Network Management as a Service

Łukasz Łopatowski
GN4-3 WP6 T3 / NMaaS Team

18th STF, Copenhagen, 22 October 2019

www.geant.org
Why do we need NMaaS?

The cost and complexity of developing and integrating in-house network management may be too high for many NRENs and Institutions.

Out-of-the-box solutions might not be suitable and might be costly.

NMaaS aims to support these users to provide an effective, efficient network and service management platform.
What NMaaS offers?

NMaaS simplifies intra-domain network management by providing the infrastructure and tools for building a cloud-based, network management system.

It enables management and monitoring of client networks through on-demand deployment of network management tools in the cloud infrastructure.

Using a multi-tenant approach, each NREN or Institution has private access to their network and services from a highly available cloud based platform.
Who is NMaaS for?

Small and Emerging NRENs
Campuses
Small Organisations / End institutions
Distributed research projects
Other teams within the GÉANT Project
How NMaaS works?

- NMaaS uses a secure shared cloud platform managed by the GÉANT Project
- Each user has an isolated tenant environment connected over a VPN to his network
- Users can deploy and access network management applications via a web portal
How can NMaaS be used?

Option 1: Organisation implementation

• Each organisation offers a platform for their participating institutions
• GÉANT Project co-ordinates development and standards and provides 2nd level support for the software usage

NMaaS instance in RENATER
How can NMaaS be used?

Option 2: GÉANT Project implementation

• GÉANT Project offers a centralised platform for participating NRENs and/or their institutions ("white labelled")
• GÉANT Project co-ordinates development, standards and provides the 1st and the 2nd level support for NMaaS use

https://nmaas.eu
NMaaS production instance (hosted in PSNC)

https://nmaas.geant.org
NMaaS test / playground instance (hosted in GÉANT)
Who is using NMaaS?

- **NRENs**
  - CYNET (with intent to offer the service to end institutions)
  - PSNC (distributed research infrastructure)
- **End institutions**
  - Franja Malgaja Primary School (OSFM) / ARNES
  - Friedrich-Alexander-University (FAU) / DFN
- **GÉANT Project Team**
  - PMP: Performance Measurement Platform (central servers and particular nodes)
NMaaS Architecture

NMaaS components

- **NMaaS Platform**: Tool deployment process
- **NMaaS Portal**: Web-based user front-end
- **NMaaS Tools**: Packaged applications

Goals

- Easy to install and use
- Easily extendable with more tools
- Federated login

Both tools and NMaaS components are run in Kubernetes

Secure connectivity provided by OpenVPN
NMaaS tool deployment process
NMaaS Tools Portfolio

Oxidized
LibreNMS
NAV
Prometheus
Grafana

Work in progress ...

perfSONAR

- esmond
- MaDDash
- pSConfig Web Administrator

Users can select the tools required for their purposes and create a customised toolset tailored for their network
Is NMaaS reliable?

• Kubernetes cluster
  • Node redundancy: 3x master, 8x worker and 2 route reflectors
  • In case of a worker failure services are spawned on different worker (minimum downtime)
  • NMaaS tools data kept in external persistent volumes

• Data stored in a CEPH cluster
  • Components redundancy: 3x monitor, 2x metadata server, 12x OSD (over multiple physical servers)
  • Data replication

• Backup strategy in place
  • Scheduled VM backups
  • Additional file and directory backups
NMaaS instance monitoring

- Infrastructure monitoring
  - VM level resource utilization
  - Ceph storage cluster available capacity
- Kubernetes cluster and services
  - NMaaS components availability
  - NMaaS tool instances availability
  - Service level resource utilization
- VM and Kubernetes service logs monitoring
  - Retrieval – Fluentd, Rsyslog
  - Parsing, analysis and visualization – Graylog (+ Grafana)
  - Storage – Elasticsearch

Prometheus Operator
- Prometheus
- Alertmanager
- Grafana

SIG-PVM presentation on Kubernetes and microservice monitoring
K8s monitoring: Cluster
K8s monitoring: Node / VM
K8s monitoring: Namespace / User
K8s monitoring: Ingress controller
Graylog ingress logs from PfSense

[DAILY] Visits per Country

[DAILY] Most Popular Endpoints by Customer

[DAILY] Response Codes

[DAILY] Most Popular vhosts

[DAILY] Hits by Customer

296.14
0.09
0.02
Is NMaaS secure?

• **Client-to-Site VPN** – secure user web-access to the UI of deployed NMaaS tools

• **Site-to-Site VPN** – secure data exchange between the devices being monitored and NMaaS tools running in the cloud

• **Routing and firewall** settings on a central PfSense Firewall VM

Set up based on domain name and IP addresses of monitored devices provided by the user
NMaaS VPNs setup

Virtual subnet assigned to customer 1 (152.158.101.0/24)

MetaLB

Pull-type applications
Exposed by the ingress controller

192.168.101.100

Push-type applications

PostgreSQL

192.168.101.101

Customer #1 equipment

10.1.0.1
10.1.0.2

Gateway for 192.168.101.0/24

VPN client VM
192.168.99.4 - VPN Subnet

Gateway for 192.169.101.0/24

192.168.31.200
192.168.99.5 - VPN

192.168.31.201
192.168.99.6 - VPN

10.168.31.0/24

Customer #1 clients

www.geant.org
NMaaS Site-to-Site VPN on the user side

Option 1

- Static route for NMaaS subnet and dedicated customer subnet
- On-Premise OpenVPN Site-to-Site Client
- Equipment #1 to be monitored
- Equipment #n
- Router (GW)
- NMaaS Infrastructure
- VPN STS Connection
- Packet originating from NMaaS will have a source IP in the 172.16.11.0/24 range.
- VPN Client Access Connection (Access only to web interfaces)
- Administrator workstation
More Information

Main GÉANT web page:
• geant.org/NMaaS

Contact e-mail address of NMaaS team:
• nmaas@lists.geant.org

NMaaS production instance:
• https://nmaas.eu
Your feedback is very welcome

- Other use cases?
- New tools?
- Additional features?

Would you like to try NMaaS out?

Any questions?
Thank you

Any questions?

Łukasz Łopatowski / PSNC
email: llopat@man.poznan.pl

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3). 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).