28-11-2022

GÉANT OAV Architecture Analysis White Paper

Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 2
Dissemination Level:	PU (Public)
Document ID:	GN4-3-22-86FF51

Authors:	Simone Spinelli (GEANT), Donal Cunningham (HEAnet), Eduardo Jacob (RedIRIS), Estela Carmona Cejudo (I2CAT/RedIRIS), Iacovos Ioannou (CYNET), Ivana Golub (PSNC), Jasone Astorga (RedIRIS), Kostas Stamos (GRNET), Maria Isabel Gandia Carriedo (CSUC/RedIRIS), Roman Lapacz (PSNC), 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 GÉANT network architecture to the TM Forum's Open Digital Architecture (ODA). This analysis is one of a series of such documents aiming to provide a standardised view of the components and implementations of orchestration, automation and virtualisation (OAV) within the community.

Table of Contents

Table of Figures

Executive Summary

This document maps GÉANT's current Operations and Business Support Systems (OSS and BSS) to the TM Forum (TMF) [TMF] Open Digital Architecture (ODA) [ODA] reference architecture to demonstrate the flexibility and the benefits that the ODA model offers.

A reference architecture like ODA supports the transition from traditional work organisation based on manual work and procedures to a model where services are automatically provisioned and orchestrated.

The mapping of the tools in use at GÉANT to functional blocks shows, how ODA can be used as a framework to understand architectures in situations where environmental complexity and independent growth have led to dependencies that are not easy to identify. This helps manage and guide the digital transformation process in complex organisations such as GÉANT and other Research and Education (R&E) entities.

1 Introduction

The GÉANT association manages the pan-European network that connects the National Research and Education Networks (NRENs) including all its services and projects [GEA].

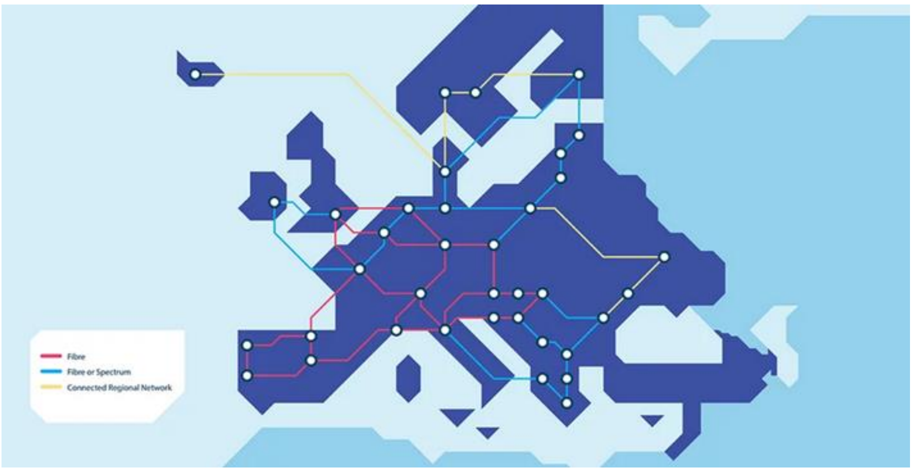

Figure 1.1: The GN4-3N Network [G3N]

GÉANT offers a broad variety of services that to its users [GAS]:

- Connectivity (e.g., Internet connectivity, R&E connectivity, dedicated L2 and L3 services, non-IP services)
- Trust and Identity (e.g., federated identity, virtual teams)
- Real time communications (e.g., EduMeet)
- Ad-hoc setups for specific projects that run on the network and on dedicated overlays built on top of it
- Virtual infrastructure for community projects and members

The non-profit nature of GÉANT Association, the Research and Education (R&E) context in which it operates, and the large community of users and peers contributing to projects, make for the extremely varied services, and the technologies used and built on top of the network. Thus, rather than supplying thousands of instances of a specific product to as many customers like a commercial service, GÉANT deals with a variety of highly customised bespoke services that change and adapt according to users' needs and requirements.

While in the past most of the service fulfilment was based on manual procedures, GÉANT has taken steps towards OAV architectures to facilitate the following aspects of the Open Digital Architecture (ODA) vision [ODAWP]:

- **Digital efficiency**: seeking to constantly improve the efficiency and scale of all core activities by incorporating automation in the network operation centres and focusing on enriched customer centric experience.
- **Digital enablement**: moving to digital platforms and digital ecosystems that bring together different vertical markets such as e-health, smart living, and manufacturing.

Naturally, these two drivers must be contextualised in the R&E environment, where digital efficiency can be translated to faster self-service service activation and increased predictability of changes, while digital enablement can be seen as the need to support more experiments and research activities, improved integration with cloud providers and so on.

In this document, the focus is placed on the GÉANT network services and the datacentre environment (virtual machines). Mapping current GÉANT architecture to ODA will help drive the process of digital transformation, in particular the adoption of an OAV architecture, by relying on a structured and holistic outlook that a reference architecture like ODA offers.

The main idea behind ODA is that of 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 a full end-to-end service lifecycle (including interoperability). The high-level ODA functional architecture maps the main components by their capabilities to ODA function blocks:

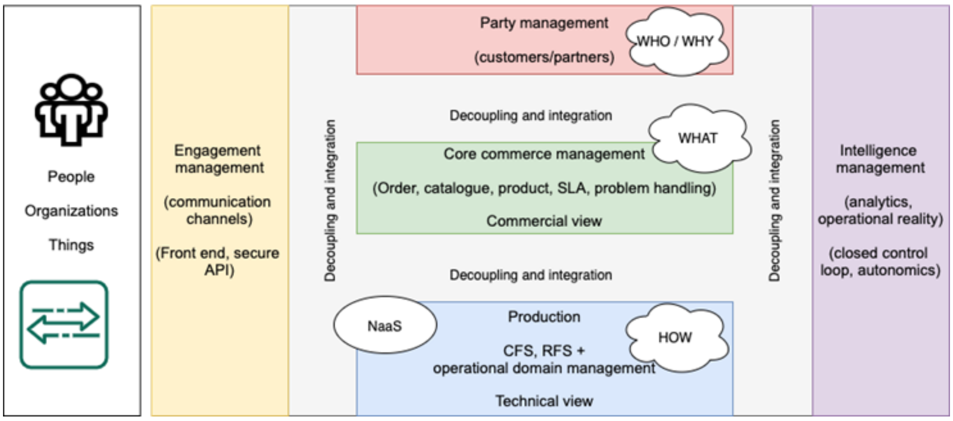

Figure 1.2: The TM Forum ODA functional architecture

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.
- **Decoupling and Integration** accentuates the separation of concerns between the functional blocks and serves as the glue between the functional blocks supporting interoperability.

2 Architecture Analysis

2.1 Goals and Requirements

At this point in time, GÉANT Association relies mostly on manual procedures and processes to deliver services, including network services. Manual execution affects predictability and quality, creating additional work to adjust inconsistencies after the work has been delivered.

However, the service providers' environment is moving towards a model where automated processes deliver complex services as a composition of small, well-defined building blocks. This enables scenarios such as self-service provisioning and on-demand services.

Introducing first automation and then orchestration in network service delivery will increase predictability in terms of speed and quality and will reduce the time to recover from incidents. Limiting (theoretically eliminating) the manual intervention from the service fulfilment processes makes it possible to introduce a self-service model, where GÉANT users will be able to self-provision network services. This is already possible for some network services such as L2 connections (using the GÉANT Connection Service (GCS)) and for IT resources such as virtual machines.

The goal is to extend similar mechanisms to the whole network fulfilment chain: from node provisioning/deprovisioning to atomic custom changes on specific service instances.

To achieve this goal, the main requirements for the implementation of an automated and possibly orchestrated service provisioning system are:

- A single source(s) of truth: rather than "network is king", the network configuration should be an instance of what is described in the inventory system(s).
- Data accessibility: data must be securely accessible from all departments of GÉANT Association. Using API and robust data models, information should be shared across the company and not replicated in non-authoritative domains.
- Automated management: services should be deployed using automated standard workflows. In this way, direct access to devices would, theoretically, be limited to complex troubleshooting only.

GÉANT IT already has some experience with the use of the Infrastructure as Code (IaC) [IAC] paradigm in the virtual environment, for the development of automated configuration management of virtual machines and related objects.

Infrastructure as Code represents the process of moving away from device configuration using command line interface or similar interactive tools, to taking advantage of machine-readable files that define the configuration and can be used to manage and provision physical or virtual objects in an automated way. The machine-readable files store the definitions of the required or expected configuration and are usually stored in a version control system so that they can be applied consistently.

This approach applies to virtual infrastructures, but can also be used to manage physical, bare-metal-based infrastructures such as GÉANT's backbone network.

2.2 Mapping to ODA Functional Architecture

This main aim of this document is to map GÉANT's current tools and functions to the ODA reference architecture. The figure below shows how GÉANT's components map to the ODA architecture functional blocks:

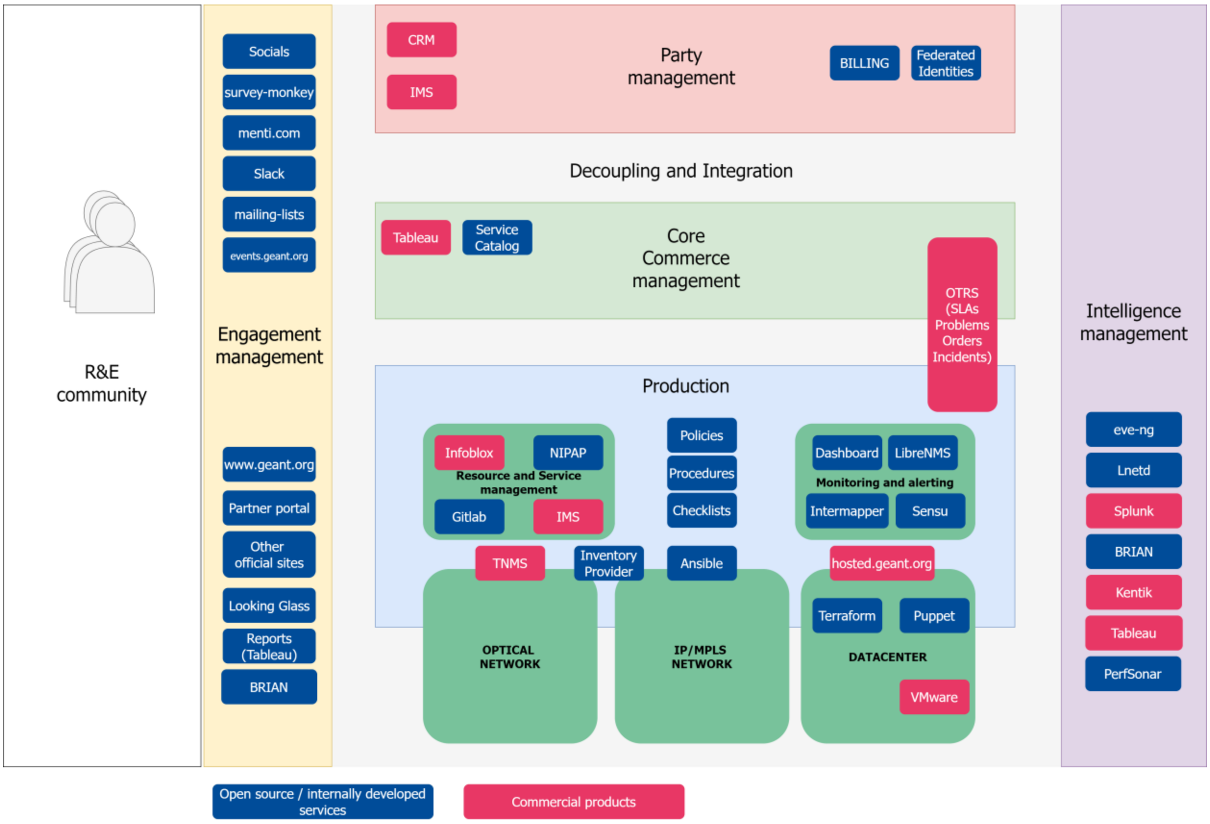

Figure 2.1: GÉANT OAV architecture mapped to TM Forum's ODA

2.2.1 Engagement Management

Engagement management is the functional block responsible for interactions with all internal and external parties.

While GÉANT is present on all the major social media platforms to advertise events and initiatives, a large portion of the communication with the GÉANT community happens through the Trouble

Ticketing System (TTS) currently based on the Open-Source Ticket Request System (OTRS) [OTRS], email, mailing lists, and Slack channels. To record user satisfaction, tools such as SurveyMonkey [SRVM] and Mentimeter [MNT] are used.

This block also maps to user facing GÉANT websites such as:

- https://www.geant.org
- https://tools.geant.org
- https://events.geant.org
- https://partner.geant.org

The list of tools used for user engagement is by no means exhaustive, as other tools are used for additional activities that are not the focus of this document. All the listed points of engagement work together with the continuous effort from the GÉANT team to coordinate virtual and real-life meetings to connect and coordinate the community on the multiple projects and initiatives that are running.

2.2.1.1 *www.geant.org*

The main official site of GÉANT Association contains information and links about projects such as GN4-3 [GN43], other network projects such as AfricaConnect3 [AC3] and Bella [BEL], Trust and Identity projects such as AARC [ARC] and REFEDS [REF], and collaboration projects such as UP2U [UP2], FED4FIRE [FED], etc. The website also provides a non-technical description of the services that are available to the GÉANT community:

- Connectivity and Network Management
- Trust & Identity and security services
- Cloud services
- Real time communication services (eduMEET)
- Professional services

Alongside social media newsletters and similar, the website is used to provide news about events and as the main public front-end of GÉANT Association.

2.2.1.2 *tools.geant.org*

This portal gives access to public tools that provide a view of the state of the GÉANT network. The main tools are:

- BRIAN: current interface statistics polling system
- Cacti: historical interface statistics
- Looking glass: a tool to execute routes lookup and connectivity tests from GÉANT routers.

Additional functionalities and information are provided after logging in to the Tools Portal, such as the option to query multiple routers using the Looking Glass, and access to the legacy monthly service reports.

2.2.1.3 *partner.geant.org*

This website is the main point of access for requesting new services, raising support requests, and checking the status of current subscriptions. The website also contains an instance of the service catalogue that describes GÉANT’s service portfolio.

2.2.2 Party Management

Party management is the functional block responsible for managing information about parties and authentication, authorisation, and accounting (AAA).

Currently, this function is replicated across multiple tools in different architectural blocks: addresses and supplier and Network Operations Centres' (NOCs') phone numbers are stored directly in the inventory management system, allowing the Operation Centre to reach out to technical partners in case of incidents and maintenance.

The teams responsible for partner relations have recently introduced a Customer Relationship Management (CRM) system (based on open-source Creatio [CRO]) where they collect information about parties such as which services they subscribe to, service feedback, proposals and similar.

Access to GÉANT services and resources, as part of AAA, is managed using federated identity. This service is managed by the Trust & Identity team.

The finance team is responsible for managing funding, billing, and payments. The nature of the GÉANT Association makes these operations quite delicate and complex: services that GÉANT offers are billed “per usage”, and managing all the different partners as well as the different suppliers in different countries while following EU regulations is very labour-intensive. Tools and procedures related to this aspect are out of scope for this document.

2.2.3 Core Commerce Management

The Core Commerce management functional block is responsible for product management which includes the product catalogue, inventories, configuration, and Service Level Agreements (SLAs).

These functions are currently replicated across multiple tools in different functional areas of the organisation: Partner Portal and CRM contain the service catalogue and its copy which are manually kept in sync, in addition to similar lists on various websites. Both tools store information about which services have been subscribed to by which partner, as does the Inventory Management System (IMS) used by GÉANT Operations.

Product specifications are stored as high-level designs in MS Word documents (stored on Box) and on Wiki pages which describe the more technical implementation and basic maintenance operations.

SLAs aspects are covered by the following tools:

- TTS takes care of tracking the SLAs for incidents and maintenance [OTRS].
- Tableau is used to present usage and global availability of services [TAB].

In addition, TTS is also the tool of choice for:

- Tracking orders, both externally (from partner portal, emails and similar) and internally (for example, capacity upgrades or requests for internal services).
- Managing problems.

2.2.4 Production

The production block encompasses all the functions needed for fulfilment and management of resources and services. For the purposes of this document, this block can be decomposed in 5 different sub-blocks:

- Resource management
- Monitoring and alerting
- Checklists
- Three technical domains:
  - Optical network - currently expanding and evolving to include a new generation of Reconfigurable Optical Add/Drop Multiplexers (ROADMs) and Data Centre Interconnects (DCIs)
  - Internet Protocol/Multiprotocol Label Switching (IP/MPLS) network based on Juniper MX routers
  - Data centre - a private virtual infrastructure capable of delivering virtual machines for multiple tenants.

2.2.4.1 *Resource Management*

The Inventory Management System (IMS) is a commonly used tool that sits outside any specific domain. It contains information about physical resources including routers, switches, servers and patch cables, logical entities such as VLANs, logical systems, and services. The IMS also contains administrative data such as of the contact details of NRENs, peers and suppliers [IMS].

The IMS is designed to work in a "PLAN->DISCOVER->RECONCILE" manner, which is particularly important in the development of the optical layer. All components like fibres, patches, devices, ports, frequencies, and similar are inserted into the database before they are deployed. The discovery phase queries the Network Management System (NMS) (or the routers directly, in case of the IP/MPLS network) and extracts the relevant information for the reconciliation phase where what has been discovered is compared with what is present in the database. At this point, it is the operator who takes the necessary actions to reconcile the information if necessary.

The IMS is used to correlate events between optical and IP/MPLS layers, and more in general, to analyse impact, i.e., understand which services are impacted if a component fails. For instance, all the services transiting on a particular link will fail if the link fails.

Previously, this function was fulfilled by OpsDB, an in-house developed software tool. However, as part of the GN4-3N project's network expansion, a new commercial software tool was acquired and rolled out. The IMS exposes a REST API that makes it more interoperable than direct SQL queries.

Besides the management of physical resources, there are also components for managing and keeping track of logical resources such as numbers and names:

- Domains and domain names
- IPv4 and IPv6 address space
- Other numbered resources like Route Targets / Route Distinguishers (RTs/RDs).

The Neat IP-Address Planner (NIPAP) is a network IP Address Management (IPAM) solution for IPv4/IPv6 address management and assignment, and it also keeps track of RT/RD in use [NIP]. For domains and domain names, Infoblox is used [INF].

Both of these tools expose their own APIs that can be used to interact with them and are currently used when deploying virtual machines on the virtualisation platform.

2.2.4.2 *Checklists*

Fulfilment of services can involve multiple teams and different layers in the network stack. The rollout of a new backbone link, for example, involves the coordination of remote operators to physically connect patches, turning on equipment, and configuring the router's interfaces with the correct Interior Gateway Protocol (IGP) metric. In addition, services must be correctly monitored and ready to be handed over from the implementation team to the NOC.

For this reason, checklists are in place to describe the workflow that must be followed to rollout every specific service. A single document describes all the high-level technical and documentation steps that are verified by the NOC to ensure quality requirements are met.

2.2.4.3 *Technical Domains*

The GÉANT network comprises three relevant technical domains:

- Optical network
- IP/MPLS network
- the network in the data centre

Optical network

The TNMS Network Management System (NMS) provided by Infinera covers all the aspects of node and service management in the optical technical domain [TNMS]:

- Monitoring and alerting
- Node inventory
- Service inventory

TNMS is used by the inventory management system to build the relationship between different layers in the network to allow the impact of a failure to be evaluated for all related services.

IP/MPLS network

The IP/MPLS is probably the most dynamic layer of the GÉANT network. Routers and links are added and decommissioned, and new configurations are deployed following the ever-changing needs of the community.

This is the main area that the current automation effort in GÉANT focuses on. The current approach Infrastructure as Code (IaC), where data and templates are stored in Git (YAML for data, Jinja2 for templates) and Ansible is used as an automation engine to interact with the network [ANS]. In addition, CI pipelines (with custom python scripts) ensure that at every commit the data is still valid and correct.

The configuration of a network element comprises multiple functional parts:

- Base configuration
- Service configuration
  - Resource-Facing Services (RFSs)
  - Customer-Facing Services (CFSs).

The base configuration includes all the configuration necessary to provision a new node and include it in the network. It covers aspects such as:

- Standard routing configuration for reachability of the node itself
- User access configuration and AAA
- Standard security/hardening related configuration
- Monitoring and event management

This configuration is generally the same across all the network elements or has specific values that depend on the node itself (for example, loopback address or hardware type).

The node deployment could be described as "One Touch Provisioning" where, once the node is reachable, the automation takes care of installing the entire base configuration and connecting the node to the rest of the network. Information needed to configure the node is retrieved from the authoritative sources:

- IP addresses from DNS
- Location from IMS
- Hardware configuration is discovered at runtime.

The process is managed via a Jenkins pipeline that calls Ansible playbooks to interact with the device [JNS].

Additional pipelines, playbooks, and templates are being developed to accommodate the provisioning and deprovisioning of the services in the GÉANT portfolio.

The next step would be to implement service orchestration where customer-facing services are implemented as a composition of smaller resource-facing services that are automatically configured using the IaC approach. This would allow the organisation to support agile dynamic service composition tailored to the user requirements.

Data centre environment

The data centre environment is based on VMWare, and hosts virtual machines for internal use and for the GÉANT Project. The data centre network is stretched over three different locations in Europe to facilitate geo-replication in case of disaster. Every location has shared storage (using VMware vSAN [SAN]) to allow in-service migration or relocation of VMs in case of maintenance or faults. From a security point of view, a distributed firewall based on VMware NSX provides basic filtering outside the VMs [NSX].

Configuration management is done using Puppet which is responsible for deploying services and configurations [PUP].

Internal VMs are deployed using Terraform [TRF] which rely on Consul [CON] as an inventory database. Terraform is responsible for instantiating VMs, and connecting to the VMware vCenter [VMC] which manages the entire infrastructure. It is also used for updating IPAM and DNS with IP information of the newly created VM. At the end of this process, the virtual machine is up and running with the basic configuration which enables it to connect to Puppet, and apply the roles that finalise the OS setup and deploy the necessary services for the specific instance.

Clusters and high available services are published using HAProxy, which uses DNS entries managed by Consul to select the healthy instances that can be inserted in the pool [HAP].

Users from the GÉANT project can request virtual machines on the same virtualisation platform using a frontend self-service interface based on Cloudbolt [CLB]. Users can choose between a “managed” and an “unmanaged” flavour. The former provides basic firewalling, automated system upgrades, and monitoring, while the latter gives more freedom and responsibility to the final user providing a system with basic configuration.

2.2.4.4 *Monitoring and alerting*

As part of service management, monitoring and alerting are key components to ensure that nodes and services are healthy, and to proactively react to faults and potential issues.

The different technical domains of the GÉANT network are monitored with different open-source tools. Virtual machines are monitored using Sensu [SEN] which is responsible for executing checks and shipping metrics to a time-series database based on InfluxDB [IDB]. The Sensu agent on the host to be monitored, connects to the Sensu server, NSX and subscribes for the checks to be executed. This provides auto-provisioning of nodes on the monitoring platform, making it very suitable for a fully scalable, fault tolerant environment.

Alerts are based on emails and Telegram [TLG]. In certain cases, the TTS [OTRS] incident is automatically opened so that operators and users already have a communication channel open.

In the optical network domain, TNMS checks the health of nodes and services, and sends out SNMP traps to the dashboard platform. The dashboard is responsible for collecting SNMP traps from the IP/MPLS layer (routers and switches). The dashboard system (internally developed and maintained) correlates alerts from different layers in the network, and summarises the fault to help the operator identify the root cause. The dashboard is also service-aware and generates the TTS ticket that alerts the users that are impacted by the fault.

In addition to the dashboard, which is primarily used for service-related faults, there is Intermapper [IMP] which is responsible for offering a weather map with basic health information about the network: an overview of the entire infrastructure in terms of the status of backbone trunks and external connections.

All network devices like routers, switches, console servers, are inserted in LibreNMS [LMS], an open-source SNMP Poller that gathers all relevant metrics such interface statistics, CPU and memory utilisation, temperatures, and power levels/consumptions. LibreNMS is also used for custom checks (based on Nagios-plugins), and it is the backend of Oxidized [OXD], a configuration backup system based on Git. This set of tools is replacing the legacy set based on Observium and Rancid.

The provisioning/deprovisioning of nodes from these systems is completely automated and based on the Ansible inventory as depicted in the following figure:

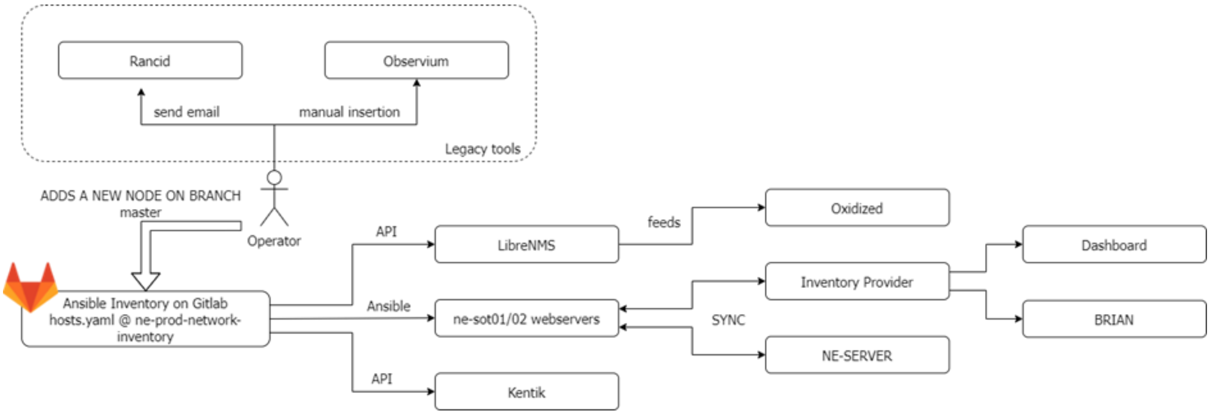

Figure 2.2: Automated process for provisioning/deprovisioning of nodes

Finally, event management is common to all domains. Every network device or virtual machine sends syslog messages to a Splunk cluster [SPL]. The platform is used for multiple purposes:

- Custom alerts based on log patterns
- Statistics and trends for day-by-day operations
- Security audits

2.2.5 Intelligence Management

The intelligence management block comprises the data analytics components which map event logs and metrics.

For event log management, two different platforms are used, Elastic [ELS] and Splunk [SPL]. While Elastic collects events from all virtual machines and applications hosted on the virtualisation platform, Splunk is used for event inspection, alerting, security audits, and to create specific availability reports, where this is required. Splunk is available to every component connected to the network:

- Routers and switches
- Optical network components
- Virtual machines and applications that are network related (automation / monitoring / network services)

For performance monitoring and capacity planning, BRIAN [BRN] is used. It relies on a time-series database that is based on InfluxDB for collecting the traffic metrics from network devices and systems. Grafana [GRF] offers dashboards for data visualisation and tooling for data manipulation to make it easier to aggregate and correlate metrics.

In addition to BRIAN, Kentik [KNT] is used to collect flows from GÉANT's routers and provide information about network utilisation, traffic distribution, traffic matrices, and capacity forecast.

Currently, the output of this functional block is key for capacity planning. The process is still largely manual and combines trends discovered by tools and human judgement. A more automated, software-driven version is currently being developed.

Tools for modelling and forecasting are also mapped in this functional area:

- EVE-ng [EVE] is used to simulate network topologies using virtual routers and infrastructure.
- Lnetd [LTD] is used to forecast traffic shift when links metrics are changed or when links are added or removed.

The NOC takes advantage of all monitoring systems and intelligence platforms to ensure that incidents are resolved quickly and efficiently, services stay within SLAs, and users are kept informed. The monitoring and intelligence management platforms are also used for network planning in activities like capacity forecasting and resource utilisation.

Most of the activities are largely manual, human-based processes. However, the introduction of automated configuration management and service deployment will facilitate troubleshooting by reducing inconsistencies and exceptions.

To help collate, analyse, and display information from various sources, including those detailed above, GÉANT uses Tableau [TAB]. Views and dashboards are generated for the benefit of internal GÉANT staff, NRENs and the European Commission (EC), in the form of the regularly updated Network Service Report (NSR), summary Monthly Service Report (MSR), and various views showing mostly static customer- and resource-facing service information. Future improvements will include integration with a federated IdP and a more automatic data refresh.

2.2.6 Decoupling and Integration

Although a large part of the GÉANT workflow is based on manual processes and procedures, everything is recorded in the Ticket Management System (TTS). For example, request fulfilment is tracked from the moment the service is requested until it is deployed and operational. In addition to the TTS, Jira [JRA] is used to manage the work of the software development team and track feature requests and bugs.

All communication between users and operators, and across different teams is tracked using the TTS. This is done for new deployments, updates, and incidents. From this point of view, the TTS carries out the role of decoupling and integration between all the different teams involved in the service deployment.

There are examples of orchestration, but they are limited to specific use cases (for example, provisioning VMs or new routers) and in general within a specific technical domain. The challenge is to extend this type of interaction to the entire organisation with standard and well-established data flows, endpoints, and APIs as suggested by the ODA model.

3 Conclusions

Based on the analysis of the GÉANT architecture, it can be observed that the ODA reference architecture is generic and flexible enough to accommodate mapping even in complex environments such as GÉANT's. Adapted and adjusted as it helps the organisation, it allows a more structured approach to the digital transformation process that many organisations, including GÉANT, are undertaking.

Using a common reference architecture for the entire organisation leads to a more holistic approach to the organisation's evolution, avoiding technical and organisational silos which are typical for complex, fast-paced organisations. From a community perspective, adopting a standardised approach helps communication and knowledge sharing, facilitating the creation and dissemination of common tools for well-defined and understood functions.

The digital infrastructure that GÉANT uses to manage its network contains elements that map to all functional blocks of the ODA. Several portals and tools are performing functionalities of the engagement management block, party management is performed through the CRM, federated identity and billing system, core commerce management includes service catalogue, and the OTRS system manages some functionalities of the production block. Three technical domains are relevant to GÉANT – the optical network, IP/MPLS, and the data centre. All have their individual and specific tools, but also the same approach towards long-term automation and orchestration goals. Intelligence management is well advanced as well, with an area for future work identified.

The main activities regarding automation in the GÉANT network are focused on the use of the Infrastructure as Code approach to standardising the configuration of different service components. New service instances are created by combining configuration templates stored in Git, and are then pushed to the network devices using Ansible. A similar approach has already been used successfully in the GÉANT virtual infrastructure.

There is a robust effort in the direction of orchestrated service delivery and automated networks. Applied within the organisational environment, the ODA reference architecture remains the main framework for creating and applying the automation strategy in GÉANT.

References

[AC3] Africa Connect 3, https://africaconnect3.net/
[ANS] Ansible, https://www.ansible.com/
[ARC] AARC project, https://aarc-project.eu/
[BEL] BELLA Programme, https://bella-programme.redclara.net/index.php/en/
[BRN] BRIAN - Backbone Router Interface Analytics, https://connect.geant.org/2021/07/07/welcome-brian-backbone-router-interface-analytics
[BRN] BRIAN https://public-brian.geant.org
[CLB] CloudBolt, https://www.cloudbolt.io/
[CON] Consul, https://www.consul.io/
[CRO] Creatio CRM, https://www.creatio.com/
[ELS] Elastic stack, https://www.elastic.co/
[EVE] EVE-NG, https://www.eve-ng.net/
[FED] Federation for Future Internet Research and Experimentation, https://www.fed4fire.eu/
[G3N] GÉANT Network, https://network.geant.org/gn4-3n/
[GAS] GÉANT Services, https://geant.org/services/
[GEA] GÉANT Association, https://about.geant.org/
[GN43] GN4-3 project, https://geant.org/projects/a-european-success-story/
[GRF] Grafana open observability platform, https://grafana.com/
[HAP] HAProxy, http://www.haproxy.org/
[IAC] Infrastructure as a Code, https://www.ipspace.net/kb/tag/network-infrastructure-as-code.html
[IDB] InfluxDB Open Source Time Series Database, https://www.influxdata.com/
[IMP] Intermapper network monitoring software, https://www.helpsystems.com/products/network-monitoring-software
[IMS] Inventory Management System, https://valid.com/what-we-do/iot-and-track-trace/ims-inventory-management-system/
[INF] Infoblox, https://www.infoblox.com/
[JNS] Jenkins, https://www.jenkins.io/
[JRA] Jira, https://www.atlassian.com/software/jira
[KNT] Kentik, Network observability, performance and security, https://www.kentik.com/
[LMS] LibreNMS, https://www.librenms.org/
[LTD] Lnetd, dynamic network topology from IGP information, https://github.com/cpmarvin/lnetd
[MNT] Mentimeter, https://www.menti.com/

[NIP] NIPAP open- source IP address management, https://spritelink.github.io/NIPAP/

[NSX] VMware NSX, https://www.vmware.com/products/nsx.html

[ODAWP] TM Forum IG1166 ODA Architecture Vision R18.0.0, https://www.tmforum.org/resources/standard/ig1166-oda-architecture-vision-r18-0-0/

[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/

[OTRS] Open-Source Ticket Request System OTRS, https://otrs.com/

[OXD] Oxidized, https://github.com/ytti/oxidized

[PUP] Puppet Powerful infrastructure automation and delivery, https://puppet.com/

[REF] Research and Education FEDerations group, https://refeds.org/

[SAN] VMware vSAN documentation, https://docs.vmware.com/en/VMware-vSAN/index.html

[SEN] Sensu Observability pipeline, https://sensu.io/

[SPL] Splunk Data Platform, https://www.splunk.com/

[SRVM] SurveyMonkey, https://www.surveymonkey.com

[TAB] Tableau, https://www.tableau.com/

[TLG] Telegram Messenger, https://telegram.org/

[TMF] TM Forum, https://www.tmforum.org

[TNMS] Transcend Network Management System, https://www.infinera.com/products/infinera-transcend-network-management-system/

[TRF] Terraform, https://www.terraform.io/

[UP2] UP2U – Up To University, https://up2university.eu/overview/

[VMC] VMware vCenter, https://www.vmware.com/products/vcenter-server.html

Glossary

AAA	Authentication, Authorisation and Accounting
API	Application Programming Interface
BRIAN	Backbone Router Interface Analytics
BSS	Business Support System
CFS	Customer-Facing Service
CI	Continuous Integration
CPU	Central Processing Unit
CRM	Customer Relationship Management
DCI	Data Centre Interconnect
DNS	Domain Name System
EC	European Commission
EU	European Union
GCS	GÉANT Connection Service
IaC	Infrastructure as Code
IdP	Identity Provider
IGP	Interior Gateway Protocol
IMS	Inventory Management System
IP	Internet Protocol
IPAM	IP Address Management
IPv4	IP version 4 address
IPv6	IP version 6 address
IT	Information Technology
L2	Layer two – Data Link Layer
L3	Layer three – Network Layer
MPLS	Multiprotocol Label Switching
MS	Microsoft
MSR	Monthly Service Report
NIPAP	Neat IP-Address Planner
NMS	Network Management System
NOC	Network Operations Centre
NREN	National Research and Education Network
NSR	Network Service Report
NSX	Network Virtualization and Security Platform
OAV	Orchestration, Automation and Virtualisation
ODA	Open Digital Architecture
OpsDB	Operations Data Base
OS	Operating System
OSS	Operations Support System

OTRS	Open-Source Ticket Request System
R&E	Research and Education
RD	Route Distinguisher
REST	REpresentational State Transfer
RFS	Resource-Facing Service
ROADM	Reconfigurable Optical Add/Drop Multiplexer
RT	Route Target
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TMF	TM Forum
TTS	Trouble Ticketing System
VLAN	Virtual LAN
VM	Virtual Machine
vSAN	Virtual Storage Area Network
YAML	YAML Ain't Markup Language