Orange GNOCe ONAP PITEC robot use-case  1st stage and development plan

Marian Skorupa

OPNFV Plugfest &ONAP Developer Design Forum   2019
January 8-11
Topics

- Orange GNOCe ONAP PITEC rationale
- ONAP & PITEC building blocks
- Issue – distant OSS tools connectivity failures
- PITEC connectivity chain
- PITEC set up architecture
- ONAP PITEC set up containers
- PITEC open loop – ticketing
- ONAP PITEC analytics
The ONAP PITEC Robot E2E user experience solution provides continuous control over whole GNOCe operation scope toolbox accessibility and provide operations teams with visibility and control of network environments even if complex and geographically dispersed with multi vendor factor.

The intelligent automation of the OSS tools of multinational operations will support services reliability by accessibility control, discovering quality of application connectivity and proactive service continuity risk analysis.

Automating business processes relating to tools access management provides organizations quantifiable savings in terms of personnel time by freeing up staff to focus on more strategic, more business critical tasks.

ONAP allows us to integrate the tooling box used for network management and to automate operations e.g to on-board and instantiate IPTEC probe VNFs, and to collect measurements results through VES collector and DMaaP.

For any questions, suggestions, feedback or comments to the solution, please e-mail leader of the ONAP PITEC project – marian.skorupa@orange.com
ONAP & PITEC building blocks
The issue - Connectivity Failures

1. „Hard” failures:
   - are the kind of problems every organization understands
   - Fiber cut
   - Power failure takes down routers
   - Hardware failure
   - monitoring systems are good at alerting hard failures
     - i.e. GNOC staff sees something turn red on their screen
     - Engineers have been alerted by monitoring systems

2. „Soft” failures:
   - are different and often go undetected
   - Basic connectivity (ping, traceroute, web pages, email) all of it works correctly but...
   - Performance is just poor
PITEC connectivity chain

Interconnection Reference model ITU T Layers

Application
Presentation
Session
Transport
Network
Data link
Physical

RTT [ms]

Expected timing chain:

< < < < <
CITRIX internal
application
external
application
PITEC set up - architecture

ONAP

- VES Collecto
- DCAE
- DMaaS
- ... ...

PITEC

- VES Agent
- ... ...

Measured system

Orange Data Center

GNOCe OSS2 ecosystem and networks

ONAP

- VES Collector
- ... ...

DMaaS

Grafana

InfluxDB

VES Agent

OSS2 ecosystem and networks

GNOCe

THE LINUX FOUNDATION
ONAP PITEC set up - containers

ONAP’s DCAE elements

- PITEC
- VES Collector
- DMaaP
- Zookeeper
- DMAAP
- Kafka
- Adapter
- Influx DB
- Grafana

- Docker Container
- Application developed in project

docker-compose.yml
ONAP PITEC

Next steps
**ONAP Analytics for PITEC**

**Input:**
An ordered sequence of Lag values in [ms] at equally spaced time intervals.

**Job:**
- Analytics is based on time stamped connectivity performance measurements
- The output value should be understandable for the non-specialist, we decide to use 0-100% scale
- Have been decided using the concept of medicine Survival Function as output
- Cumulative Distribution Function (Survival Function) would be used to normalize & quantify measurements

**Description:**
In PITEC case the survival function gives the probability that a connection will survive beyond given specified time (maximum time is given by history buffer of measurement in Analytics).

Analytics should have historical data to process current measurement.

**Proposed alarm policy by 20% of health = 105ms RTT**
ONAP Policy for PITEC

Input:
Estimated by Analytics current connection Survival Probability.

Description:
• They determine current business rules to normalize analytics output in order to apply it to threshold.
• Policy may include events history eg. pre-Christmas peak of network utilization
• Tasks related to scheduled work or failures (ticketing systems form or automated action).
• Policy should apply coefficient related to known scheduler of everyday routine traffic changes.

Output:
Current connection health in %.
Input:
Current connection health in %

Job:
It is used to generate actions by APPC for given by Policy rated, quantized and standarized health value

Description:
The PITEC threshold exceeded event class indicates that ONAP module detects a query that exceeds the threshold specified for the measurement.

Note:
The detection interval for this event is 15 seconds. It is guaranteed that an event will be generated if a query exceeds the specified limit by at least 15 seconds. However, if a query exceeds the specified threshold by less than 15 seconds, its detection might be missed depending on the timing of the query and the time of last detection sweep.
ONAP Automated actions

**Job:**
After the action is triggered by TCA, it is proposed to change the measurement configuration for given connectivity chain in order to provide better performance overview.

**Description:**

No action:

Action in loop:
Questions
1. Exemplary OSS application
2. Startup:
   a) Cactus
   b) Citrix
   c) VDI viewer
3. VDI viewer disconnection
4. StartMenu opening lags
5. Tests:
   a) Cactus login overload
   b) Network problems

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>UX measurement</th>
<th>Proposed management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Lags time</td>
<td>1. Alarms</td>
</tr>
<tr>
<td></td>
<td>2a. Startup time</td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>2b. Startup time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2c. Startup time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Amount of drop rate</td>
<td>3. Alarms</td>
</tr>
<tr>
<td></td>
<td>4. Round trip time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.</td>
<td>4. Alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|              | a) amount rate | a) amount rate |
|              |                |                |

a) amount rate
b) KPI transgression monthly
### Connectivity

1. Exemplary OSS application Lags
2. Startup:
   - a) Cactus opening
   - b) Citrix opening
   - c) VDI viewer opening
3. VDI viewer disconnection
4. StartMenu opening (rtt)
5. FailTests:
   - a) Cactus login overload
   - b) Network problems

### Data Preparation

1. Survival Function
   - 2a. Aggregation
   - 2b. Aggregation
   - 2c. Aggregation
3. Hazard rate
4. Survival Function
5. 
   - a) Aggregation
   - b) Aggregation

### Proposed Alarm Threshold

1. Alarm < 20% of health (?)
2. KPI Average total time access to applications
   - a) + b) + c)
3. Alarm > 3 x / hour
4. Alarm < 20% of health
5. KPI Connectivity success rate
   - a) + b)
Thank you