Software Asset Management Approach in NFV Context

Anne-Lucie Vion[1,2](✉), Noëlle Baillon[1], Fabienne Boyer[2], and Noël De Palma[2]

[1] Orange SA, Paris, France
annelucie.cosse@orange.com
[2] Université Grenoble Alpes, LIG, CNRS, Saint-Martin-d'Hères, France

Abstract. The relation between network software vendors and service providers is deeply changing due to a confluence of economic, market, and technological factors. Software licensing is complex and may become a hindrance to the adoption of new transformative technology. In such context both service providers and network software vendors would be well advised to bet on trustworthy partnership, promoting emergence of Software Asset Management in such environments.

Keywords: Software · SAM · Licensing · NFV

1 Introduction

Many techno-economic drivers are currently converging to create a paradigm change in the design and operation of future telecommunications networks and services. These drivers encompass progress in Information Technologies (IT), pervasive diffusion of ultra-broadband access, commoditization and falling costs of hardware, and the maturity of virtualization techniques. Paradigm change includes Network Function Virtualization (NFV), a concept pushed by the industry to virtualize network equipment using generic-built hardware platforms, in order to reduce costs and increase network operation and performance efficiency/agility. The NFV concept separates network functions from the hardware they run on using virtual hardware abstraction, and attempts to virtualize entire classes of network node functions into building blocks that may be connected/chained together to create communication services. Alike, "Softwarization" is an overall techno-economic transformation impacting the design, implementation, deployment and operations of infrastructures, deeply integrating network nodes and IT systems. For both network functions and services, flexibility and agility of software is highlighted. This transformation enables new architectural models along with an automation of operational processes. All these considerations question a new dimension of network management: as software becomes omnipresent, we assume that software license's management in real-time and on large-scale cloud environments will sophisticate Virtualized Network Function (VNF, or Network Software) onboarding processes.

A. Yang et al. (Eds.): SERVICES 2018, LNCS 10975, pp. 145–154, 2018.
https://doi.org/10.1007/978-3-319-94472-2_11

Network virtualization and softwarization lead to a disruption in terms of software licensing business model; thereby, we develop in this article the necessity to adopt existing and relevant software license optimization (SLO) IT process. We do believe that this experience and expertise acquired from IT will facilitate this NFV turn. In other words Software Asset Management (SAM), as defined by ISO (19770-1) [1] should play a major role in defining best practices the network industry could follow. The contributions are as follows: (i) we question the emerging contractual relation trends between service providers and network software editors, (ii) we argue that SAM is necessary in NFV environments and (iii) we propose a SAM prerequisite approach for NFV environments. The remaining of this paper is organized as follows. Section 2 presents a synthesis about the state of the art and discussion about VNF provider's position; Sect. 3 discusses convergence with IT SLO approach. Section 4 presents our proposition for a VNF's license management model, we conclude in Sect. 5.

2 State of the Art

2.1 Context and Literature

Manzalini [2] states that NFV principles are going to impact not only the evolution of current networks, but also the services and applications platforms running on them. The paper argues that, in this evolution, the border between the networks and the Cloud-Edge Computing platforms will gradually disappear. As well, the distinction between the networks and the future "terminals" (i.e., devices, smart objects, drones, and robot) will blur, raising a need for using Software Asset Management facilities in virtualized network environments.

From Matsumoto [3], the promise of NFV is to move network functions out of specialized appliances onto off-the-shelf servers, with the intent of both saving money and gaining in time factor. The paper recalls that the normal process of installing new gear for new services can take weeks. Jones [4] stresses that NFV can shrink that process down to minutes as it is promising agility and flexibility. The paper also mentions that many challenges are involved in deploying and operating a cloud-based NFV platform regarding software licence management.

Contreras [5] argues that virtualization and dynamic "on-demand" services bring new challenges for traditional network ecosystems that are used to have license keys to enforce entitlement. In NFV, virtualization eases "copy/distribute/run" applications and software. Especially, VNFs have a passing lifecycle and are not typically locked to a physical host. Having available licenses keys at the right time and place drives administrative costs for a global distributed cloud system such as a NFV infrastructure.

Adler [6] underlines that VNF software vendors have relationships with NFV service providers, who, in the long run, need to integrate with the vendor platform. By convention, VNF vendors have been selling their VNF products directly to service providers. For the latter, there is a need for homemade or third-party integration and bundling of VNF products together to reduce operational expenses and/or engineering expenses. For some it would be advantageous to have a pluggable framework for a cloud-based NFV system allowing integration of VNF products to provide a diverse catalog of VNF services in an integrated manner. As an example Jones [4] proposes a dynamic licensing method, implemented in an integrated system, including a third-party application; an exchange of private/public keys transiting through the integrated system validates the validity of the application's license key, determining whether to run the application.

2.2 This Context Justifies Reinforcement of SAM

From Vion [7], SAM enables tracking software uses with the finest possible granularity. The aim is to constantly reconcile the real uses with the usage rights acquired from software providers in order to optimize and control the risks of non-compliance (i.e., counterfeiting). The current economic climate underlines this particularly burning issue, as each non-compliance situation is heavily penalized in financial aspects. This change from traditional architectures to cloud environments, virtualized to the extreme, is still a virgin territory. Cloud environments add many degrees of complexity. Among others, tracking software becomes more challenging because installation is disconnected from true physical infrastructure. Altogether, the complexity of software lifecycle management, the multiplication of actors in this cycle and the lack of efficient tools, lead to an understandable disconnection between software usages, associated hardware and the related licensing model. Also, because cloud environments tend to automate software lifecycle management, SAM processes are expected to be integrated and automated as well. On the contrary, automation is currently circumscribed to asset management in traditional architecture.

Going further, in NFV environments, SAM is not only assets management, but also service management, which must be done in real time taking into account the fast rhythm of changes: services are provisioned, configured, reconfigured and terminated, retired in a matter of minutes. Compliance risks are increased by the ease and speed of provisioning, which can bypass traditional centralized processes. In such conditions, SAM controls are challenging to implement.

3 Adapting SAM to NFV

3.1 Convergence Between IT and Network

NFV architecture separates software purchase decisions from hardware decisions by splitting closed appliances into separate hardware and software components, enabling independent selection of each. Until now, service providers had almost exclusive relations with hardware big vendors (licensing based on invariants such as chassis ID, etc.). They have been accustomed to this sort of comfortable situation. First steps towards NFV force them to take ownership of their own stack.

Temptations exist to keep old habits instead of starting a new NFV initiative which will probably cost more than promoting dedicated resource management process. Many service providers have deployed Proof of Concepts (PoC) use cases (vIMS, vEPC, vCE, vCDN, …) in this network function virtualization software but few have the all needed operational tools in place to orchestrate and manage VNF from multiple vendors.

ETSI MANO standards and Open Source initiatives (i.e., OPNVF, OpenMANO, and ONAP) will help service providers in moving toward real implementations. Nevertheless, from Open Source Mano [8], The Linux Foundation [9], OPNFV [10], nothing is easy and complexities of licensing have to be addressed specifically: while service providers and VNF suppliers have different interests to defend in this aspect the value creation for each of them is generated from their collaboration and interdependency. The firsts want to pay as little as possible and only for what they are using, only when they are using it, with the smallest impact on VNF-onboarding process and no service disruption. The seconds need to plan their business and claim they have to protect intellectual property rights (IPR). Basically, Service providers have interest to promote a usage-based licensing (habitual model in IT), in other words, licensing models with fees that vary with uses, “uses” encompassing notions like time, bandwidth, packets, peaks, etc.

Figure 1 proposes to differentiate usage in three categories: allocation – supervision - consumption. Each variation might represent a metric (in that licensing meaning). *Allocation* covers resource configuration like virtual machine (VM) host, maximum allocated VM resources. It represents theoretical resource uses unlike *consumption* which encompass real resource uses, observed traffic, consumption of service, object, time, access. S*upervision* is not based on resources allocation or consumption but on the service ability to manage/create objects or services. Typically, an orchestrator use can be quantified by its amount of managed/created container. This usage distinction allows to link usages and licensing models and to forge a bond between the software licensing costs and service providers’ business value-added.

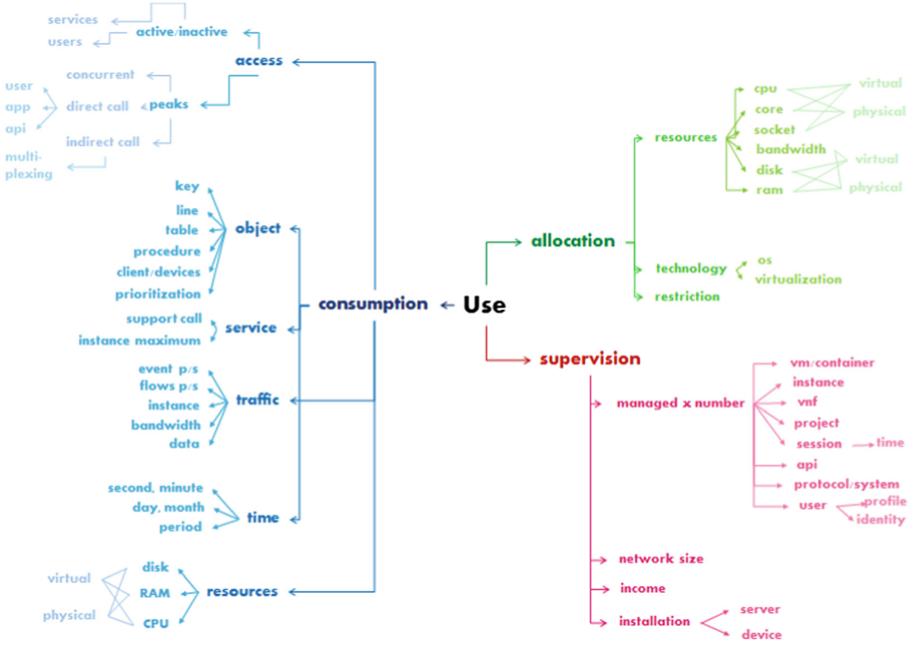

Fig. 1. Different measures of uses that could be translated in licensing model

Convergence with IT is clearly displayed by the emergence of new players that come with open source “DNA” and open source business model but also with IT inspired business models. Era of single vendor delivering turnkey solution is over and like in IT, service providers needs to integrate new technologies from different vendors. Main VNF supplier’s concerns are about Intellectual Property Rights (IPR) protection and revenue recognition.

IPR Protection. Licensing must meet service provider requirement while being easy to implement but preventing unauthorized use of the software. Network functions are virtualized and may run on different host hardware at different times, (e.g., elastic scaling). They may be easily cloned as part of regular operations like migration/backup but enable rogue employee or attacker running stolen software. Vendors want to prevent misuse to secure their IPR, but it comes with inconvenience: too much protection could be too inconvenient to use (i.e. service interference, legitimation of VM cloning, tie to specific hosts, extension to future applications, etc.). It implies that the responsibility of the license compliance fall back on Software vendors; just the same, regarding usage monitoring and control.

Revenue Recognition. VNF vendors propose to connect their license manager to business system to be able to recognize what to bill and consider as revenue. It questions about the vendor usage supervision legitimacy and might convey a business encroachment to the cost of service providers.

3.2 Accompany This Convergence in License Management

The fact is that since years, IT Software is mainly distributed on “declarative license” mode. In other words, during contracting phase, Software supplier trusts Software buyer and adjust negotiated license quantity on the amount of licenses that will be installed. Software installation and usage do not required interaction with any license manager because IPR protection is guaranteed by first clause of contract signed between Software vendors: *“This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.”* This clause quoted from a standard End-User License Agreement (EULA) proposed by Oracle [11], is nearly the same than clauses proposed by other well-known IT software vendors. These contracts are often jointly proposed with “True-up” process (Microsoft [12]): an annual reconciliation process through with you can increase or decrease your license subscription counts. Main benefit from this system is that customer keeps controls on what, where, when and how he deploys Software, processes his own allocated/consumed resource and asset optimization. It is translated into usage-based metrics like on Fig. 1.

Hard truth is that while NFV offers stronger partnership opportunities between service providers and Software vendors, first contracting methods do not reflect expected trust between partners. Trust is not a matter of technique, tricks or tools but of character and will.

Considering experience and process maturity on IT level, relation with software editors based on declarative license uses and perpetual usage rights seems to be the best approach to follow. Our aim is to replicate relevant software IT processes on production optimization as much as possible when relevant. VNF vendors can allow tremendous innovation and growth to telco industry, on condition that related software licensing is adapted to the service providers and do not stand in the way of fast onboarding of VNF.

4 SAM Implementation Strategies

The fact is that trust is built with consistency so: to turn into declarative license uses and perpetual usage rights, service providers need to have generic and reliable processes and tools to demonstrate their audit-readiness and accurate counting loop. It involves setting up relevant SAM program which will first address the following prerequisites.

4.1 VNF Identification

In our previous works, Vion [7] we highlighted software identification problems and inadequacy of SAM market tools, especially because matching between information from contracts, usages and technical view is, at least, not easy. Yet, it is a prerequisite for all relevant SAM approaches that service providers should implement (see Fig. 2). These weaknesses have to be overcome first by establishing identification processes through all the software lifecycle.

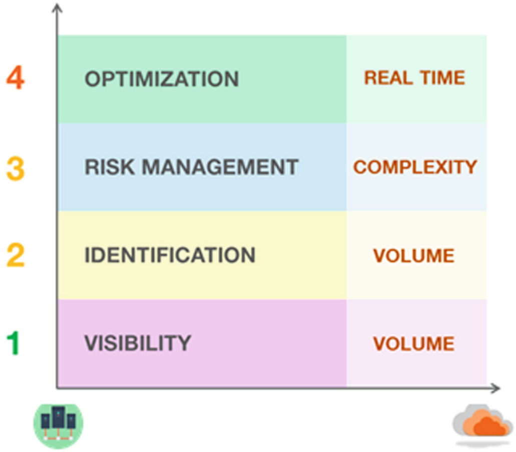

Fig. 2. SAM processes maturity scale

Identification consists in translating any resource in its associated assets. In other words, it translates software installation/Instanciation in terms of related licenses and products user rights. It can be identifying a product as a trial version or circumscribed to a particular scope; diagnose that it belongs to a software suite or that it is an option whose use is conditioned by the use of the basic product. It allows Risk management (consists in reconciling data. Namely, to compare product usage rights with real uses. Mainly, the aim is to prevent two kinds of risks: the first one is a legal one, counterfeiting, the second is a financial risk, over-deployment) and Optimization (mainly automation and real-time approach).

To achieve this, we propose to combine two well-known notions to facilitate a relevant SAM identification of VNF: Software Identification Tag (SWIDTag) proposed by (19770-2, 2015) and Stock Keeping Unit (SKU) widely used in retail.

SWIDTag records unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. The structure of SWID tags is specified in the international standard ISO/IEC 19770-2:2015 [13], which defines an XML (eXtensible Markup Language) data structure aiming to the precise identification of software.

SKU identify Software and its Product Usage Rights (PUR): to be informative, let's consider two vivid examples.

About SKU: On the shop's juice shelf, the same orange juice from the same producer can be sold in three different packaging: containers like a glass bottle, a can and plastic bottle. These three products containing the same juice will have three different SKU. But if we put three glass bottle of this juice in our basket, they will have the same SKU; it is not possible to find any difference between them. Making a parallel between Software and Juice: Software is the content (Juice), and Product Usage Rights are the packaging (PUR) (Bottle).

About PUR: Purchasing a train ticket (Thompson [14]). For the same journey, a myriad of options and variations and the price can vary significantly. Among others: the type of ticket (flexible or no), the time of the day (peak or off-peak), the class (first or cattle), age of customer (infant/child/adult), additional evidence (season ticket, student card, loyalty card). It is the same for the software industry, licensing provides options and flexibility, called PUR.

Combining these two notions by including SKU in the SWIDTag allows identifying software and its PUR with the highest accuracy. This combination is also key in allowing identification to be possible throughout the entire lifecycle of software. Therefore, from this proposition, the aim is that service providers become able to assess use compliance with contracts, and optimize Software usages.

4.2 Tracking and Controlling VNF Software

The previous proposition goes with tracking the complete lifecycle of VNF software in order to be able to track usages. Regarding this aspect, we firstly propose to consider the lifecycle detailed hereafter, composed of six main steps (some steps can be played several times):

Need's Expression (1). The consumer justifies his need and choice of software.
Purchasing (2). This step encompasses sourcing processes, negotiation, contract, billing etc. At this stage, we get a Stock Keeping Unit (SKU) identifying the purchased software and its own [product] usage rights (PUR) created by manufacturer and acquired during purchasing processes.
Delivery (3). This step corresponds to the software receipt via downloading platforms, preparation for installation on user platform, entry into a software catalogue. Through this step, we get a SWIG Tag containing the software's SKU created by the manufacturer and extendable with client-specific information. SWID tag will be the default software identifier.
Instantiation (4). Software is installed in an environment (for instance, a given Cloud), in other words, software is able to be used.
Usage (5). A user consumes a service/software. Here, we have to identify the cases where multiple users consume the same service simultaneously and translate this in terms of use (multiplexing, multi-device …).
Optimization (6). This corresponds to confronting the need/contract/installation/use with the license stock according to a measure of consumption previously defined (metric). Here we can create a model of costs for any measure of use and identify the most suitable scenario of consumption or of customer billing.

Based on this lifecycle, we propose that each step feeds a Software Database (SWDB). All possible information related with the use of software should be indeed captured and stored in order to implement all the required usage controls. Thus, at each step, one or more SAM control actions (that we call SAM check-points) are performed.

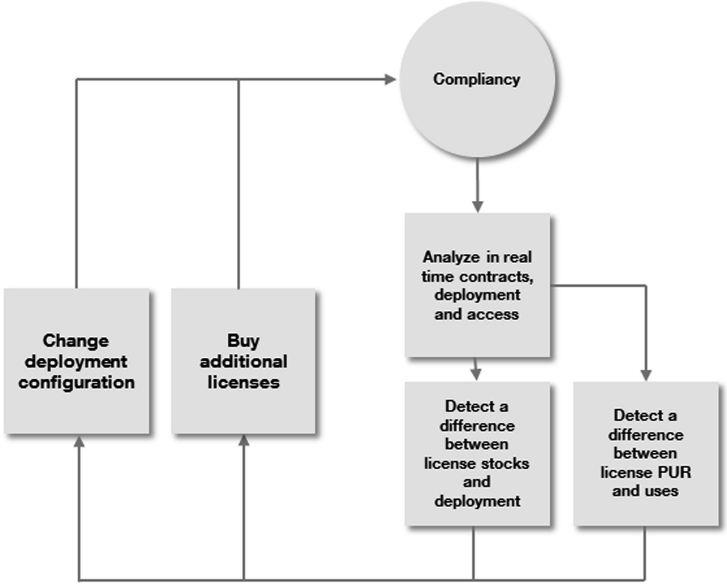
Compliancy
Analyze in real time contracts, deployment and access
Change deployment configuration
Buy additional licenses
Detect a difference between license stocks and deployment
Detect a difference between license PUR and uses

Fig. 3. Compliancy control loop

Through these check-points, the SAM processes analyze the current situation in real-time, confronting the use of services with the license stock. SAM processes also take potential optimization decisions, creating two control loops presented on Fig. 3 for compliancy check and Fig. 4 for optimal deployment purpose.

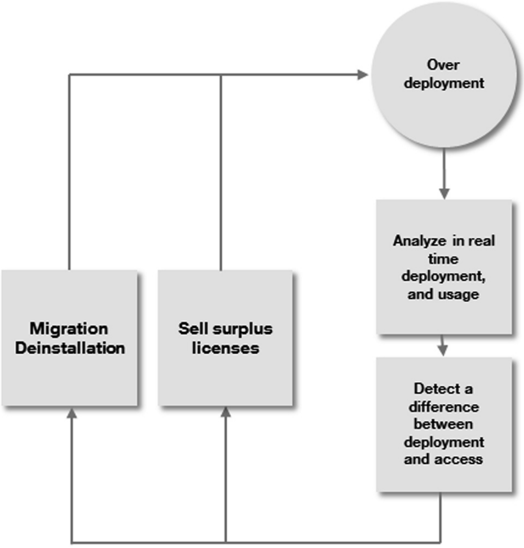
Over deployment
Analyze in real time deployment, and usage
Detect a difference between deployment and access
Migration Deinstallation
Sell surplus licenses

Fig. 4. Optimal deployment control loop

5 Conclusion

The power balance between software vendors and enterprise customers is deeply changing due to a gathering of economic, market, and technological factors. As a consequence, VNF Vendors have to redefine the terms and conditions of how they sell and price their products. They should take into account a new type of customer that judges software by its value-added to the organization, measuring where, when, how much, and how well software is used. This changing dynamic will have significant impact on how software is priced and what customers pay for, in addition to the software delivery mechanism. As well as in other industries, software vendors should adopt value-based pricing models that focus on customer demand and value perception and are directly linked to the customer's insight into how the software affects its business. In this regard, we argue that software licensing business should be based more than ever on trustful relations in order to allow durable partnership between service providers and network vendors and boost development and adoption of new technologies.

The approach proposed in this paper can be considered as a first step towards such direction. This approach leverages a mechanism for identifying software, and an associated model for tracking and controlling software usages. We believe this first step as valuable since software licensing is more than ever complicated, which may become a hindrance to the adoption of new transformative IT technology in the context of VNF.

As future work, we will propose and extended architectures to implement SAM during VNF on-boarding and monitoring of it whole lifecycle and quantitative evaluation of this implementation.

References

1. 19770-1 ISO Information technology: Software asset management - Part 1: Processes and tiered assessment of conformance. International Organization for Standardization, Vol. 1, ISO/IEC JTC 1/SC 7 Software and systems engineering (2012)
2. Manzalini, A., Gladisch, A., Kellerer, W.: Softwarization of telecommunications, Special issue: SDN and NFV. In: Revue: Information Technology, pp. 321–329 (2015). https://doi.org/10.1515/itit-2015-0025
3. SDX Central Homepage. https://www.sdxcentral.com/articles/news/ciena-turns-nfv-online-shopping-experience/2014/12/. Accessed 1 Apr 2017
4. Jones, R., Nguyen, P., Ciolfi, P., Meek, K., Nursimulu, K., Rahimi Koopayi, H., Wang, S., Barbarie, S.: Ciena Corporation Dynamic licensing for applications and plugin framework for virtual network systems. Patent: US20160226663 A1: Demande, US, 4 April 2016
5. Contreras, L., Doolan, P., Lonsethagen, H., Lopez, D.: Operational, organizational and business challenges for network operators in the context of SDN and NFV. Comput. Netw. **92**(Part 2), 211–217 (2015)
6. Adler, M., Enderwick, T., Koeten, R., Popp, N.: Systems and methods for identifying a secure application when connecting to a network. Patent: US20140282821 A1: Request, US, 18 September 2014
7. Vion, A.L., Baillon, N., Boyer, F., De Palma, N.: Software license optimization and cloud computing. In: Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Athens, pp. 116–121 (2017). ISBN 978-1-61208-529-6
8. Open Source Mano, An ETSI OSM Community White Paper. Technical Overview, Vol. OSM Release Two. Sophia Antipolis (2017)
9. The Linux Foundation, Harmonizing Open Source and Standards in the Telecom World The Linux Foundation (2017)
10. OPNFV, State of NFV and OPNFV, Study on “What Operators Think of OPNFV”, The Linux Foundation (2016)
11. Oracle License and Service Agreements. Oracle Homepage. http://www.oracle.com/us/corporate/contracts/license-service-agreement/license-service-agreement-070712.html. Accessed 8 Dec 2017
12. Microsoft License Review, Microsoft Homepage. http://www.microsoftlicensereview.com/?p=1159. Accessed 5 May 2017
13. 19770-2 ISO: Information technology – Software asset management – Part 2: Software identification tag. [s.l.]: International Organization for Standardization. Vol. ISO/IEC JTC 1/SC 7 Software and systems engineering (2015)
14. ITAM Review Homepage. https://www.itassetmanagement.net/2010/10/28/license-managers-learn-railways/. Accessed 5 May 2017