Towards Autonomic Policy-based Network Service Deployment with SLA and Monitoring

G. Xilouris[*], S. Kolometsos[*], C. Parada[†], J. Bonnet[†], P. Stavrianos[‡], E. Kapassa[‡], M. Touloupou[‡], D. Kyriazis[‡], P. Gouvas[§], E. Fotopoulou[§], A. Zafeiropoulos[§], F. Vicens[¶], J. Martrat[¶], P. Alemany[‖], R. Muñoz[‖], and R. Vilalta[‖]
[*]NCSRD, Greece
[†]ALTICE LABS, Portugal
[‡]UNIVERSITY OF PIRAEUS, Greece
[§]UBITECH, Greece
[¶]ATOS, Spain
[‖]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Spain
ricard.vilalta@cttc.es

***Abstract*—Unlike previous generations, 5G will need to be faster, more efficient, reliable, flexible, agile, and, at the same time, cost less. For this to be possible, 5G has to engage with the best-of-breed of the emerging technologies, where NFV is definitely in the top list. In this context, this paper describes the SONATA Service Platform, an open source MANO framework extended in the scope of the 5GTANGO H2020 project. In particular, this demo presents some features that go beyond the state-of-the-art including Monitoring, Policy, and SLA Management.**

***Index Terms*—Network Slicing, planning, (re-)optimization, 5G, SDN/NFV, DevOps, SDK.**

I. Introduction

ETSI ISG NFV [1] standardization group has significantly progressed in defining a comprehensive framework for the virtualization of network functions (VNFs) and network services (NSs). At the same time, proof-of-concept (PoC) activities have shown the impact fostered in the telecom market. Moreover, ETSI NFV has promoted PLUGTEST events, with the purpose of allowing vendors and open source NFV providers to validate their interpretation of the NFV standards, as well as to assess their interoperability levels. The implementation landscape is continuously evolving, in particular, in the Management and Orchestration (MANO) dimension. ETSI hosts the development of an open source tool called OSM (Open Source MANO). Other open source implementations have also gained some momentum. Recently, ONAP (Open Network Automation Platform) got some highlight.

5GTANGO 5GPPP Phase2 project has taken the open source software SONATA Service Platform, which has been prevously demonstrated at [2]. In this demo, we present the novel SONATA 4.0 release, and we demonstrate its new enhanced features with special dedicated focus towards Monitoring, Policies and SLA Management.

II. SONATA Service Platform architecture

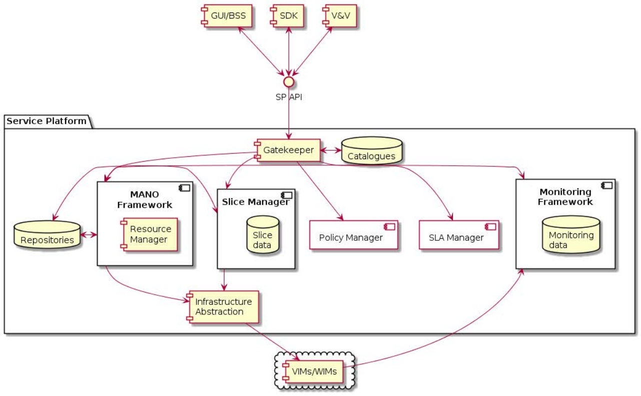

Fig. 1. 5GTANGO Service Platform high-level architecture

The SONATA Service Platform (SP) architecture (see Fig. 1), provides the service and function orchestration features, plus all the needed complementary and supporting features, like monitoring, policy and SLA management, user access management and infrastructure abstraction. The complementary features enhance the existing solution, as well as better support the vertical industry (e.g., automotive, e-health,...) requirements.

The SP interacts with OSSs/BSSs of the platform owner. The entry point of the SP is the Gatekeeper, controlling who tries to access the platform and the privileges. Assets submitted to the platform by authenticated and authorized users are stored in a Catalogue for future use. When there is a service instantiation request (or any other kind of request that affects the service instance life-cycle), the Gatekeeper forwards to the MANO Framework all the necessary data, which instructs the Infrastructure Abstraction for the required resource allocation at the Virtual Infrastructure Management (VIM) and WAN Infrastructure Management (WIM) levels. A successful request will store those records in the Repository.

Monitoring Framework provides the developer of the service or function with streams of monitoring data of relative short duration or alerts, which allow to better trim the service or function he/she owns. This effectively closes the loop, from service and function on-boarding to performance analysis, allowing for the quick iteration of updated services and functions versions, a flexibility that is key in 5G ecosystems.

Policies consider deployment and operational aspects of network services over programmable infrastructure [3]. Deployment policies regard the production of an optimal deployment plan, taking into account the set of constraints and objectives, as they are defined on behalf of network services developers and network services providers. Operational or runtime policies regard the run-time adaptation of network service mechanisms, in order to optimally support the overall performance achieved. The main objective of the introduction of policies management within the SONATA SP is the injection of intelligence in the various orchestration mechanisms.

To enable the provision of a NS with the corresponding quality requirements, SLA management should provide mechanisms to capture its network-related parameters, reflecting the corresponding quality levels. These may be included in policy rules as the Service Provider is able to modify them accordingly, through updating existing ones and enrich SLAs with additional parameters. High-level parameters (performance, availability, security) specified for the NS in an SLA, are linked to low-level requirements encapsulated in the respective policies [4] .

III. Proposed workflow

The proposed demonstration follows the explained steps:

1) Service on-boarding into the production SP: A developer uses SP API to on-board the newly created package.

2) Define Service Level Agreements (SLAs) : Operator can define the customer facing characteristics of the services, in particular the SLAs. Several Templates might be created, such as resilience over 1min/24h or over 1min/6h. Finally, the SLA is uploaded to the Catalogue associated to that service;

3) Define Operator's Policies: A developer has created a set of VNFs and the corresponding NS. Within the provided VNF and NS descriptors, a set of conditions are detailed (e.g., if avg_CPU_usage > 50% then "high_CPU_notification") that lead to notifications during run-time. Such conditions can be related to infrastructure resources (CPU) or software specific metrics (e.g. cache_hit_ratio). The objective is to provide a collection of insights during run-time.

Service Provider designs Policies for services. During this process, the information provided by the descriptors is used, as well as exploited his internal knowledge of the programmable infrastructure capabilities within the Service Provider's network. Thus, the objective of service provider is to achieve the provision of the NS with the desired QoS, while in parallel achieve optimal management of the infrastructure resources. Finally, once a Policy Descriptor is created, it is validated and uploaded to the Catalogue.

4) Assign a default and SLA-associated policies to a service: Service Provider is responsible to assigned SLA-associated and/or default policies to services. When a service is instantiated, and the customer associates an SLA (e.g., gold or silver SLA), the policy associated to this particular SLA is applied. In case no SLA-associated policy exists for that SLA, the default policy is applied. If there is no default policy, none is applied.

5) Service instantiation request: A customer logged in the Service Platform and is able to request a network service with Premium characteristics.

6) Service availability notification: Once the service is ready to be used, the customer is notified in the Portal. Service instantiation data (e.g. service IP address, management IP address, etc.) will be made available in the Portal;

7) Service usage: The customer starts using the service. While the service instance is running, monitoring data is collected and stored. Thresholds defined for the monitoring parameters are checked. Run-time Policy conditions are evaluated and actions triggered in case required.

8) Service Scaling-out: The user Increases the generated traffic through the network service. The SP checks Policy actions and triggers the scale out of the network service. Finally, SP checks that new resources are there.

9) Service SLA Violation: The SP is able to check an SLA violation, such as an interruption of the service.

10) Service Termination: The customer is able to terminate the service.

IV. Conclusion

We are adding a significant amount of features to the SONATA Service Platform results, which we think are key differences both in enriching 5GTANGO's software assets and in bringing them closer to the real world where these issues of validation and verification of network functions and services, Service Level Agreements, Policies Management and Monitoring are becoming the cornerstones of products and services that are ready for 5G. Our work improves SONATA Service Platform (powered by 5GTANGO) release, and it makes a relevant actor in the 5G ecosystem.

The presented demo reveals all the complex interactions that allow the stakeholder to inter-wind in order to move a Network Service concept to the production environment to be deployed by the Service Platform. Moreover during operation the Network Service is being monitored end-to-end by the SONATA hybrid monitoring framework.

Acknowledgment

This research has been partly funded by Spanish MINECO project DESTELLO (TEC2015-69256-R) and EC H2020 5GPPP 5GTANGO (H2020-ICT-2016-2 761493).

References

[1] ETSI ISG, "Network Functions Virtualisation (NFV); Architectural Framework," ETSI, February 2014, Tech. Rep.

[2] T. Soenen, S. Van Rossem, W. Tavernier, F. Vicens, D. Valocchi, P. Trakadas, P. Karkazis, G. Xilouris, P. Eardly, S. Kolometsos *et al.*, "Insights from sonata: Implementing and integrating a microservice-based nfv service platform with a devops methodology," in *NOMS2018, the IEEE/IFIP Network Operations and Management Symposium*, 2018, pp. 1–6.

[3] P. Gouvas, E. Fotopoulou, A. Zafeiropoulos, and C. Vassilakis, "A context model and policies management framework for reconfigurable-by-design distributed applications," *Procedia Computer Science*, vol. 97, pp. 122–125, 2016.

[4] E. Kapassa, M. Touloupou, A. Mavrogiorgou, and D. Kyriazis, "5g & slas: Automated proposition and management of agreements towards qos enforcement," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2018.