occurs directly where the agents are active in the environment- data is not sent to a central processing location. The agents are also completely vendor agnostic- it does not matter which network function vendors are present in the environment. The CVF can monitor any and all NFs/microservices that are deployed within the cluster.

As mentioned above, the MantisNet agents are automatically deployed using Kubernetes/OpenShift/etc. via a helm chart, operator, or manually as a replicaset.

The specific metadata types that the MantisNet CVF produces includes the following data sets

- Topology | mapping of anything related to the production containers- links, flows, processes, containers, images, labels and annotations, etc.
- Flow | cloud-native flow data that is centered on network functions/microservices as opposed to IP relationships. Flow data also includes correlating information regarding end point activity (this network event came from container x, parent process ID y, etc.
- Protocol metadata | breaking down 5G specific protocol data into key value pairs. SBI, PFCP, eCPRI, service APIs in the MEC and the O-RAN, etc.
- Payload/packet metadata | capture packets from anywhere in the environment
- Encrypted session metadata | extract payload plaintext from encrypted traffic without requiring a decryption engine or key management system

The Unryo Platform

Unryo is a performance and analytics solution that monitors all your infrastructure, datacenters, clouds, and services, across the stack, and at scale.

The platform collects metrics, events, logs, and metadata from all sources, detects anomalies and performance problems in real-time, and delivers valuable insights and dashboards for your users and customers.

Unryo is built on a modular, scalable container-based architecture, to enable state-of-the-art data collection, time-series storage, log search, APM, analytics, and visualization. The Unryo Connect technology, patent-pending, is the heart of the solution. This is the industry-first cloud registry service that connects and manages every distributed component automatically and securely, as one unified, consistent, and ready-to-use system. With that, Unryo gives you the agility to operate your distributed, scalable micro-services architecture in just a few clicks, across all your data centers and public clouds.

Use Cases

5G Dynamic Topology Discovery and Inventory

The Topology and Inventory function of the MantisNet CVF observes and identifies the resources and connections the agents "see" from their deployment on the network. The CVF agents stream this topology data to a Message Bus for consumption by the Unryo data analytics platform. Additionally, the agents performing the topology function can connect to other agents to produce an aggregate mapping of all network resources.

The topology output from the MantisNet sensors can include a lot of items, but it fundamentally provides output based on a schema (see chart below) to produce the topology information that includes information about the resources under control- Flow data, machine info, processes running, process IDs, container information, etc.

Machine	Defines the machine / node / server	ID, Name, Timestamp
Container	Description of the container	Name, Namespace, Label, Image
Process	Process(es) running on a machine, in that namespace	PID, Name, Namespace, CMD
Link / Interface	Network interfaces on that machine / node / server	Name, Address, State, MTU

Subnet	Active subnet connections	IP Address, Mask
Flow	Information transmitted and received over a specific link	Source, Destination, Packets, Bytes
I/O Statistics	Raw packet counts and statistics for a specific link	Rx, Tx, Errors, Drops

Understanding the basic tenants of cloud-native resources is essential to establishing an accurate topology view of a 5G network. These environments are very complex and contain multiple levels of abstraction- the schema outlined above helps assist in creating a topology view that is not only comprehensive, but also able to detect the dynamic nature of cloud resources. The CVF agents provide this data continuously to the Unryo platform, allowing the collective solution to be aware of the dynamic resource scaling (up and down) and resource modification that often is found in distributed computing environments.

It is also important to note that the CVF agents can observe very granular metrics associated with the entities that are key to understanding topology (machine, container, process, etc.). In the below example of CVF metadata that is provided to the Unryo platform, one can see that there is detailed information available regarding processes, CRI, and k8s resources...

Figure 2: Example metadata from CVF agent:


```
"container": {
  "id": "85cc1390f2b9c4bacb66c30fa3e629f914a72da68f55ccecd41b44e45f13cef4",
  "name": "/k8s_nrf_free5gc-free5gc-nrf-nrf-66c5ff5d89-tp97v_default_ec61c6f7-01eb-409f-8d49-d1606391fb5d_0",
  "cri": "Docker",
  "labels": {
    "annotation.io.kubernetes.container.hash": "c64d95b6",
    "annotation.io.kubernetes.container.ports": "[{\"containerPort\":8000,\"protocol\":\"TCP\"}]",
    "annotation.io.kubernetes.container.restartCount": "0",
    "annotation.io.kubernetes.container.terminationMessagePath": "/dev/termination-log",
    "annotation.io.kubernetes.container.terminationMessagePolicy": "File",
    "annotation.io.kubernetes.pod.terminationGracePeriod": "30",
    "io.kubernetes.container.logpath": "/var/log/pods/default_free5gc-free5gc-nrf-nrf-66c5ff5d89-tp97v_ec61c6f7-01eb-409f-8d49-d1606391fb5d/nrf/0.log",
    "io.kubernetes.container.name": "nrf",
    "io.kubernetes.docker.type": "container",
    "io.kubernetes.pod.name": "free5gc-free5gc-nrf-nrf-66c5ff5d89-tp97v",
    "io.kubernetes.pod.namespace": "default",
    "io.kubernetes.pod.uid": "ec61c6f7-01eb-409f-8d49-d1606391fb5d",
    "io.kubernetes.sandbox.id": "1c21fa989720b22394781ebcdd95550135c08da00b04efb9849a48b127a9a5de",
    "maintainer": "raoufkh <khichane.araouf@gmail.com>"
  },
  "image": "sha256:46b1740cd93249086b9468c1d2ffd6f86a3deee68f424428a71d1b4c58955b00",
  "cmd": "-nrfcfg ../config/nrfcfg.yaml"
},
"pid": 86071,
"ppid": 86001,
"name": "nrf",
"cmd": "./nrf -nrfcfg ../config/nrfcfg.yaml",
"exe": "/free5gc/nrf/nrf",
"ns": "4-4026532370",
"startedAt": "2023-01-23T16:43:51Z"
```


Looking at “container” metadata in Figure 2, for example, the CVF agents are providing more than just a container name. This includes information on the CRI, labels and annotations, and

associated image and cmd…all of which can be very helpful in creating a clearer picture of what a cloud-native environment looks like at any given point in time.

Anomaly Detection & Event Correlation

As the data stream from the MantisNet agents is received, the Unryo platform performs on-the-fly analytics and correlation to detect issues and gives context to facilitate the resolution.

Anomaly Detection: With machine learning capabilities and statistical algorithms, the analytic engine uses several techniques to analyze data, including adaptive thresholding, baseline deviation, outlier detection, forecasting and more.

Root Cause Analysis & Impact: From the metadata and topology information provided by MantisNet probes, Unryo dynamically builds the relationships and displays it in an interactive topology map, across multiple layers (5G, containers, service). This topology knowledge is used by the RCA engine to correlate, finding the root-cause and its impacts.

Service Monitoring (with SLA breach analysis): The correlation engine lets you define or import Business Services such as Customers, Department, Contracts and more; then calculates their status, based on impact analysis driven by propagation rules, to determine how Services are affected.

Team Collaboration & Remediation: An alarm Console helps teams collaborate for efficient fault resolution. The alarm console is fully customizable, allowing users, support teams and domain specialists to configure their own panels, columns and filters.

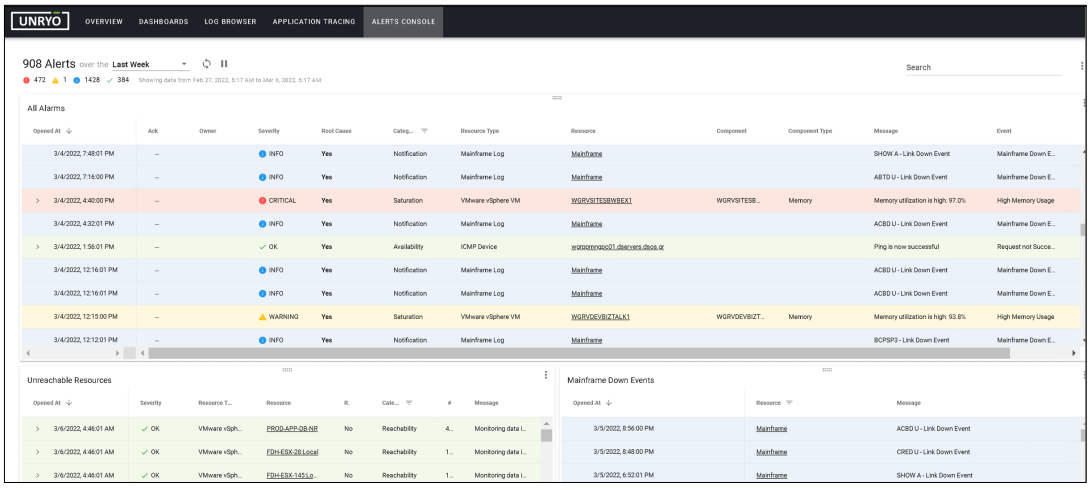


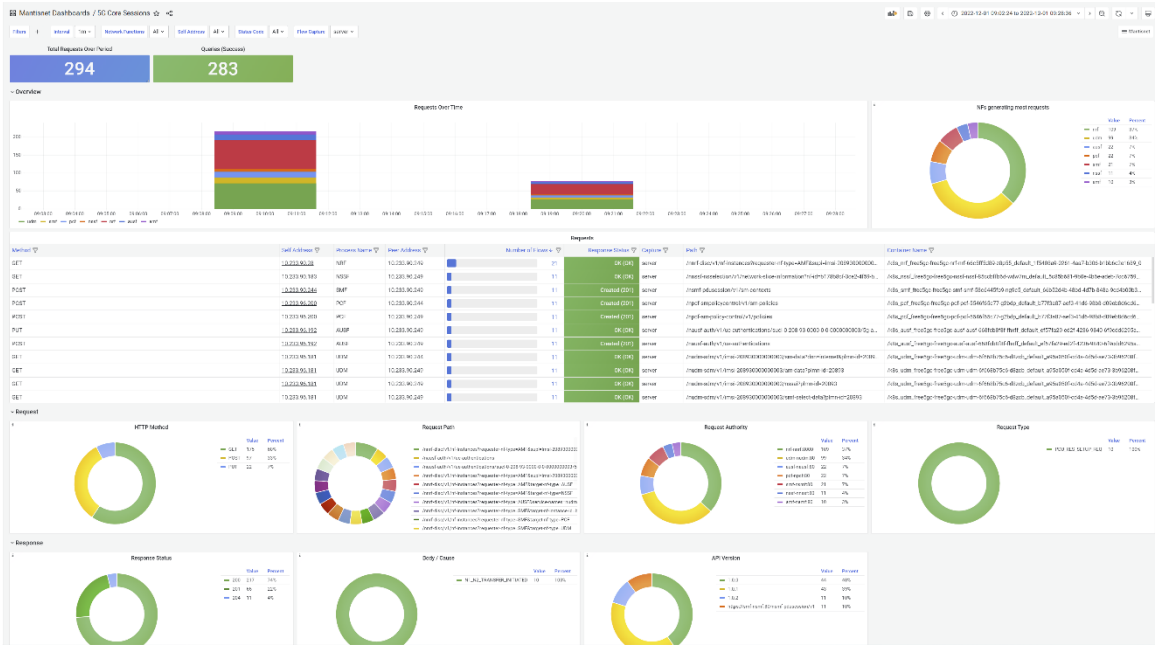
Figure 1 – Customizable Alarm Console for cross-team collaboration

Real-time Insights & Dashboards

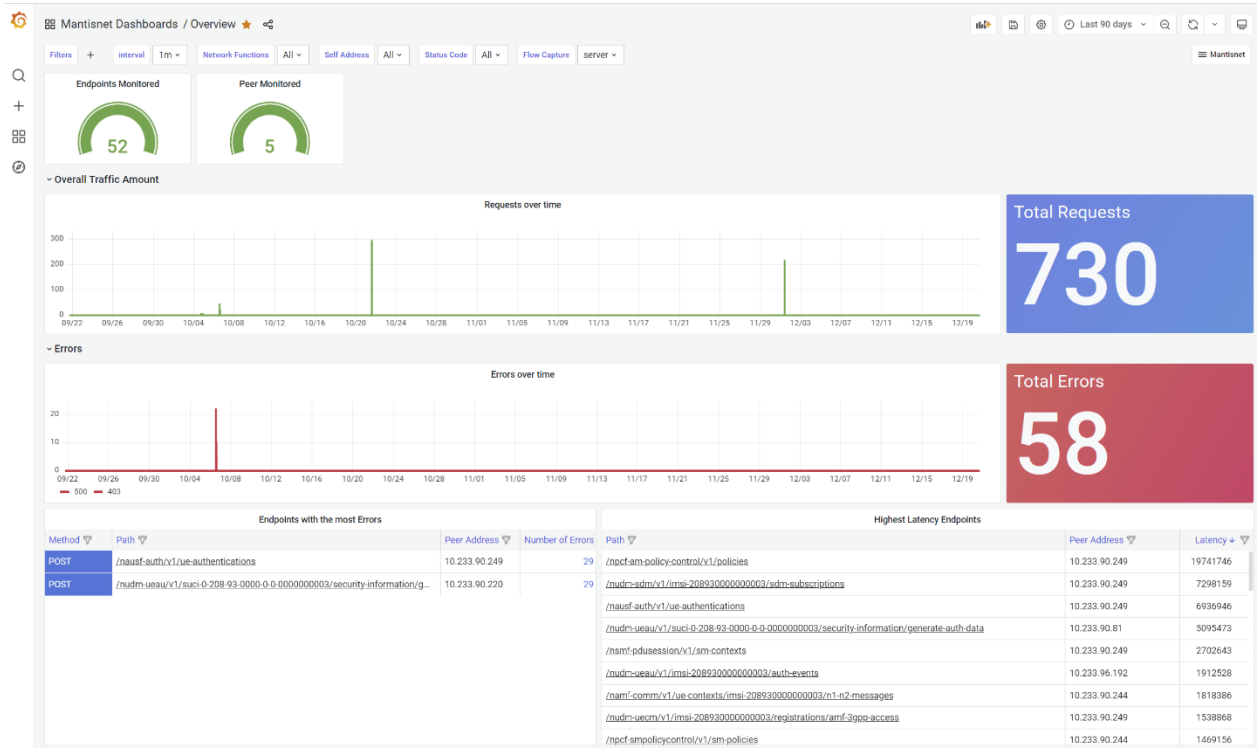
The Unryo Portal lets users visualize, explore, monitor, and share data. Users instantly get insights on the performance, health and capacity of the entire infrastructure and all services.

All insights and data from MantisNet probes are stored and consolidated on the platform. Global dashboards show the overall view across all sites, down to API-level statistics. Every metric is enriched with metadata tags such as the location or namespace to allow for dynamic grouping, filtering and analytics.

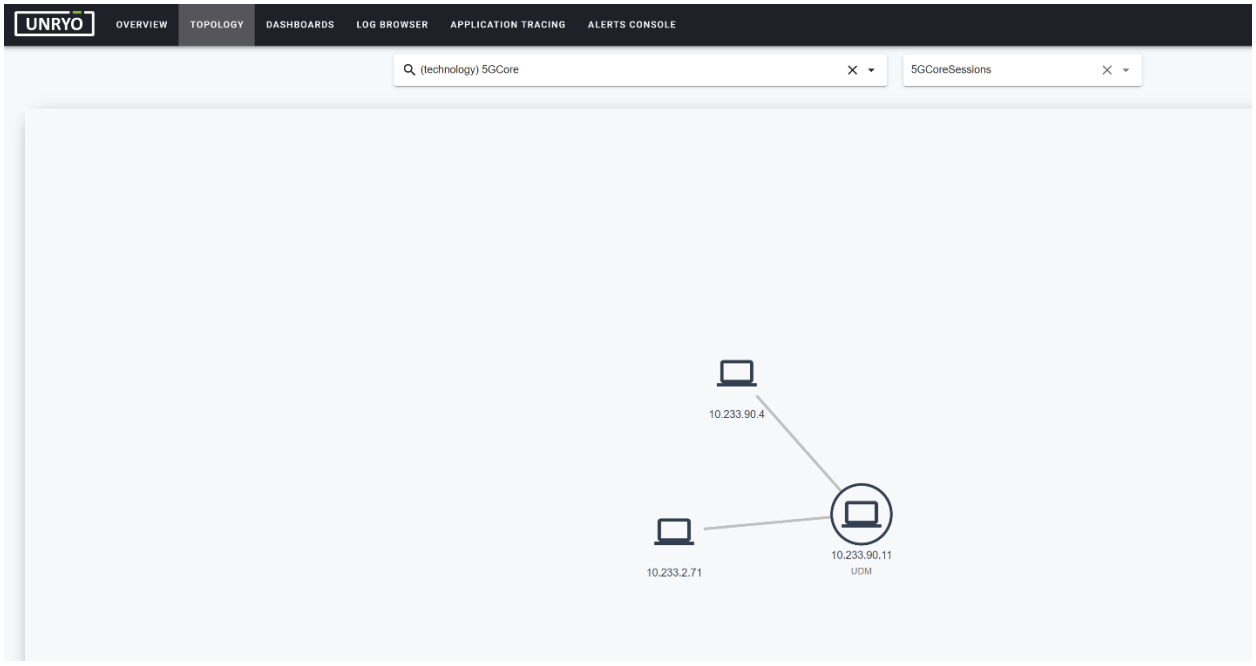
The portal is packaged with out-of-the-box dashboards, and users have full flexibility to create their own very simply. Drag-and-drop panels, group and filter data using metadata tags or compute your own KPI with booleans and mathematical formulas.



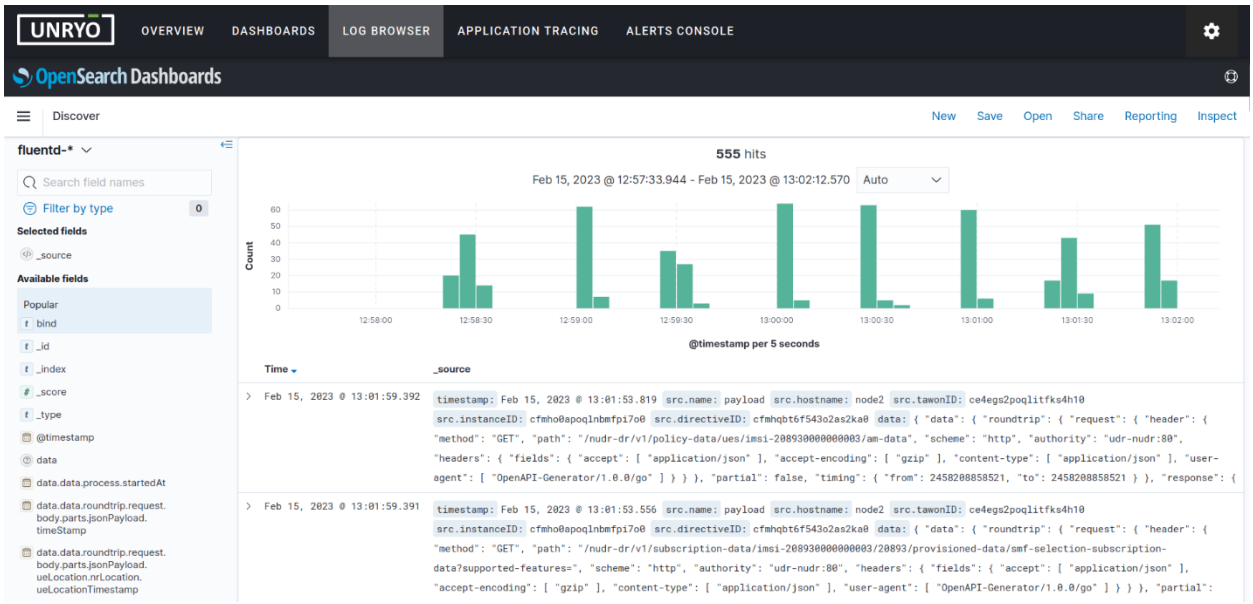
Example 1: API Observability



Example 2: Success Rate over Time



Example 3: Topology Discovery & Visualization



Example 4: Packet Inspection

Benefits

High Data Quality

5G Topology Discovery & Visualization

Real-time insights

Single pane of glass, with detailed, technical and service-centric dashboards

Topology Map (components & dependencies)

Alarm Views, with triage and cross-team collaboration

Reduced Outages & Increased Customer Satisfaction

Early Detection of Problems

Root-Cause Detection & Impact Calculation of Services

AI-powered Anomaly Detection

Alarm Reduction & Prioritization

Modern & Scalable Platform

Cloud-Native Architecture

On-Premise or SaaS

CONCLUSION

The Mantisnet/Unryo platform offers a real-time and multi-vendor visibility on the 5G network, from core to edge. By capturing various metadata sets - topology, flows, sessions and payload - and by monitoring it using analytics and ML engines, the platform provides service providers with actionable insights and reporting, and with proactive triage of network and service issues.

About Unryo

Unryo is a modern performance monitoring and analytics platform that lets organizations gain full visibility into all the layers of their infrastructure, from the network all the way up to deep inside their applications. Unryo detects problems across virtual, physical, and multi-cloud networks, then it uses correlation to identify the root cause and impacts, so organizations reduce the service outages and ensure strong customer satisfaction. For more information you can contact us at:

300 4670, Desserte Sud, A-440 Ouest
Laval, Québec, Canada H7T 2Z8
(514) 900-1068
INFO@UNRYO.COM

About MantisNet

MantisNet is a leader in the observability and cloud-native technology revolution that is rapidly disrupting IT operations. The MantisNet observability platform—the Containerized Visibility Fabric (CVF) — provides access and visibility into the inner workings of cloud-native, micro-services based environments—from the core to the edge. The MantisNet CVF platform is both vendor and cloud agnostic; it combines the power of deep kernel-level instrumentation, a composable event-driven architecture, and in-node processing to deliver continuous, real-time visibility. As a result, the MantisNet CVF provides significant cost, operational and security benefits. For more information you can contact us at:

11160 C1 South Lakes Drive,

Suite 190, Reston VA, VA 20191

(571)306-1234

INFO@MANTISNET.COM