05-01-2022

NMaaS OAV Architecture Analysis White Paper

Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 2
Dissemination Level:	PU (Public)
Document ID:	GN4-3-22-B9209C

Authors: Łukasz Łopatowski (PSNC), Donal Cunningham (HEAnet), Eduardo Jacob (EHU/RedIRIS), Estela Carmona Cejudo (I2CAT/RedIRIS), Iacovos Ioannou (CYNET), Ivana Golub (PSNC), Jasone Astorga (EHU/RedIRIS), Kostas Stamos (GRNET), Maria Isabel Gandia Carriedo (CSUC/RedIRIS), Roman Lapacz (PSNC), Simone Spinelli (GEANT), Sonja Filiposka (UKIM/MARnet), Susanne Naegele-Jackson (FAU/DFN), Tim Chown (JISC)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

The document analyses the mapping of the NMaaS (Network Management as a Service) architecture to the TM Forum's Open Digital Architecture aiming to provide a standardised view of the components and implementations of orchestration, automation and virtualisation for network management services.

Table of Contents

Table of Figures

Executive Summary

Analysing network management architectures from an orchestration, automation, and virtualisation (OAV) point of view using a common reference architecture helps align efforts, and find similarities in the way different functionalities and components are implemented, which in turn facilitates potential collaboration between organisations and future interoperability. In pursuit of this goal, the GN4-3 *Network Technologies and Services Development* Work Package (WP6), *Network Services Evolution & Development* task (T2) selected the TM Forum Open Digital Architecture (ODA) as a reference blueprint architecture that can be used for such cross-comparison. The rationale for that choice is described in Deliverable D6.6 *Transforming Services with Orchestration and Automation* [DEL].

The WP6T2 team is working with the GÉANT project development teams and NRENs to perform such mappings. In this document the team reports on the analysis of the different functional aspects of the Network Management as a Service (NMaaS) architecture and how its components map to the ODA reference model. The mapping highlights the main characteristics and capabilities of the NMaaS architecture as it is implemented in its production version in GÉANT, and how they fit into the main functional domains of ODA. The analysis was carried out by the NMaaS development team supported by the WP6T2 team.

1 Introduction

Network Management as a Service (NMaaS) is a platform as a service (PaaS) based solution that provides a large portfolio of applications that can be used for network management and monitoring purposes [NMI]. The instantiation of each offer in the catalogue is done on a per-user basis: isolated containers that host the application instance are created on demand, and the user can access and manage the provided application using a secure Virtual Private Network (VPN) connection.

In this way, NMaaS offers an isolated network management environment that can be used by individual users or organisations to test the features of the available network management applications or, more importantly, use the applications to manage their production networks [NMS]. The NMaaS catalogue is regularly being updated with additional applications based on user requests. Most of the applications are commonly available as open-source solutions or are developed within the GÉANT community either as part of the work on the GÉANT project or internal work of the NRENs.

The NMaaS catalogue, also called application marketplace, offered via the NMaaS portal, is behind the scenes powered by the NMaaS multi-tenant PaaS system. This system is in charge of the provisioning of the chosen network management applications, enabling the users to use the applications without the traditional overhead of owning and maintaining the infrastructure where the applications are running. One of the wide-scale examples of using NMaaS includes the network management of the GÉANT P4 Laboratory, which is carried out within the RARE project [RAN].

In effect, the NMaaS service comprises three components:

1. Providing, managing and maintaining the infrastructure of the NMaaS software components and selected network management applications.
2. Support for users that use the NMaaS portal and for the tools they select for network management via NMaaS.
3. Support for contributors that would like to offer their applications/tools/software via the NMaaS marketplace.

It is important to note that, although the initial set of tools offered via the NMaaS portal focuses on network management and monitoring, the platform can be used for any type of application added to the catalogue.

From an OAV point of view, the development of NMaaS within the GÉANT project is of great interest because it is an example of a highly automated system that provides full container lifecycle orchestration using a mix of open-source and in-house developed components. There are few cloud-based platform offerings in the GÉANT community, with the trend rapidly rising as the cloud platform approach has been recognised as one of the driving technologies in the digital transformation process [CDT].

This document is focused on the analysis of the general NMaaS system architecture and the particular implementation of the GÉANT-hosted NMaaS production service from the point of view of the TM Forum Open Digital Architecture (ODA) concepts of decoupling and functional grouping.

2 Architecture Analysis

2.1 Main ODA Functional Domains

The main idea behind ODA is the decoupling and integration of components which enables an independent choice of solutions for each component, while at the same time maintaining a unified overall approach that supports the full end-to-end service lifecycle (including interoperability). The high-level ODA functional architecture [ODA] maps the main components by their capabilities to the so-called ODA functional blocks (see Figure 2.1).

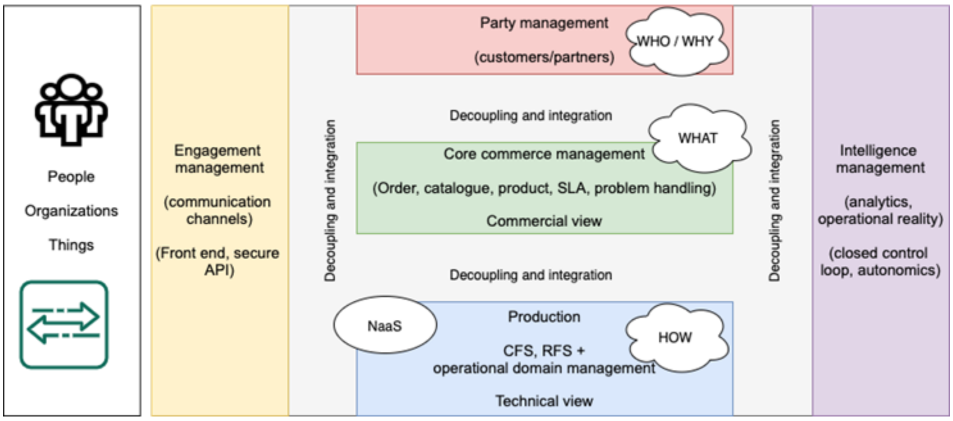

People
Organizations
Things
Engagement management
(communication channels)
(Front end, secure API)
Decoupling and integration
Party management
(customers/partners)
WHO / WHY
Decoupling and integration
WHAT
Core commerce management
(Order, catalogue, product, SLA, problem handling)
Commercial view
Decoupling and integration
NaaS
Production
HOW
CFS, RFS +
operational domain management
Technical view
Decoupling and integration
Intelligence management
(analytics, operational reality)
(closed control loop, autonomics)

Figure 2.1: The TM Forum ODA functional architecture

In a nutshell:

- The **Engagement Management** functional block focuses on the engagement with the end-users (people and systems) that can interact via multiple channels.
- The **Party Management** functional block handles the processes that are related to all parties that interact with the organisation and defines their roles and relationships.
- The **Intelligence Management** functional block is in charge of the implementation of data analytics processes and, based on the analysis, provides closed control loops for full automation wherever possible.
- The **Core Commerce Management** functional block focuses on the placement of products and services to the customers and manages the product lifecycle.
- The **Production** functional block manages the delivery and lifecycle of all customer-facing and resource-facing services that can be based on different technologies or might be a

combination of multiple operational domains including multi-domain services provided with the cooperation of other parties.

2.2 NMaaS High-Level Components Overview

The complete NMaaS solution is composed of custom software components that are implemented within the GÉANT project and complemented with third party open-source solutions [NMC]. Together they form a cloud-based ecosystem enabling on-demand deployment of user applications, using Docker containers deployed in a Kubernetes cluster.

The high-level NMaaS design includes several components [NMS], see Figure 2.2:

- NMaaS Portal – a web-based front-end user interface (UI) application (in-house developed) that runs in the user's web browser. It retrieves all relevant data from the back-end systems and displays it to the user. This is the user view of the NMaaS catalogue/marketplace that provides the main functionalities offered to end-users.
- NMaaS Platform – the core component (in-house developed) responsible for serving content to the UI application (NMaaS Portal). The main functionalities of the NMaaS Platform include user management, application portfolio management, orchestration of application deployment and configuration. For these purposes, the NMaaS Platform interacts with the central NMaaS database where the user and application data are stored.
- NMaaS Janitor – a second back-end application (in-house developed) with a specific set of responsibilities closely related to the interaction with the Kubernetes API. These include:
    - setting up basic authentication for some of the applications
    - application deployment status verification
    - initial creation, upload and syncing of deployed application configuration between its container and a respective Git repository
- NMaaS Repository – implemented as a custom GitLab application instance, this component supports the Platform functionalities by storing the configuration files that are dynamically prepared and maintained for each application instance that is deployed in the cloud [GIL].
- NMaaS Docker Registry – either a single or multiple Docker Registry [DOR] instances used to store the Docker images of all applications available in the marketplace.
- NMaaS Helm Repository – either a single or multiple Helm Chart Repository [HER] instances hosting charts for all applications in the marketplace
- Virtualised infrastructure – built using a Kubernetes cluster for deploying and orchestrating application instances as containers and secure data communication networks (DCNs) that connect the application instances with the user networks [KUB].

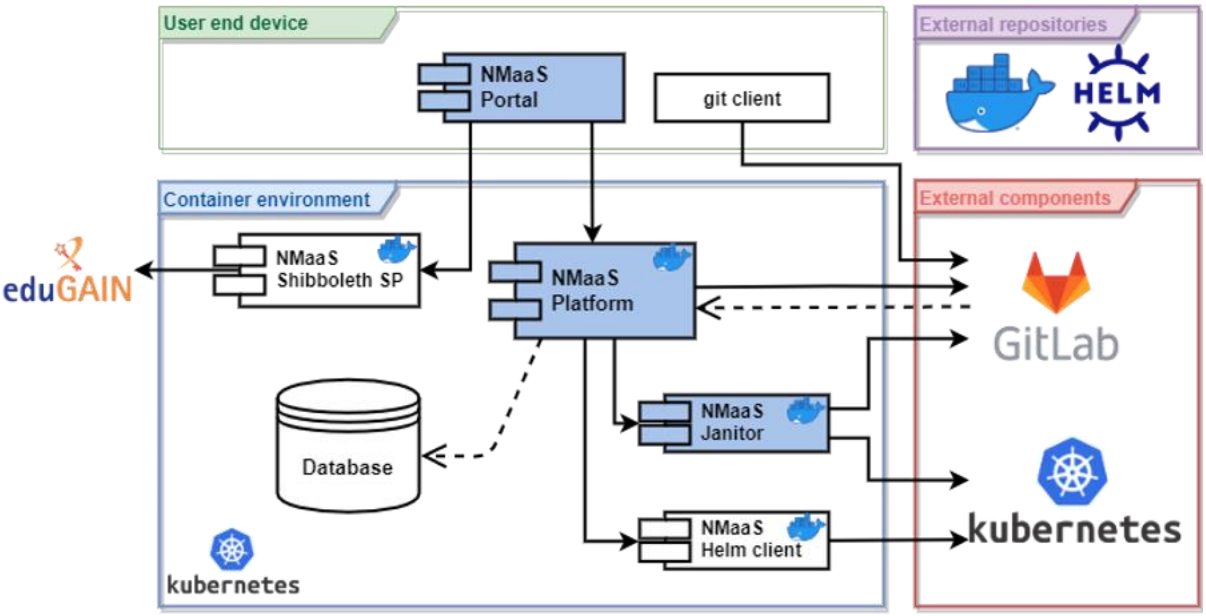


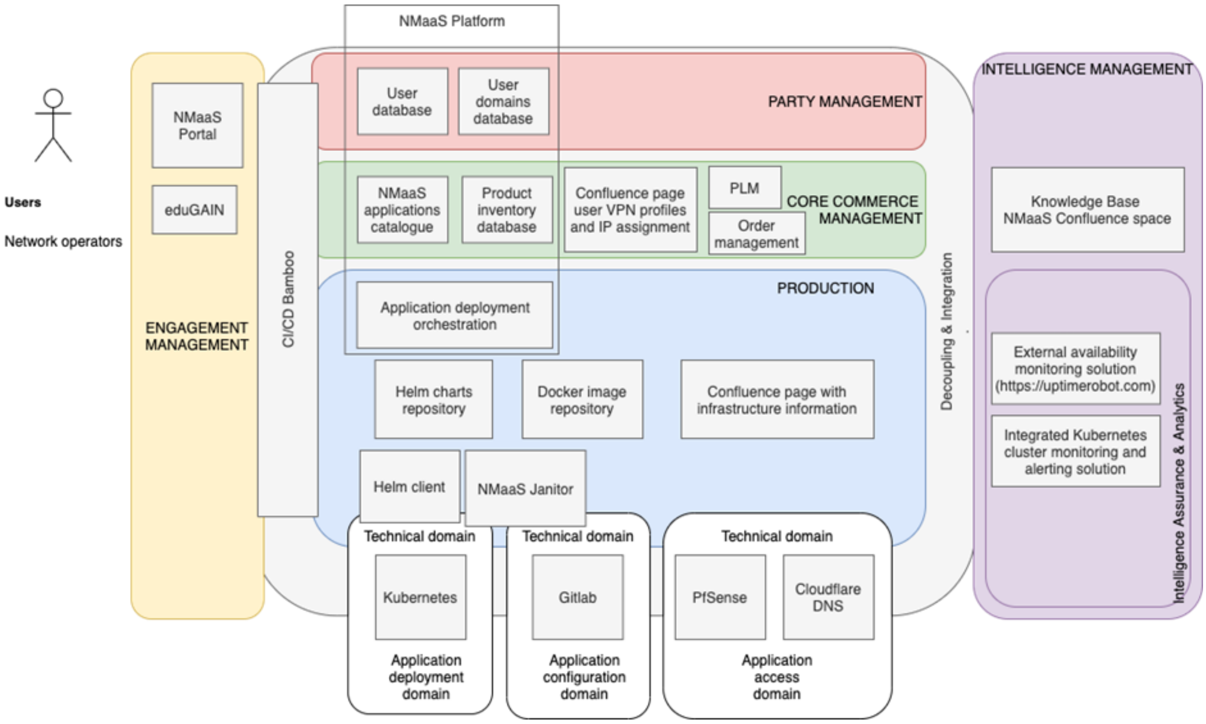
Figure 2.2: NMaaS system components

2.3 Mapping of NMaaS System Components

The functionalities offered by each of the NMaaS components can be mapped to one or multiple functional domains of the TM Forum Open Digital Architecture. This mapping is presented in Figure 2.3 specifically for the NMaaS service operated by the GÉANT project which is deployed in PSNC and offered at https://nmaas.eu.

It is important to note that users can and are encouraged to deploy NMaaS on top of their own custom infrastructures. In such cases, the NMaaS in-house developed components are mandatory. However, the third-party components used for the repositories and registry can easily be replaced with others that provide the same functionality.

As presented in Figure 2.3, some of the NMaaS components span several ODA functional blocks in which case they are broken down into lower level modules with specific functionalities that correspond to the functional domain where they are located.



NMaaS Platform
Users
Network operators
NMaaS Portal
eduGAIN
ENGAGEMENT MANAGEMENT
CI/CD Bamboo
User database
User domains database
PARTY MANAGEMENT
NMaaS applications catalogue
Product inventory database
Confluence page user VPN profiles and IP assignment
PLM
Order management
CORE COMMERCE MANAGEMENT
PRODUCTION
Application deployment orchestration
Helm charts repository
Docker image repository
Confluence page with infrastructure information
Helm client
NMaaS Janitor
Technical domain
Kubernetes
Application deployment domain
Technical domain
Gitlab
Application configuration domain
Technical domain
PfSense
Cloudflare DNS
Application access domain
Decoupling & Integration
INTELLIGENCE MANAGEMENT
Knowledge Base NMaaS Confluence space
External availability monitoring solution (https://uptimerobot.com)
Integrated Kubernetes cluster monitoring and alerting solution
Intelligence Assurance & Analytics

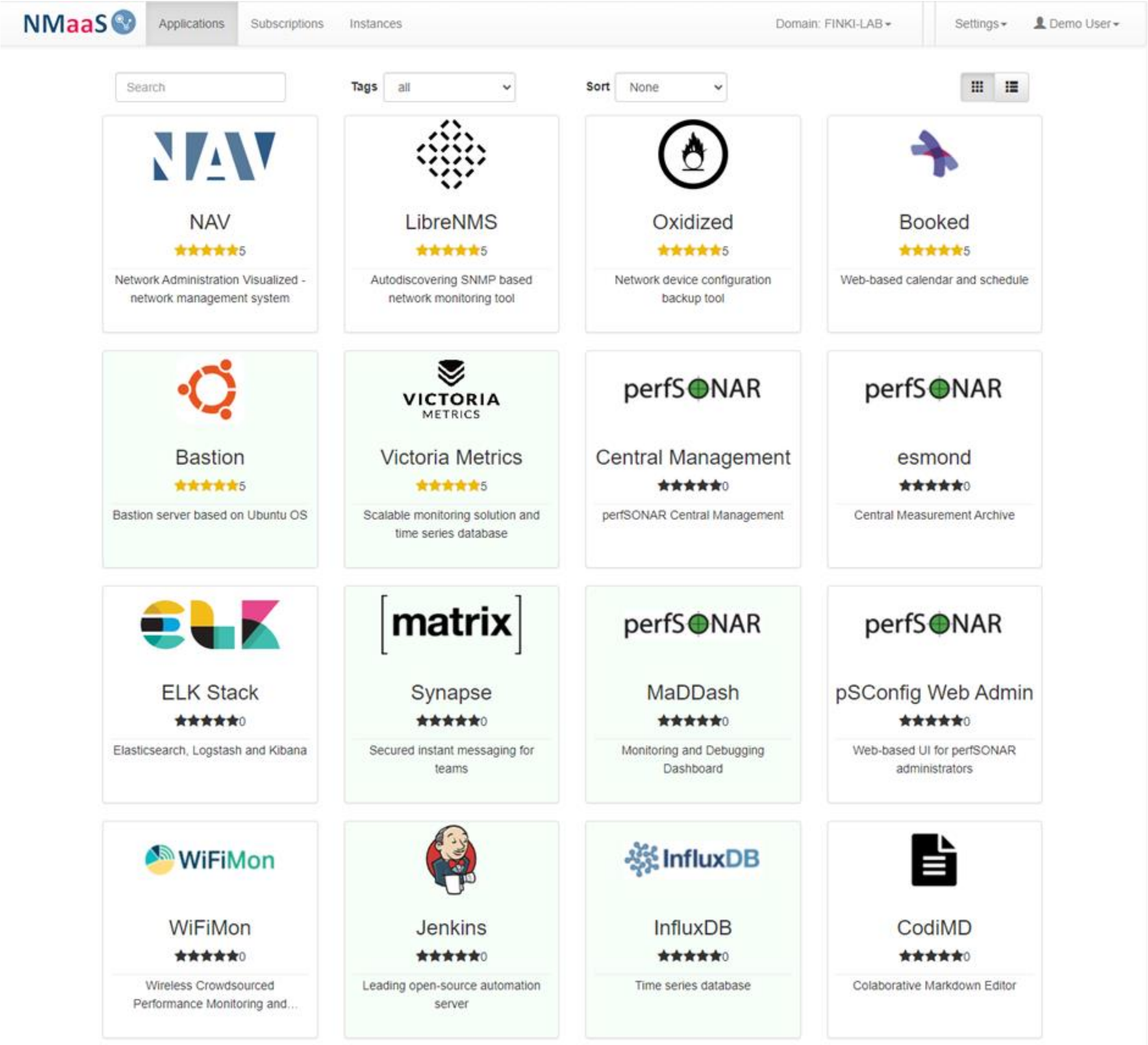
Figure 2.3: NMaaS components mapped to the TM Forum ODA functional blocks

2.3.1 Engagement Management

The user interaction with the NMaaS service is done exclusively via the NMaaS Portal as it is the user front-end application. The NMaaS Portal provides an overview of the available applications using the information stored in the NMaaS application catalogue, and offers a GUI that enables the user to order application instances. The main view of the application catalogue as provided by the NMaaS Portal is presented in Figure 2.4.

The portal also offers a contact form that consists of a set of predefined options that enable users to issue requests for new applications, provide information about useful new NMaaS features that are input into the NMaaS Product Lifecycle Management (PLM) process, ask for technical support, or submit general questions and comments.

Only authenticated users can use the NMaaS Portal. Authentication is enabled either via an eduGAIN login or local user account registration. The hook to eduGAIN is implemented using a Shibboleth service provider [SSP].



NAV ★★★★★5 Network Administration Visualized - network management system

LibreNMS ★★★★★5 Autodiscovering SNMP based network monitoring tool

Oxidized ★★★★★5 Network device configuration backup tool

Booked ★★★★★5 Web-based calendar and schedule

Bastion ★★★★★5 Bastion server based on Ubuntu OS

Victoria Metrics ★★★★★5 Scalable monitoring solution and time series database

Central Management ★★★★★0 perfSONAR Central Management

esmond ★★★★★0 Central Measurement Archive

ELK Stack ★★★★★0 Elasticsearch, Logstash and Kibana

Synapse ★★★★★0 Secured instant messaging for teams

MaDDash ★★★★★0 Monitoring and Debugging Dashboard

pSConfig Web Admin ★★★★★0 Web-based UI for perfSONAR administrators

WiFiMon ★★★★★0 Wireless Crowdsourced Performance Monitoring and...

Jenkins ★★★★★0 Leading open-source automation server

InfluxDB ★★★★★0 Time series database

CodiMD ★★★★★0 Colaborative Markdown Editor

Figure 2.4: NMaaS portal

2.3.2 Party Management

The core component of NMaaS, the NMaaS Platform, comprises a number of modules that offer the main back-end functionalities of the solution. The User database and User domain database modules are located within the Party Management functional block, both of which are implemented as parts of the database that stores all NMaaS-related information.

The User database stores and manages individual user information, including user contact information, user preferences and personal SSH keys.

The User domain database stores and controls information on an organisation/project level. Namely, when using NMaaS, users can create Domains (tenant environments) that are then used and managed by a given number of users that belong to the same project or organisation. Multiple users that belong to the same domain have access to all applications that are instantiated for the given domain. In this way collaborative work is supported.

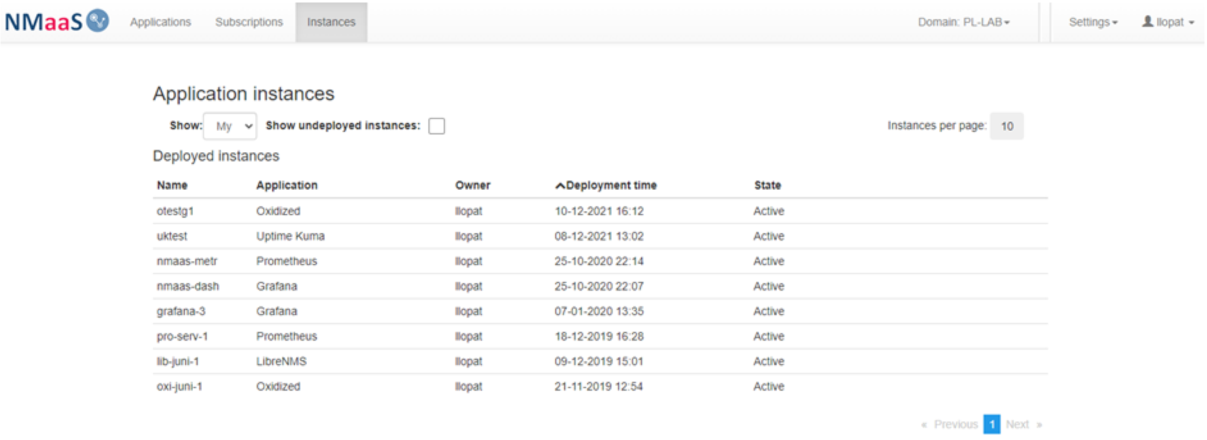
The information stored in the Party Management modules is used to determine user roles and access rights within the NMaaS Portal either in the scope of the entire system or within a particular domain. Depending on the role assigned, users are only allowed to view deployed application access information or manage the entire application lifecycle.

2.3.3 Core Commerce Management

The second set of functionalities of the NMaaS Platform can be mapped to the Core Commerce Management functional block. These are all functionalities related to the management of the NMaaS application offerings and their lifecycle.

The NMaaS application catalogue is part of the NMaaS database that stores the specifications of all available applications offered to users.

The NMaaS Portal exposes an application ordering process that tracks and manages the users' order requests, interfacing with the Production application deployment orchestration for the creation of application instances. In addition, users can also use the NMaaS portal to add new applications to the catalogue, provided they have sufficient rights and permissions to use this feature. This automated process of extending the NMaaS application catalogue enables users to be directly involved in the creation of application offerings.



Application instances

Show: My Show undeployed instances: □ Instances per page: 10

Deployed instances

Name	Application	Owner	^Deployment time	State
otestg1	Oxidized	llopat	10-12-2021 16:12	Active
uktest	Uptime Kuma	llopat	08-12-2021 13:02	Active
nmaas-metr	Prometheus	llopat	25-10-2020 22:14	Active
nmaas-dash	Grafana	llopat	25-10-2020 22:07	Active
grafana-3	Grafana	llopat	07-01-2020 13:35	Active
pro-serv-1	Prometheus	llopat	18-12-2019 16:28	Active
lib-juni-1	LibreNMS	llopat	09-12-2019 15:01	Active
oxi-juni-1	Oxidized	llopat	21-11-2019 12:54	Active

Figure 2.5: Application instances view from the NMaaS portal

All application instances (seeFigure 2.4) are stored and managed in a separate NMaaS database module that acts as a product inventory. In addition, the information about the user VPN profiles and the IP assignment is maintained manually in a Confluence Wiki page. Two types of VPN profiles are used to access all applications deployed in a given domain. A static site-to-site VPN (one profile created for a given domain) is used to connect the applications hosted in Kubernetes with the managed devices. However, dedicated, personal client-VPN profiles enable users to connect to the application UI.

If a user problem needs to be handled by the service support team, information is gathered via an NMaaS Portal user form, that is then sent as an email to a dedicated mailing list. When the problem is confirmed as an issue, a corresponding JIRA ticket is created.

The complete NMaaS service development is managed via a PLM process that implements regular reviews and determines the development of new features based on account user feedback. The NMaaS team also generates regular KPI reports that are available for administrators and managers, which refer to the NMaaS software components' performance only. Public KPI values are regularly published in the Service Statistics section of the NMaaS wiki [NMW].

2.3.4 Production

The final set of functionalities of the NMaaS Platform is focused on the implementation of the application deployment orchestration that is in charge of instantiation, configuration, and management of the application containers in Kubernetes.

Based on the input parameters provided by the NMaaS Platform, the Helm client [HEL] (package manager for Kubernetes) is in charge of application deployment and management. The packages are called Helm charts. Helm charts describe the Kubernetes resources that will be used for the application deployment. All application deployment charts are stored in the Helm chart repository.

The NMaaS Janitor is used to facilitate the automatic configuration of the deployed user applications based on the specific application configuration stored in GitLab.

All Docker images for the NMaaS applications, as well as for the NMaaS components themselves, are stored in a Docker image repository.

For the purposes of implementing a Resource inventory, the NMaaS team maintains a Wiki Confluence page with all infrastructure-related information regarding both the IT and the network infrastructure configuration hosting the NMaaS service.

2.3.5 Technical Domains

Three technical domains should be mentioned:

- **Application deployment domain** - Both the NMaaS software components and the user application instances are deployed in a Kubernetes cluster installed on top of a set of bare metal servers managed by Proxmox [PRO].
- **Application configuration domain** - The core component of the user application instances' configuration process is a dedicated, private instance of GitLab that hosts a number of user Git repositories created on demand for each application instance that needs to store any kind of configuration files.

  During the new application instance configuration process, the NMaaS Platform creates a new project (repository) on GitLab and pushes a set of configuration files specific to the application that is being deployed. NMaaS Janitor then picks up these files to create ConfigMap objects in the Kubernetes cluster. Users can clone their repositories and apply changes to the content of the files utilising SSH key-based authentication.
- **Application access domain** - To enable secure user access to application instances deployed within the Kubernetes cluster, some third-party solutions are used:

  - ○ The PfSense software firewall appliance is used to control the network traffic passed in and out of the cluster by being a single point of entry to the cluster from the external world. It is also used to terminate VPN tunnels established between the user end devices or user networks and their application running in the cluster.
  - ○ A Cloudflare DNS solution is used to manage domain name assignment.

2.3.6 Integration and Decoupling

The high-level architecture of NMaaS enables users that are interested in hosting their own NMaaS solution to choose some of the components for their customised environment. This is made possible by developing the NMaaS in-house components in such a way that they expose well-defined APIs that can be used to perform the integration with other components. Specifically:

- NMaaS Platform exposes a REST API that is consumed by the NMaaS Portal.
- NMaaS Janitor exposes a Google Protobuf style API.

2.3.7 Intelligence Management

Regarding the aspect of available data that can be stored and used for "intelligent" analysis there is:

- External availability monitoring based on UpTimeRobot [UTR] which is used for tracking availability of user-facing application components including the NMaaS Platform and the NMaaS Portal (in terms of the endpoint from which the Portal software is downloaded to user browser). At the moment the gathered data is used for the periodical KPI reporting.

- Integrated Kubernetes cluster monitoring and an alerting Prometheus-based solution that provides comprehensive monitoring information about the Kubernetes cluster (including the underlying infrastructure) as well as the applications running on top of it.

In addition, the NMaaS Confluence space [NMW] is used as a documentation/knowledge base that stores a vast amount of information related to the service. The public space includes general information about the service and user guidelines.

3 Conclusions

NMaaS provides a fully automated cloud platform for hosting user applications instantiated as containers hosted in a Kubernetes cluster. The custom-built application deployment orchestrator is also in charge of setting up a VPN connection between the user and the application instance enabling an isolated, secure environment that can host production-level tools and applications.

The in-house developed NMaaS software components are developed with decoupling in mind, following the general ODA recommendations. While further improvements could be made to modularisation, the option to replace some of the third-party components with others in different NMaaS implementations provides great flexibility for interested parties that would like to host their own NMaaS solution.

With the increasing trend of providing applications and tools as services in the cloud, and thus removing the responsibilities of installation and infrastructure maintenance from the user, NMaaS represents a success story that can easily be adapted for different uses and host any type of applications turning into a generalised PaaS solution.

References

[CDT] McKinsey Digital, *How CIOs and CTOs can accelerate digital transformations through cloud platforms*, September 2020, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms

[DEL] GN4-3 D6.6 *Transforming Services with Orchestration and Automation*, November 2020, https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D6.6-Transforming_Services_with_Orchestration_and_Automation.pdf

[DOR] Docker Registry, https://docs.docker.com/registry/

[GIL] GitLab, https://about.gitlab.com/

[HEL] Helm, https://helm.sh/

[HER] Helm Repository, https://helm.sh/docs/topics/chart_repository/

[KUB] Kubernetes, https://kubernetes.io/

[NGP] Łukasz Łopatowski, NMaaS GÉANT production service, GÉANT NMaaS Infoshare, November 2020, https://wiki.geant.org/download/attachments/133762699/20201125%20-%20NMaaS%20Infoshare%20-%20Geant%20production%20service.pdf?version=1&modificationDate=1607550102651&api=v2

[NMC] Łukasz Łopatowski, NMaaS concept, architecture and deployment, GÉANT NMaaS Infoshare, November 2020, https://wiki.geant.org/download/attachments/133762699/20201125%20-%20NMaaS%20Infoshare%20-%20Concept%2C%20Architecture%20and%20Deployment.pdf?version=1&modificationDate=1607550062984&api=v2

[NMI] Pavle Vuletić, NMaaS Introduction, GÉANT NMaaS Infoshare, November 2020, https://wiki.geant.org/download/attachments/133762699/20201125%20-%20NMaaS%20Infoshare%20-%20Introduction.pdf?version=1&modificationDate=1607549938984&api=v2

[NMP] Łukasz Łopatowski, NMaaS Application Portfolio, GÉANT NMaaS Infoshare, November 2020, https://wiki.geant.org/download/attachments/133762699/20201125%20-%20NMaaS%20Infoshare%20-%20Application%20portfolio.pdf?version=1&modificationDate=1607550087719&api=v2

[NMS] GN4-2 D8.7 *Network Management as a Service Production Service*, May 2018, https://www.geant.org/Projects/GEANT_Project_GN4/deliverables/D8.7%

	20Network%20Management%20as%20a%20Service%20Production%20Service.pdf
[NMW]	NMaaS Home, https://wiki.geant.org/display/NMAAS/NMaaS+Home
[ODA]	TM Forum, GB998 Open Digital Architecture (ODA) Concepts & Principles v2.1.0, March 2021, https://www.tmforum.org/resources/reference/gb998-open-digital-architecture-oda-concepts-principles-v2-1-0/
[PRM]	Prometheus, https://prometheus.io/
[PRO]	Proxmox, https://www.proxmox.com/en/
[RAN]	Frédéric Loui, RARE @ NMaaS, GÉANT NMaaS Infoshare, November 2020, https://wiki.geant.org/download/attachments/133762699/20201125%20-%20NMaaS%20Infoshare%20-%20Demonstration.pdf?version=1&modificationDate=1607550149305&api=v2
[SSP]	Shibboleth SP, https://wiki.geant.org/display/eduGAIN/How+to+set+up+a+Service+Provider+for+eduGAIN
[UTR]	UpTimeRobot, https://uptimerobot.com/

Glossary

API	Application Programming Interface
CI/CD	Continuous Integration / Continuous Deployment
DB	Database
DCN	Data Communication Networks
DNS	Domain Name System
GUI	Graphical User Interface
IP	Internet Protocol
KPI	Key Performance Indicators
NMaaS	Network Management as a Service
NREN	National Research and Education Network
OAV	Orchestration, Automation and Virtualisation
ODA	Open Digital Architecture
PaaS	Platform as a Service
PLM	Product Lifecycle Management
RARE	Router for Academia Research Education
SSH	Secure Shell
UI	User Interface
VPN	Virtual Private Network
WP	Work Package