Service Monitoring Team VM Requirements

This document contains requested requirements for the virtual machine configuration, with justifications and use cases.

Contents

[Overview 1](#_Toc155089383)

[Project Canary Purpose and Summary 2](#_Toc155089384)

[Data 4](#_Toc155089385)

[Connectivity 5](#_Toc155089386)

[Configurability 5](#_Toc155089387)

# Overview

The Service Monitoring Team (SMT) within Service Assurance requires their own server to host existing and future web applications, projects and tools which can be used to improve the observability of data to teams across the business. Currently the main project is Project Canary (described further below) which aims to centralise monitoring of key services into a single interactive view.

Stakeholder list:

1. ELT (incl. Martin)
2. Simon, Fiona and other SLT members.
3. MIM Team
4. ESMAT.

|  |  |
| --- | --- |
| **Requirement** | **Justification** |
| Connectivity to SharePoint API will be downloading files from <https://hutchison3g.sharepoint.com> | Data will be sent from partners to an email address, then uploaded onto SharePoint. SharePoint API will be used to download from SharePoint onto the server to visualize the data. |
| Ability to send and receive emails to H3G email addresses. | Server is to host monitoring platform. Emails are needed to send email alerts when monitoring/data thresholds are reached. |
| MQTT port 1883 open. | To allow for MQTT protocol to be used internally for communications between front end and backend. |

# Project Canary Purpose and Summary

Hosted at [arcade.h3gprod.net:8071](http://arcade.h3gprod.net:8071/honeyc_home), Project Canary is a web app that will centralise monitoring and data processing for the following key services:

MNP

Roaming

Voice / Data / Messaging

MVNO

B2B

Order Management

Finance

Retail

Contact Centre

Online / Digital

It will receive data for each service, and display aspects of that data to allow a user to view the health of key services. When investigating, users can click through different layers to view specific KPI data, and be linked to specific dashboards depending on the services.



Figure 1: Main view of Project Canary Home Screen. There is a serious problem with Voice & Data so it has been tagged in red.

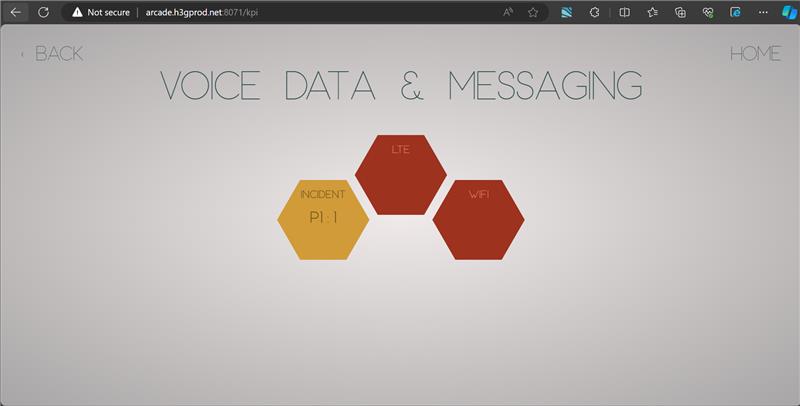


Figure 2: Example user journey part 1. Clicking on Voice & Data, the next layer and breakdown of health is visible. This shows that there is an active P1, as well as problems with both VoLTE and VoWIFI.



Figure 3: Example user journey part 2. Clicking on the WIFI hexagon in Figure 2 shows the breakdown of WIFI data. Specific figures are displayed that are the reasons for the colour change. These figures update in real time, and will vary for different types of KPI.

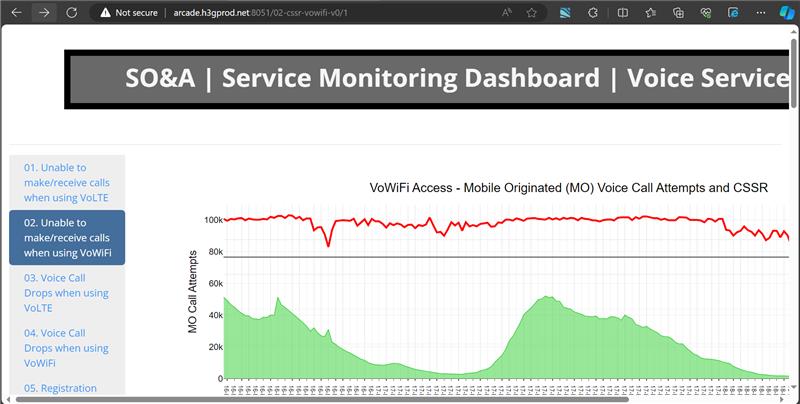


Figure 4: Clicking further on the hexagons in Figure 3 link the user to a dashboard where they can view the information as in depth as possible.

This journey will be similar for each KPI, where users can view a very brief summary of data. Security requirements can be put in any layer.

A diagram of a computer

Description automatically generated

Figure 5: Diagram of Canary operation

# Data

Data will be updated in real time on the server. Some data may be sensitive if it is required for an important KPI. Individual files for data will be held in a directory, that can only be accessed through administrative logon to the VM via ssh. This will only be possible by the Service Monitoring Team.

**Users will have NO direct access to the data, outside of summaries shown like in Fig. 3.** **Linked dashboards (Fig.4) will have their own, separate access considerations on the dashboard end.**

Data files will not be held longer than 24 hours, typically around 2 hours or less, however in the event there is a problem with the data supply, and no new file arrives on the server, the server will keep the previous file unless set otherwise.

Additionally, databases may be employed which track some datapoints over longer than 24 hours, such as MNP operations over weekends.

Current examples of data files that are/will be imminently used are:

CSV for most recently active ~10,000 incidents, with summary, priority, dates of modification, assigned group, submitter, SLA status etc.

XLS file for Voice over LTE data from Nokia. This file contains values for numbers of call drops, successful/failed call setups and metadata.

XLS file for Voice over WIFI data from Nokia. This file contains values for numbers of call drops, successful/failed call setups and metadata.

MNP data on number of stuck ports, which networks, dates and times etc.

Orders data, status of all current orders and fulfilment from SO&A SRE.

**These are examples that will be similarly detailed to the types of data Project Canary will be ingesting in the future.**

All received data will be processed and summarised for relevance as shown in above figures.

# Connectivity

This list is in priority order.

1. The web app must be accessible from the standard corporate network. It is designed and intended to be used across multiple departments by Three employees as well as trusted partners such as other monitoring teams in the future.
2. Sharepoint API connectivity. Data will be being downloaded from H3G Sharepoint to be processed. It will be regularly checked and updated.
3. VM SSH login must be accessible from the corporate network for the Service Monitoring Team to connect and operate without losing other monitoring connections to remote desktops etc.
4. Some form of SMTP setup and connectivity. This will be used to email specific parties when specific alert thresholds are met for specific services. For example, Nokia incident management may be alerted if a serious voice alert is detected. These emails would ideally contain a summary of the alert profile but it is configurable. Emails would be infrequent and likely at most 50 emails sent out per month once multiple services are up and running in the distant future.
5. MQTT port 1883 open internally to allow for efficient communications between different parts of the program.

# Configurability

With the exception of Sharepoint API connectivity, all security aspects and access aspects have some malleability. Any advice or requirements can be considered if constraints are present.