Incident Management for Network Service

draft-feng-opsawg-incident-management-01

Chong Feng (frank.Fengchong@Huawei.com)
Tong Hu (hutong@cmhi.chinamobile.com)
Luis Contreras (luismiguel.contrerasmurillo@telefonica.com)
Thomas Graf (Thomas.graf@Swisscom.com)
Qin Wu (bill.wu@huawei.com)
Chaode Yu (yuchaode@huawei.com)
Nigel Davis (ndavis@ciena.com)
Motivation

• The management system is overwhelmed by the frequency and quantity of alarms, KPI, trace information with the growth of new service and service complexity
  • Data compression method is time consuming, labor intensive
    • low processing efficiency
  • Two many duplicated tickets are triggered
  • Usually rely on maintenance engineers’ experience
    • inaccurate root cause identification

• It is difficult to assess the impact of alarms and/or metrics on network services
  • Some KPIs affect the network service, however there are no tickets to be triggered

• The management system is built as a silo and manages performance data, fault data, trace information separately
  • However the investigation of some faults also depends on some other data like topology data or performance data
What is the Incident?

- Incident Definition: The unexpected interruption of network services, degradation of network service quality or sub-health of network services.
  - Incident is the network level event,
  - used in the interface between OSS and Domain controller

- One incident can take multiple alarms/performance metrics, abnormal operation event as input and is triggered when the service is affected;

- multiple alarms, metrics, or hybrid can be aggregated into one incident after analysis.
How Incident management works?

Incident is the unexpected interruption of network services, degradation of network service quality or sub-health of network services.

- **Incident management** is proposed to:
  - Provide consistent management of different type of data sources by aggregating various different Performance data, alarm data, trace information into the incident for the network service
    - Align with TMF724A “Incident Management API Profile”
  - Correlate topology data together with alarm, KPI, etc by
    - Add leafref to specific hardware component and node in the network topo model
  - Identify the relationship between the incident and the network service
    - The relationship between the incident and the network service can be preconfigured
      - E.g., derived from the relation between subservice and symptom in the Service assurance model
    - The relationship between the incident and the network service can be identified
      - Using Service Impact analysis
  - Use AI and troubleshooting API to accurately identify the root causes of device, network, and service faults and report the root causes to the O&M system of the carrier through the incident northbound interface
    - Incident report/querying
    - Incident diagnosis
    - Incident resolution
Incident Identification Use Cases

Case 1 – Incident Identification based on alarm data
Preconfigure the relation between the network service, incident, trigger the incident when a set of alarms (e.g., IGP down) affect the service

Case 2 – Incident Identification based on KPI data
Preconfigure the relation between the network service and incident, trigger the incident when degraded service Impact user experience

Case 3 – Incident Detection based on Service Impact Analysis
Identify the relation between the network service and the incident Dynamically based on Service Impact analysis results

Orchestrator

Controller

PE1
P1
P2
PE2

VPN A Unavailable
IGP Down
Interface Down
IGP Peer Down

VPN A Degradation
Packet Loss
Packet Delay

Orchestrator

Controller

PE1
P1
P2
PE2

Service Impact Analysis
Root Cause Analysis Results
Root Cause Identification
• Root Cause Analysis
• Failure Case Analysis
Cluster Analysis
• Time based Correlation
Topo based Correlation

Impact Level or degrees/ Packet loss, Latency

The number of Base Station to be impacted

IETF 117
Interworking with Alarm Management

• Incident management can work together with alarm management
  • Alarms can work as one of data sources of incident management
  • Alarm may be aggregated into few amount of incidents by correlation analysis
  • Incident server may use alarm management interface [RFC8632] to shelve some alarms.

• In addition, the incident has established relation with service instance
  • One incident can be mapped to multiple service instance
  • Service impact analysis and root cause analysis determines this mapping.
Incident Data Model Design Overview

An incident instance is identified by incident-id, associated with one or more service instances, and specify the following key attributes.

- **Incident-id**: The identifier of an incident instance, it MUST be unique in the whole system.
- **Domain**: Indicate the domain where the incident instance occurs. Such as RAN, OTN, PTN, etc.
- **Category**: Indicates the component where the incident instance occurs. Such as power system, line card, protocol, etc.
- **Priority**: Indicates the priority of this incident instance.
- **Sources**: Indicates the objects that have symptoms related to an incident instance. Such as down interface, high CPU, etc.
- **Root-causes**: Indicate the root cause objects related to a incident instance.
- **Events**: the events associated with an incident instance, including alarms, logs, KPIs and other events.

- Incident Notification: Triggered by incident identification or update of incident Instance
  - Incident Diagnosis RPC performed on some detection tasks, such as BFD detection, flow detection, telemetry collection, short-term threshold alarm, configuration error check, or test packet injection.
  - Incident Resolve RPC allows multiple incident instances to be resolved trigger notification for incident status change.
Comments? Questions?
Interworking with SAIN

- SAIN can be one way to identify incident for incident management system
  - If some metrics are evaluated to indicate unhealthy for specific sub-service, some symptoms will be present.
  - Incident server can generate the incident based on symptoms, and then report it to upper layer system.
    - E.g., Healthscore for sub service meets specific threshold
    - Incident MUST be at the network level.
When network services are deployed/updated, the trace information will be collected by analytics.

If some lower level errors (hardware malfunction) occur, the analytics will analyze the trace information. If these errors match the incident rule (e.g., $a > 100$), an incident at the service level will be triggered.

The impacted network services can also be determined according to the trace information.
Relation with TMF Incident Management Profile

Scope of draft-feng-opsawg -incident-management-00
Define YANG model for incident lifecycle management

TMF724 defined Incident Management API profile including Requirements, functions, Component capability.

TMF656 Service Problem Management API User Guide
TMF724 Incident Management API Profile
TMF628 TMF628 Performance Management API REST Specification