05-03-2015

Deliverable D12.1 (DJ1.2.1) Network Architectures for Cloud Services

Deliverable D12.1 (DJ1.2.1)

Contractual Date:	31-01-2015
Actual Date:	05-03-2015
Grant Agreement No.:	605243
Activity:	JRA1
Task Item:	Task 2
Nature of Deliverable:	O (Other)
Dissemination Level:	PU (Public)
Lead Partner:	CARnet
Document Code:	GN3PLUS14-976-38
Authors:	Damir Regvart (CARNET), Yuri Demchenko (UvA), Sonja Filiposka (MARNET), Migiel de Vos (SURFnet), Tasos Karaliotas (GRNET), Kurt Baumann (SWITCH), Daniel Arbel (IUCC), Cosmin Dumitru, Ralph Koning (UvA), Taras Matselyukh (Opt/Net)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No.605243 (GN3plus).

Abstract

This document describes the features and benefits of GÉANT's Open Cloud eXchange (gOCX) as a proposed architecture solution to run interactive data-intensive cloud applications on top of GÉANT so as to address the growing demand for cloud services within the R&E environment. Findings and lessons learned are presented based on two demo scenarios.

Table of Contents

Table of Figures

Executive Summary

The continued rise in the use of cloud computing means that there is also a growing demand for these services in the research and education (R&E) environment. This creates new challenges for National Research and Education Networks (NRENs) as additional strain is placed on their networks. A reliable high-performance networking infrastructure is therefore necessary to facilitate the delivery of cloud computing services to end-users in the R&E community.

A major goal of Joint Research Activity 1 – Task 2: Network Architectures for Cloud Services, was therefore to review the status of the network architectures for cloud services delivery and lay down the steps for the future evolution of the GÉANT and the NRENs as a composite cloud service delivery network offering high dedicated bandwidth and QoS.

The Task proposes as a possible solution the GÉANT's Open Cloud Exchange (gOCX), which brings together cloud service users from the R&E community with different CSPs by establishing direct L0-L2 connections on-demand between the users and the providers. Designed with power cloud users in mind, the main goal of the gOCX architecture is to provide dedicated infrastructure that will bring together the CSPs and users in an efficient, fast, reliable and cost-effective manner, facilitating intercloud computing federations.

It was considered that the use of gOCX would enable the establishment of: a) a dedicated network infrastructure, implemented on top of the GÉANT/NRENs infrastructure, for the provisioning of cloud services to members of the R&E community; b) a marketplace offering a CSP service directory; and c) a Trusted Third Party.

In order to test the implementation of the gOCX design for power user use cases, the Task developed two demo scenarios. It also began early-stage negotiations with different CSPs so as to obtain valuable feedback that would enable it to assess their interest in collaborating on the gOCX proposal, as well as to ascertain the level of complexity that a direct connection setup would involve.

For the first demo, a test scenario was defined and presented in real time at the TERENA Networking Conference, in 2014. The aim of this proof of concept was to present how the gOCX solution can provide a reusable network infrastructure that will deliver guaranteed QoS compared to the public Internet best effort connection alternative. The main benefit provided by the OCX infrastructure in this demo scenario is the use of dedicated links towards the CSPs that provide substantially improved data transfer performances between the clients and the CSPs. Furthermore, the use of multi-domain L2 services ensures traffic isolation.

The second demo scenario is an extension of the proof of concept, intended to introduce more participants in the demonstration, and involved multiple cloud service users from academic institutions that are connected to GÉANT via different NRENs. The results obtained confirmed the findings of the first demo scenario, establishing the setting for future, more complex scenarios.

Demo Scenario II was also presented at the 5th-Helix Nebula Assembly in Frascati (Rome) in November 2014, in order to introduce GÉANT's gOCX activities to the Helix-Nebula Partners. The HNA is working towards a "European Cloud Marketplace service" to operate in accordance with EU regulations and legislation, providing aggregation and provisioning of cloud services offered by commercial CSPs. These requirements could be met by gOCX, which is therefore considered as a potential candidate architecture for the HNX marketplace.

The two gOCX architecture demo scenarios presented above have confirmed a number of technical and non-technical benefits that would be derived from its implementation. The gOCX architecture will inherently create a broad community of public and academic CSPs directly connected to GÉANT.
This will result in short provisioning and implementation times for connecting to CSPs, facilitating the establishment of transparent connectivity between them and R&E institutions. Furthermore, by enabling direct connectivity, a number of additional performance enhancements can be implemented. gOCX will also allow the creation of a common marketplace where CSPs can present their offers, resulting in a competitive environment that will lead to increased service quality and/or price drops.

However, the demo scenarios have also highlighted how time-consuming and error-prone the task of manually setting up the required direct connection links is. This means that in order to truly harness the potential benefits of the gOCX architecture, the connection setup process should be automated. Currently, the most promising candidate technologies to enable this are Network Function Virtualization (NFV) and Software Defined Networks (SDN). Also, gOCX's role in facilitating integration of (multi-)provider and campus cloud infrastructures poses a number of security challenges that will need to be analysed and addressed.

1 Introduction

The continued rise in the use of cloud computing [NISTdef] to perform a variety of tasks and resolve different issues also affects the research and education (R&E) environment. This creates new challenges for National Research and Education Networks (NRENs), that need to satisfy the growing demands for cloud computing, which places additional strain on their networks. On the one hand, a great number of cloud users (e.g. R&E staff, students, and other customers) rely on the NRENs for connectivity to access publicly offered cloud services. Additionally, a number of academic cloud service providers (aCSPs) may rely on the NRENs for their data centre deployment and last-mile connectivity to their targeted users (encompassing the entire GÉANT/NRENs network). Another issue that is becoming increasingly important relates to the Intercloud scenario in the form of cloud exchange, peering or roaming based on the cloud computing reference architecture as defined by NIST [NISTarch], as well as on the Intercloud Architecture for Interoperability and Integration [ICAF]. However, another dimension of the Intercloud concept is becoming even more relevant –*Intercloud Operations* where the cloud user provisions combined (or joint) cloud services offered by different CSPs simultaneously.

Regular cloud users in the R&E community: (a) use mail and other similar applications provided by different SaaS cloud service providers (CSPs), or (b) are using the services offered by IaaS CSPs in order to create and work with a number of different virtual machines (VMs), or (c) design and develop new services offered in the cloud by leveraging the PaaS environment provided by the CSP. When involved in one of these use case scenarios, the typical NREN user will turn to the commodity Internet and best-effort service it offers. However, there are cases when the use of best-effort Internet is no longer sufficient to satisfy the demands of certain cloud users, such as, for example, *power cloud users* who demand high QoS and high dedicated bandwidth enabling secure and reliable connections, including to a number of different CSPs at the same time. Power users manage complex cloud services that involve transferring large amounts of data to and/or from the CSPs combined with a greater need for computing and storage resources, i.e. big data, analytic tools that work with high data volumes.

A reliable high-performance networking infrastructure is therefore necessary and will facilitate delivering services to end-users. The unification of the service edge with the data centre, the increasing role of network virtualization, and the growth of Software-Defined Networking all allow the development of a new flexible and agile framework for the delivery of services to users.

As a possible solution to the issues outlined above, Joint Research Activity 1 – Task 2: Network Architectures for Cloud Services, has proposed the GÉANT's Open Cloud Exchange (gOCX), that brings together cloud service users (users) from the R&E community with different CSPs by establishing direct L0-L2 connections between the users and the providers on-demand. The initial gOCX architecture and design issues were outlined in a whitepaper published by the Task [gOCX]. In this document, following

an overview of the gOCX concept, the setup and execution are presented of two demo scenarios that were implemented with the goal of: (a) discovering the possibilities, as well as the complexities, of the gOCX deployment in the GÉANT/NREN's network, and (b) learning how to best define the gOCX architecture in detail based on the results obtained. The benefits of using gOCX when connecting a power user with one or more CSPs, through point-to-multipoint connectivity, are also outlined. The results have shown that there is an acute need for automated interaction between all parties involved (users, OCX instances, CSPs) that will enable users to efficiently add and browse services, to instantly set up and release connections, etc. Therefore, the potential for a set of possible technologies that could be used to address this need is also discussed.

2 Cloud Service Delivery Networks

According to the NIST Cloud Computing Reference Architecture [NISTarch], all a cloud user needs in order to access and use cloud services is an Internet connection to the CSP. But is this so simple today? With many critical applications transferred to the cloud, Internet performance has become extremely important to users. The rise of cloud computing has increased the demand for broadband Internet connection to levels previously unexpected by network administrators. Cloud services must be accessible to users in a consistent and secure manner, anytime, anywhere. The traditional architecture that is based on routing Internet traffic through a limited set of Internet gateways entails performance and availability issues for cloud service users. With cloud computing, delivering applications to users is becoming more complicated and the network must perform appropriately in many different situations. In order to keep up with the current trend towards growth, cloud service delivery networks must adapt to meet the users' ever-increasing demands. The next generation of cloud delivery architectures will therefore include **cloud-ready networks** that will guarantee the performance of (un)critical cloud services, without sacrificing security.

In order to satisfy users' requirements, the service delivery infrastructure must guarantee Quality of Service (QoS), security and SLAs, while maintaining high-quality service performance and monitoring. As service providers move their data centres closer to their customers, the need for scalable, seamless and unified solutions to interconnect and deliver services to users takes on more importance. Scalable multi-tenant solutions aimed at providing high-performing service delivery are needed. Today's solutions are based on Layer 3 Virtual Private Routed Network (VPRN) [Affiniti] or Virtual Private LAN Services [VPLS] enabled via Layer 2 MPLS VPNs [Brocade].

The deployment of cloud services requires taking into account the network in its entirety, including the cloud data centre and the service delivery network connecting the data centre to the end users. The increased data consumption and bandwidth needs of power users are placing further pressure on current networks. Service providers that have their own service delivery network have an advantage as they can deliver cloud services via their WAN, providing end-to-end service-level guarantees. In addition they can leverage their geographic proximity to the end customer through their Point of Presence/Network Access Points to push content and latency-sensitive application services to the edge of their network, close to the customer. In cloud computing, the data centre is the service delivery point, therefore moving data centres to the service edges helps reduce backhaul and deliver latency-sensitive, interactive and location-based services. By decreasing the gap between the CSP and the user, one of the main challenges of the bandwidth-hungry cloud computing services of today can be alleviated.

In this context the GÉANT/NREN network clearly has great potential to undertake the role of cloud service delivery network both within the R&E community (for academic CSPs), and outside it (offering

high-performing service delivery for public CSPs). In any case, the increase in use of cloud computing in the R&E environment means that the need for the GÉANT network to take on this role will be inevitable in the near future. A major goal of the Task was therefore to review the status of the network architectures for cloud services delivery and lay down the steps for the future evolution of the GÉANT and the NRENs as a composite cloud service delivery network that will offer high dedicated bandwidth and QoS to their demanding cloud end users.

With this goal in mind, a fruitful communication was initiated with a number of CSPs, which in the case of Amazon Web Services (AWS), for example, resulted in the awarding of the Amazon Educational Grant [AWS], which has been an important step in the promotion of cloud computing and cloud-ready networks in the GÉANT/NREN R&E community. Much positive feedback has also been received from Microsoft Azure, CloudSigma, Kentis and Equinix. Another possible point of collaboration is the GÉANT Cloud Catalogue that provides a list of CSPs and their offers to the R&E community [GEANTCloudCatalogue]. All of these contacts have established the ground for further strengthening collaborations, especially with the CSPs that have also supported the idea of gOCX and participated in the demo scenarios (see Section 3).

3 Open Cloud Exchange Architecture

The gOCX architecture provides a response to the demand from the R&E community for federation-based cloud services with high-performance connectivity from campuses/labs to cloud resources and scientific data sources. Designed with power cloud users in mind, the main goal of the gOCX architecture is to provide dedicated infrastructure that will bring together the CSPs and the users in an efficient, fast, reliable and cost-effective manner, facilitating intercloud computing federations. In this context and hereinafter in this document, the term user (or end-user) is used to intend a power cloud user from an R&E organisation (e.g. group of big data scientists from a research institute) wishing to use one or more integrated cloud services.

gOCX [gOCX] is defined as:

- a dedicated network infrastructure, implemented on top of the GÉANT/NRENs infrastructure, that will be used exclusively for the provisioning of cloud services to members of the R&E community. Cloud Services provided over gOCX will be able to meet certain performance and quality metrics that are difficult to achieve with standard Internet access.

- a marketplace that offers:
  - a service directory, in which CSPs publish their services and users can discover and subscribe to services,
  - "connectivity as a service" via automatic link provisioning: users can setup connectivity on-demand (which in turn provides short "time-to-market"). gOCX does not implement the commercial part of the marketplace, it only provides the means for connecting users and service providers without concerning or trying to solve the problem of how the users will pay for the services,
  - an SLA Repository and Clearing house;

- a Trusted Third Party that can act as:
  - Certificate directory that facilitates dynamic federation service agreements,
  - Trusted introducer for dynamic trust establishment.

When deployed on top of the GÉANT/NREN network, the gOCX, as defined above, involves a hierarchical distributed system with OCX instances in multiple NRENs, and one or several OCX instances at the level of the GÉANT network, which are used not only for connecting CSPs, but also for orchestration and performance purposes. GÉANT Open Exchanges [GEANTOpen] can easily add the role of OCX instance. For example, the GÉANT Open in London could comprise one such GÉANT OCX point. The physical placement of the OCX instances is mainly determined by the geographical closeness to cloud users and providers in relation to the number of willing parties (CSPs or users) to

connect in that area. This means that any NREN close to the physical location(s) of one or more CSPs could host an OCX instance to which a given CSP could connect using a direct L0-L2 connection. Once a CSP is connected to at least one OCX, the services it offers can be used by the whole GÉANT/NREN community via the same OCX instance (for local users) or a different one (for remote users), depending on availability of necessary resources (ports and bandwidth). Any provider is allowed to connect to the OCX points. However, actual network usage is subject to policy restrictions defined by GÉANT as applicable at the time.

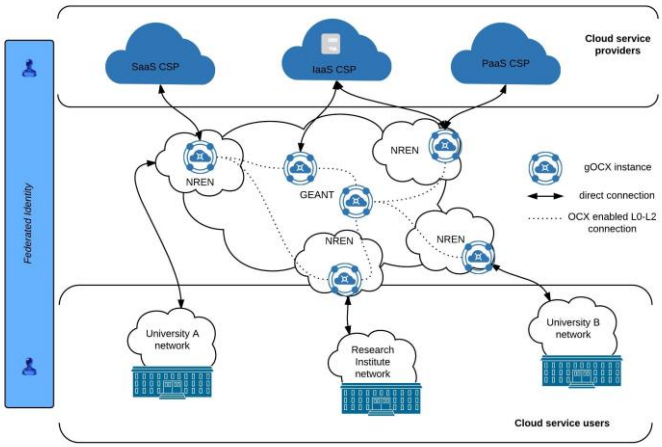

Figure 3.1:OCX instances deployed in NRENs and GÉANT connected to main stakeholders

Each of the OCX instances running on top of GÉANT/NREN infrastructure that form the gOCX network are connected to the others via backbone links engineered and dimensioned in such a way that certain performance metrics can be guaranteed. Downstream, OCX instances connect users with CSPs wishing to lease and offer cloud services (OCX Access Points). Finally, upon a user's request, gOCX will be able to provide connectivity between any two or more[1] OCX Access Points in a secure and isolated manner. OCX Access Ports could multiplex various services on one port using VLANs that maintain logical traffic separation.

3.1 API for gOCX members

Connectivity services for cloud users cannot be provided at the slow speeds of the past, but rather gOCX should match the same elasticity and dynamicity that are the hallmarks of cloud services. gOCX should therefore impose a Networking API for all participating parties, which should implement a northbound interface to their networking components, mainly for use by the CSPs. This would ensure that the necessary tools are in place to facilitate the implementation of the gOCX service at appropriate OCX points based on user demand. The aim is to provide an almost automated provisioning procedure to gOCX members, via the API, that would make instant connectivity between the CSP and the user available over gOCX. The API should incorporate AAA functionality, as part of gOCX's TTP.

[1] In other words, a E-LAN (Ethernet Virtual Private LAN) service

Working together with the CSPs, gOCX should define and install a standard set of techniques to expose (or extend) the data centre's virtual networks and multiplex different virtual networks belonging to different service instances over the same port(s) (facing OCX infrastructure). One obvious solution, as mentioned, is to use different VLANs. However, in certain scenarios/use-cases this will not be applicable and other solutions should be implemented. This networking interface should be exposed and managed using the above-mentioned API.

Since gOCX is a service that runs on top of the GÉANT/NREN infrastructure and Services, any technology that is available and deployed in this environment could in theory be used for gOCX orchestration and service provision. As discussed in the previous section, any technology and service that segments networks resources and enables network virtualisation that is available in the GÉANT/NREN ecosystem, such as L2 P-2-P MPLS VPNS, VPLS, Bandwidth on Demand-BoD, MD-VPN, and SDN, can be used for gOCX. The exact implementation path and components that will be used will need to be defined at a later stage.

3.2 Added Value Services Using gOCX

The gOCX architecture described offers a wide spectrum of added value services for the R&E community:

- First of all, via gOCX, the user *needs to use only one port (the port that connects them to their local OCX) to connect to a number of different CSPs*. In this way, the client is provided with virtualized private direct connections that bypass the Internet, offering increased security and enhanced service performance, which is of particular importance for data-intensive applications. In this way cloud users will be just "one hop" away from their chosen CSP, only needing to connect to the nearest OCX.

- The proposed architecture offers a *solution to the last mile issues* affecting cloud service delivery, by leveraging the GÉANT/NREN infrastructure. For example, the distributed gOCX architecture allows the users to establish direct connections to CSPs that may be located on the other side of the continent using only their local access port to GÉANT.

- The OCX infrastructure offers the possibility for an aggregated demand to CSPs. The gOCX framework interconnects CSPs and cloud consumers wherever they are located within the area covered by NRENs/GÉANT. This means gOCX can enable GÉANT to become the facilitator of the *largest cloud ecosystem for R&E communities*, including a vast number of cloud users and public and academic CSPs.

- In the case of a *coordinated effort*, only one party (e.g. GEANT Limited, representing the GÉANT network) will act as guarantor for the signed SLA. A coordinated approach will also enable the creation of an efficient single point of contact Service Desk (for an example at GEANT Limited) to assist users should they require information or encounter any problems.

- gOCX's distributed nature means the whole GÉANT community will be able to access a *wide choice of public, as well as academic, CSPs*, similarly to the variety of choices available today via the commodity Internet. gOCX will enable direct connections, providing not only additional

security, but also higher overall performance, through bandwidth on-demand (BoD), lower latency, etc.

- Having a great number of possible services on offer to choose from creates a *common marketplace that fosters competition.* The combination of the advantages provided in terms of geographical distribution and aggregated demand means that GÉANT is in a position to negotiate better terms of use with the CSPs towards creating a single platform on which they can offer their services to the entire GÉANT R&E community.

Thanks to the factors listed above, NRENs will be well placed to offer better cloud services at lower prices to their clients. A common marketplace and platform will equally enable users to evaluate the CSPs offers against their costs, thereby making the cost-benefit analysis public and transparent. This on the other hand will force the CSPs to offer improvements in their services, reflected in specialised SLAs, or to lower their costs in order to stay competitive compared to other offers.

4 gOCX Demonstration

In order to test the implementation of the gOCX design for power user use cases the Task started with the organisation and deployment of the demo scenarios. These demo scenarios also helped to obtain an increased understanding of the necessary steps that need to be defined and further automated within gOCX, as well as of any possible difficulties and side issues that might have been overlooked. The main aim of developing the demo scenarios was to start early-stage negotiations with different CSPs so as to obtain valuable feedback which would enable the Task to assess their interest in collaborating on the gOCX proposal. Another goal was to ascertain the level of complexity that a direct connection setup would involve when observed on all three planes (client to OCX, OCX to another OCX, and CSP to OCX) independently. Based on the lessons learned from the deployed scenarios, the Task's next steps will be to define a detailed design and specification of the gOCX architecture and functional API.

4.1 Demo Scenario I: Power Client to Remote CSPs

In order to create a proof of concept demo that would highlight the benefits of using gOCX, a simple test scenario was defined and presented in real time at the TERENA Networking Conference, in 2014 [TNC2014]. The aim of the proof of concept is to present how the gOCX solution can provide a reusable network infrastructure that will deliver guaranteed QoS compared to the public Internet best effort connection alternative.

The scenario is based on one of the main use cases that would benefit from dedicated connections to CSPs (cloud power users related to big data). In this specific demo scenario, the use case is based on real-time HD video streaming and editing, where the power user defined a multi-server video encoding that was done by transcoding very high-resolution frames from their original lossless format into a compressed video format suitable for web viewing. This is a computationally-intensive task which has a target performance of 24 frames per second.

The demo scenario is defined as follows: two institutions (A and B) would like to combine and edit several, locally available, HD video streams. Two video streams provided separately are to be combined into a single HD video stream using a cloud IaaS and storage provider [Okeanos]. The single combined stream is edited using image manipulation software available from a different CSP [CloudSigma]. The video data located at the University of Amsterdam (UvA) is transferred to and from the computing resources demanded from Okeanos and CloudSigma via the direct connections established using the OCX instances. The resulting video is then sent to both participating institutions (clients).

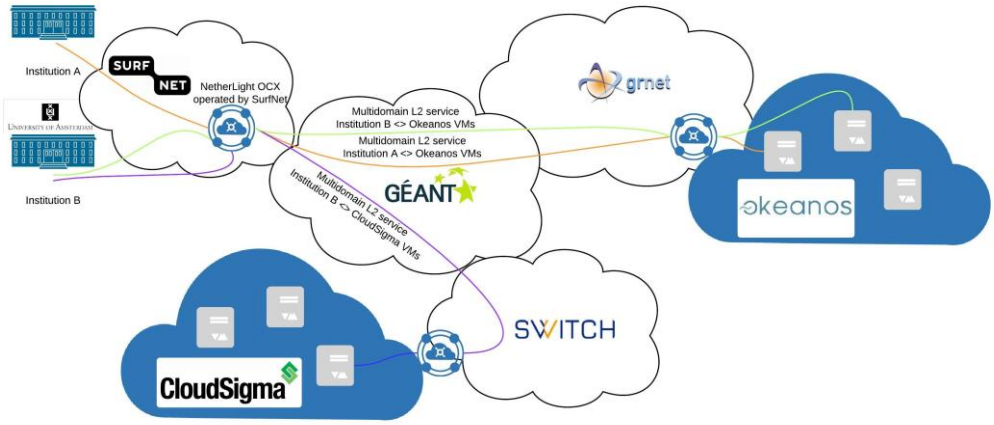

Figure 4.1:gOCX proof of concept: demo scenario I

If such a scenario were to be implemented using a traditional approach using the public Internet to connect to the CSPs, a number of steps would be needed in order to accomplish the task described above: (1) both of the clients would have to send their videos to the cloud storage; (2) the resulting combined video data would be sent back over the Internet to one of the clients; (3) this client then sends the combined video to the other CSP that is used for video editing purposes; (4) one of the clients receives the final video back after editing; (5) this client shares the final video with the other client. All these data transfers take place over the public Internet using the best-effort approach without any QoS guarantees or special traffic isolation.

However, if instead of a traditional approach we use the OCX infrastructure and deploy the same scenario (Figure 4.1**)**, the same task can be accomplished in a more efficient manner. To begin with, three OCX instances will need to be in place in order to provide direct connections for all parties: the two clients (both at UvA) and the CSPs. The OCX boxes/configurations are placed at the respectively nearest network providers (NRENs): SURFnet for the clients, GRNET for Okeanos, and SWITCH for CloudSigma via [Equinix]. Via these OCX instances, the cloud clients and cloud providers are directly connected to the OCX infrastructure.

As illustrated, the interconnection between the clients and the CSPs is then provided using multi-domain Layer 2 services. These services are established on-demand between the OCX instances and are implemented using the underlying services offered by the GÉANT/NREN network (e.g. bandwidth on demand [BoD]). This, in effect, means that in order for the client to gain dedicated access to any CSP connected to the OCX infrastructure, a single L0-L2 connection to their local (nearest) OCX instance is required. This OCX instance will in turn connect the client to the respective CSP(s) on L0-L2 via the GÉANT/NREN network.

The main benefit provided by the OCX infrastructure in this demo scenario is the use of dedicated links towards the CSPs that provide substantially improved data transfer performances between the clients and the CSPs, while completely by passing the public best effort Internet. Furthermore, the use of multi-domain L2 services ensures traffic isolation.

The demo was run several times (twice before the real-time presentation at the at the TERENA Networking Conference, in 2014 [TNC2014], once during the reserved presentation slot at the

conference, and several times for different visitors to the GÉANT booth were more information was made available to interested guests). The user side performances recorded in terms of network throughput and quality of the video were consistent throughout all tests. In order to carry out a first-order comparison of the improved performances, the same demo scenario was executed using standard Internet connectivity. When the clients connected to the CSPs using a standard Internet connection, the maximum throughput achieved from the UvA storage server to any of the two cloud providers enabled roughly 10 processed fps. In comparison, when leveraging the OCX network infrastructure, the maximum throughput achieved from the storage server to any of the CSPs provided a three-fold increase compared to the public Internet connections. This performance increment enables a processing rate close to 30 fps, i.e. real-time viewing of the transcoded movie without any buffering or delays. In networking terms this translates to 3 Gbps compared to the 1 Gbps obtained when using a traditional setup. The network was constantly monitored in real-time via a network weathermap webapp hosted at GRNET [GRNET Demo]. The enhanced cloud service experienced by the end users was also confirmed by the results of the second, more complex, demo, discussed in the next section. Further information on improved network performances using gOCX are given in the results on network throughput at different points in the OCX architecture presented in Appendix A.

A major argument in favour of gOCX is that all previously available L2 connections can be reused for future cloud service delivery so that after initial setup clients can use the cloud service transparently. Furthermore, since the connections to the cloud providers take place on L2 (or lower), the available cloud services can easily be expanded with more advanced features (e.g. extending the customer network into the cloud).

4.2 Demo Scenario II: Multiple Users & CSPs

The second demo scenario is an extension of the proof of concept intended to introduce more participants in the demonstration. The extended demo scenario involves multiple cloud service users from academic institutions that are connected to GÉANT via different NRENs. Most of the users have opted for gOCX to benefit from a joint service from multiple CSPs, while one uses the traditional approach (commodity Internet instead of the direct L0-L2 connections provided by the OCX infrastructure) so as to enable a qualitative and quantitative comparison of both approaches to be carried out. The demo scenario and its results were presented live at the Super Computing conference SC2014 in the USA [gOCXSC14].

The task to be completed in this demo scenario is ultraHD Video Editing and Streaming. Several institutions (University of Amsterdam (UvA), the Croatian NREN (CARNet) and the NREN from Israel (IUCC)) collaborate on efficient transcoding and streaming of 4Kmovies stored at UvA. In the extended version, the resource pool is enlarged with a number of new CSPs. To transcode the vast amount of data, a number of VMs are spawned at Okeanos via GRNET OCX, at Cloud Sigma via SWITCH OCX, and at Kentis via NetherLight-SURFnet.

This extension of the resource pool adds complexity to the task scheduler that needs to select the right set of resources on which the given workload will be executed. For these purposes, the expanded UvA's Vampires cloud scheduling software [Dumitru] is used to spawn the VMs and control the transcoding process. After the transcoding finishes, all of the collaborating parties receive the results directly from the CSPs.

As shown in Figure 4.2**,** UvA and CARNet are connected to their local OCX instances, which enable them to easily gain direct access to the necessary cloud resources via high-performance, dedicated network links. On the other hand, the IUCC demonstrates the traditional approach by connecting via the standard Internet at the closest GÉANT PoP, while accessing cloud services via GRE tunnelling.

Additionally, on-demand networking using an OGF NSI (Network Service Interface) [NSI] connection service has been implemented by the CSP Kentis [Kentis]. The service enables on-demand connectivity between Kentis and other NSI-enabled users and CSPs. In the demo, UvA uses the API provided by Kentis to setup dedicated paths via NetherLight's OCX that connect VMs spawned at Kentis to the UvA network, creating a network extension.

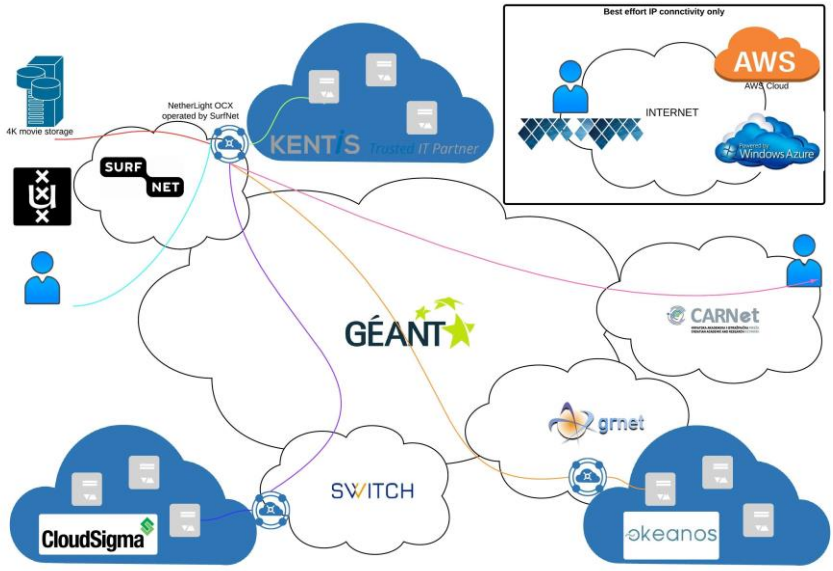

Figure 4.2: gOCX demo scenario II

A monitoring and visualization service has been implemented to manage the network and assess its performance. Based on the performance and topology information collected from the end-nodes and the Vampires Scheduler, the OptOSS NGCMS application developed and distributed by Opt/Net [NGCMS] provides near real-time visibility into the managed networks of the inter-cloud infrastructure. The results obtained have confirmed the findings of the first demo scenario, establishing the setting for future, more complex scenarios.

4.3 The 5th Helix Nebula Assembly

Demo Scenario II was also presented at the 5th-Helix Nebula [HelixNebula] Assembly in Frascati (Rome) in November 2014, in order to introduce GÉANT's gOCX activities to the Helix-Nebula Partners.

The General Assembly's mission statement is "Enabling a Dynamic Cloud Ecosystem". The Assembly presented their current activities and conveyed their inclination to seize new opportunities and address challenges in the field of cloud computing. An example of a possible area for future collaboration is a Europe-wide federated cloud marketplace for which the Assembly is currently

defining the requirements, and that will involve a large number of suppliers. A lively discussion ensued on a possible new governance model, the Helix Nebula Marketplace (HNX), to be treated and developed separately from the Helix Nebula Initiative [HNI].

The HNX can be defined as a "European Cloud Marketplace service" which operates in accordance with EU regulations and legislation, and comprising both commercial CSPs and public e-Infrastructures. Its vision is to create a form of a hybrid cloud computing environment to provide trusted cloud services on the Helix Nebula Science Cloud to serve the European research community.

Opening a discussion on the question "Who can play the role of service owner and provider of this marketplace?", it was concluded that the marketplace would have to be potentially hosted by a neutral entity providing a clearinghouse, that could act as an orchestrator and enable the sharing of resources between the demand and supply side, as well as between suppliers themselves. In considering the possibility of GÉANT's taking on this role, it should be noted that the marketplace must use a generic authN/Z schema in order to guarantee the required level of trust in the aggregation and provisioning of cloud services. All of these requirements could be met by the gOCX architecture, therefore gOCX can be considered as a potential candidate for provisioning the HNX marketplace, offering a platform where CSPs from the public and private sector are able to share their cloud resources. This platform can bring together the cloud marketplace and network provisioning, employing a model that is typical for network and cloud providers (such as the marketplace offered by the Equinix Cloud Exchange).

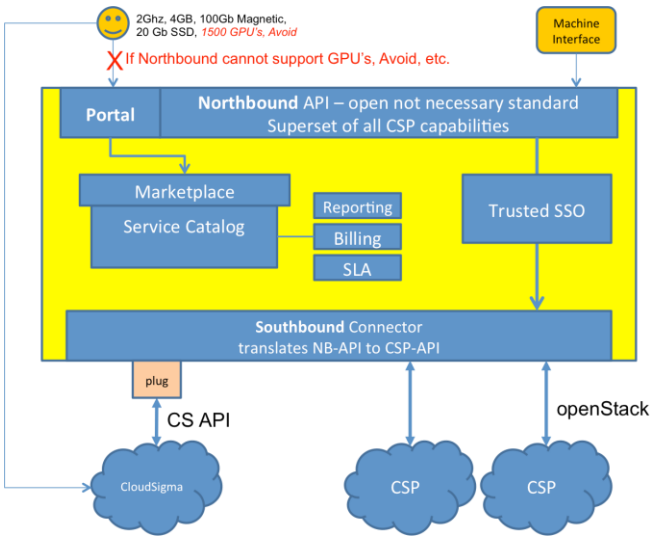

Figure 4.3: High-level approach of a generic marketplace framework

Following discussions with CloudSigma a first draft of a proposal for a generic marketplace should include the following (Figure 4.3):

- End User: Features such as GPUs multi-tiered storage and high-availability of the CSPs, provided to meet the various requirements of the end user, should be supported by the Northbound APIs towards the end-user.

- Machine Interface: Enables automated access to the marketplace for accessing a collection of possible aggregated cloud services, billing, monitoring, etc.

- User Portal: The end-user access to the cloud should be provided through a User Interface (UI)
- NBI: The Northbound APIs should be made open while covering all CSPs capabilities and potential user requirements. One possible way to achieve this is by using the most commonly accepted standards in place, e.g. using the OCCI, REST etc.
- Service Catalogue: The real purpose of the marketplace is the creation of a service catalogue including all registered cloud services that can be provisioned to the end-users or features that can be aggregated with other CSPs. It is essential that reporting is in place to keep track of which cloud services are aggregated, available or used. The service catalogue should be supported by an auditing and accounting system, a finance model and signed SLAs.
- Trusted SSO: A trusted single-sign-on should guarantee privacy and protect the Cloud federation community from misuse of services and SLA violations.
- SBI: The southbound APIs should translate the NBIs requests and talk to the CSPs' plugins.

It will be important, if implementation is to be successful, that the marketplace be technology-agnostic and flexible enough to cope with most requirements/features of the end-users/CSPs, otherwise users are likely to prefer direct peering with their chosen CSPs for cloud service aggregation and provisioning. On the other hand, CSPs accept the idea of an open marketplace since they cannot in any way prevent others from rating their services, which is the basic idea behind the open market. Thus they are going to be wiling and motivated to use the established marketplace in order to attract the R&E cloud users.

4.4 gOCX Benefits

The two gOCX architecture demo scenarios presented above have confirmed a number of technical and non-technical benefits that would be derived from its implementation, and that would enable the GÉANT network to upgrade to a cloud-ready network and offer its customers the means to efficiently use cloud services.

The gOCX architecture will inherently create a broad community of public and academic CSPs directly connected to GÉANT. Once a direct connection with a given CSP is established, using the OCX infrastructure at any point within an NREN or at the level of the GÉANT network, this connection will be available to all potential end users from the R&E community. This will not only result in short provisioning and implementation times for connecting to CSPs, but will also set up the best possible route (by choosing the closest geographic location, in terms of proximity to the CSP's data centre, best connection parameters in terms of connection type, etc.)

From a functional perspective, this will facilitate establishing transparent connectivity between the R&E community and the CSPs. Furthermore, by enabling end-to-end connectivity, a number of additional performance enhancements (compared to the traditional best effort Internet approach) can be implemented, such as using jumbo frames, bypassing firewalls/policies, using an institution's IP addressing schemes, even private addresses, that extend to the Cloud VMs/networks, etc. The feature that most enhances the proposed architecture is the ability to set up dynamic, real-time connections between CSPs and users, which can also be seen as *connectivity and bandwidth as a service*. These connections and reserved bandwidth are in addition available on-demand, dynamic and

elastic, thereby making efficient use of the underlying network infrastructure. In order to fully leverage the possibility of reserved bandwidth as a service, gOCX should be set on L1, while on L2 it can only offer shared physical line bandwidth with enabled QoS traffic prioritisation.

The performances of the system are not influenced by different MTU sizes or number of firewalls that are traversed, since all links are established below L3, which can be accomplished using different technologies such as, for example, Autobahn and BoD, L2 MPLS VPNs, Ethernet, Optical switching, OTN, etc. This means the overall performance of the user-CSP connectivity will be mainly influenced by the type of direct connection established between the CSP and an OCX instance. This also opens up the possibility of defining custom SLAs with a minimum level of agreement for CSPs supported by GÉANT or other neutral organisation.

In terms of economic benefits, it is expected that gOCX will enable long-term cost savings. The only physical infrastructure investment required is the establishment of dedicated links to the CSPs. Compared to a traditional approach, where independent dedicated links to CSPs are needed for each cloud user, the gOCX enables a broad footprint of connected service users that can be reached through a single dedicated link per CSP only. In this way CSPs are just one hop away from the R&E community connected to GÉANT, which enables a multitude of prospective cloud users to act as one big cloud service customer and therefore leverage better offers from the CSPs. gOCX will thus create a common marketplace where the CSPs can present their offers, resulting in a competitive environment that will lead to increased service quality and/or price drops.

This common marketplace will be greatly enhanced by a fully automated service provisioning offered by gOCX. This will enable users to obtain direct connectivity to CSPs in a matter of minutes, while the CSPs will be able to dynamically adjust their offers to the end-user community. In order to provide such automated functionalities and effectively reduce the “time-to-market” of connectivity as a service, new networking technologies such as BoD, NFV and SDN should be leveraged. Because of its advanced implementation requirements, the proposed gOCX architecture is seen as a challenging use case for practical deployment of new network technologies, e.g. SDN or NFV.

5 gOCX and SDN

As discussed previously, the gOCX service offers virtual, isolated and secure extensions to the direct connections to users' networks and their requested cloud services, providing a connection between service users and providers over the GÉANT backbone. The demo scenarios presented have highlighted the benefits of direct connectivity, but also show how time-consuming and fragmented the task of setting up all the direct connection links needed to interconnect the parties involved is. Additionally, when setting up such connections manually, there is a high chance of human error, delays due to poor synchronisation and misunderstandings occurring. This means that the true benefits of the gOCX architecture will be available, usable and transparent to end users only if the connection set-up process is done automatically, preferably by virtualizing all OCX instances and using a web service-based platform.

Automation using a gOCX inter/intra connectivity management web portal will allow NREN customers to choose between different CSP offers, setup their preferred connections, and manage and monitor their requested services. Furthermore, by employing an automated process, CSPs can dynamically setup their offerings on top of the network infrastructure as well as monitor their subscribers' activities. Currently, the most promising candidate technologies to enable these advanced gOCX features are Network Function Virtualization (NFV) and Software Defined Networks (SDN). In this section, their capabilities are discussed and a conceptual broad view of the gOCX implementation using these technologies is presented. However, it should also be noted that automated management could also be achieved using SNMP, although this involves a more complex process.

5.1 NFV & SDN capabilities

While NFV offers users the ability to apply services and network functions virtually across an entire network, an SDN framework provides a more adaptable way to control and manage network communications by separating the control and data planes. These two concepts combined offer great potential in terms of setting up OCX communications between CSPs and users and enhancing adaptability and performance of the direct connections.

Network Function Virtualization (NFV) is an innovative method of virtualization of network functions and services, so that these can run as VMs on general-purpose hardware [NFV]. This process of network services virtualization allows networked functions (e.g. firewalling, load balancing, QoS, IDS, etc.) to be placed and migrated dynamically so that they are detached from the infrastructure.

NFV enables co-location of multiple instances of network functions on the same off-the-shelf hardware – each running in one (or more) different VMs. This means that, using NFV, network

operators and service providers can dynamically instantiate, start, and re-allocate resources and functions, but also program functions according to needs and policies individually.

From the gOCX perspective, SDN/NFV can offer implementation of OCX instances where required (NRENs and GÉANT), in the form of VMs, using commodity hardware. This is extremely beneficial especially when taking into account that the network switching equipment used to establish direct connections is already in place, and all that is required is to apply additional logic via further configuration of the devices. The processes inside the OCX VM can interface with the corresponding networking equipment via remote network management protocols in order to deploy the configuration. The configuration setup, on the other hand, will be defined, based on the demands of the gOCX users (users, CSPs and network admins), using a single web-based management platform (portal, UI) that will interface with the virtualized OCX instances using well-defined web services.

Furthermore, the concept of Software Defined Networks [SDN] involves decoupling the software-based control plane from the hardware-based data plane (e.g. packets forwarding). This means that the network control logic (and states – network intelligence) is moved to logically centralised controllers. In SDN, decisions about switching and implementation of other networking tasks are made by a centralised SDN controller that knows the network infrastructure and current status. The controller interacts with SDN switches using a protocol. One example is the OpenFlow protocol as defined by ONF [OpenFlow]. The protocol procedures are mostly related to data flows, queues and ports, while applications and functions, running on top of the controller, are open for development.

Using network virtualization, multiple isolated logical networks, each with potentially different addressing and forwarding mechanisms, can share the same physical infrastructure. SDN offers an approach to virtualization in which the same hardware-forwarding plane can be shared among multiple logical networks, each with a distinct forwarding logic. An instance of a virtual network is called a slice, defined as a set of flows running on a topology of switches, completely isolated from each other. In order to introduce multiple virtual networks on top of the physical network, an additional network virtualization layer is needed in SDN. An example of such network hypervisor is FlowVisor [FlowVisor] that uses OpenFlow as a hardware abstraction layer and is logically placed between the control and forwarding paths on a network device. The hypervisor is aware of the slicing that can be done in multiple dimensions, e.g. bandwidth, topology, traffic, etc. Acting as proxy, it can host multiple guest OpenFlow controllers making sure that a controller can observe and control only its own slice, while isolating one slice from another (both the data path traffic belonging to the slice, and the slice control). The virtualization layer is transparent to the network hardware and the controllers managing the virtual networks.

The set of flows that make up a slice can be thought of constituting a well-defined subspace of the entire geometric space of possible packet headers, called flow space, defined using a slice policy. For a given packet header, the hypervisor can decide which flow space contains it, and which slice it belongs to. This means the virtualization layer offers complete isolation between slices.

With SDN, the network can be provisioned in an orchestrated way along with other IT components, such as servers, storage and applications. The main benefit of a software-defined network is that it can be automated; network resources are configurable and programmable through open API's (mostly NBIs). Automation allows services to be provisioned quickly and to scale with reduced chance for human error.

5.2 gOCX design using SDN

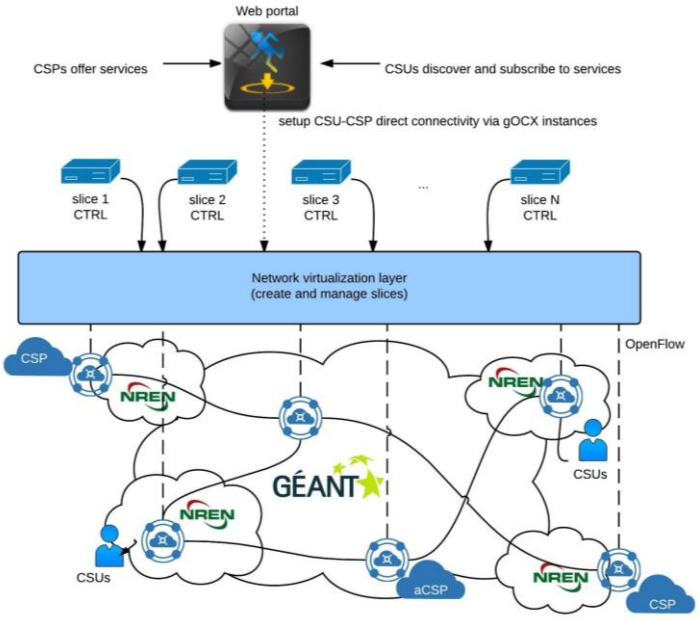

Figure 5.1: SDN-based gOCX architecture

SDN/OpenFlow and its slicing capabilities show a promising potential to be used as the underlying framework for gOCX service provisioning, but a thorough investigation of the APIs and (re)design of the control, data and orchestration plane under high network virtualization conditions is needed to achieve this. Another challenge is how such an infrastructure, which spans across multiple domains, will be managed and monitored.

However, the first steps towards a proof-of-concept solution are already in place, the NRENs' and CSPs' needs/requirements having been gathered to be later used as indicators and drivers for the implementation of a SDN-OCX-Infrastructure over GÉANT. At the same time, the main CSPs are being contacted in order to establish collaborations and define a set of standard connection alternatives that will help define an API to set up and manage direct connections to CSPs.

In an SDN-driven gOCX architecture, as shown in Figure 5.1**,** the process of setting up direct connectivity between users and CSPs involves slices of virtual networks connecting the client(s) and the provider(s). Each CSP can setup and manage its own controller that will run on top of a network virtualization layer such as FlowVisor, VeRTIGO, OpenVertex, ODL, etc. This layer will enable network extensions and user traffic isolation, thereby providing a multitenant environment with rich virtualization and policy management features. The final goal is to define an architecture that will enable dynamic connections to be established. On the orchestration plane, the end users will be able to access all SDN-based gOCX automated services via a web portal, which will provide access to the marketplace as illustrated in Figure 4.3 in the previous section.

6 Conclusions

The expansion of cloud computing services demands that the NRENs and GÉANT adapt their networks and service offer portfolios to include cloud-ready networks that offer high-level cloud services to their end users. To further this goal, the JRA1T2 team proposes that a gOCX architecture be adopted to provide a cloud-based collaborative infrastructure to support new emerging data-intensive research domains and applications. The hierarchical structure of OCX points will enable direct, on-demand connectivity between users and CSPs, providing dedicated bandwidth and the needed QoS.

The gOCX architecture presented here can be extended to bring more benefits in the future, such as offloading traffic, which could lead to lower Internet traffic costs, the provision of TTP services through eduGAIN, and a broker service/marketplace which will allow the R&E community to choose from a broad range of cloud services that guarantee network service levels while maintaining logical separation from the Internet.

However, the manual network configuration required at each OCX instance, as well as at the endpoints (users and CSPs), is a time-consuming and error-prone process. The different technologies used for VLAN handovers (802.1q and q-in-q) also presented further challenges in terms of equipment configuration. In order to make gOCX available to end-users without network configuration skills, the next step in gOCX development will beto make use of the solutions that enable flexible provisioning of multi-domain network services such as OGF NSI, or possibly SDN with NFV. Also, gOCX's role in facilitating integration of (multi-)provider and campus cloud infrastructures poses a number of security challenges which will need to be analysed and addressed.

Appendix A Technical Annex

A.1 Demo Scenario I

The gOCX demo scenario I presented at TNC 2014 includes the following OCX instances:

Country	Location	Connection
Greece	Part of GRNET network	To Okeanos IaaS Cloud
Netherlands	SURFnet	Between two client institutions
Switzerland	SWITCH	Direct to CloudSigma

Table A.1: OCX instances in Demo Scenario I

The OCX instances can run on a dedicated Ethernet Switch or a Virtual Switch instance. The GÉANT/NREN network infrastructure is used for delivering and monitoring the L2links to the OCX instances.

The Okeanos Cloud infrastructure is connected to the GRNET OCX instance through a L2 circuit provided by the GRNET Carrier Network.

In the Netherlands, NetherLight is hosting the OCX instance. NetherLight provides a platform capable of performing OCX tasks. Ethernet switching is possible and any party is allowed to connect (two clients for the purposes of the demo).

SWITCH has a router/switch located at CERN, which acts as the OCX box aligned to the SWITCH GÉANT PoP. Transparent L2 services can be setup between the OCX platforms. The connected parties can create L3 services over these transparent L2 services. For example, CloudSigma can create L3 connections and configure BGP. This L3/BGP configuration does not involve any of the OCX instances.

In order to interconnect the three OCX instances in Greece, the Netherlands and Switzerland, the GÉANT Plus (L2 BoD service) between the instances is used. This Ethernet service should have

adequate (preferably dedicated) bandwidth (at least 1 Gbps) and should allow customer VLANs to be transported transparently[2].

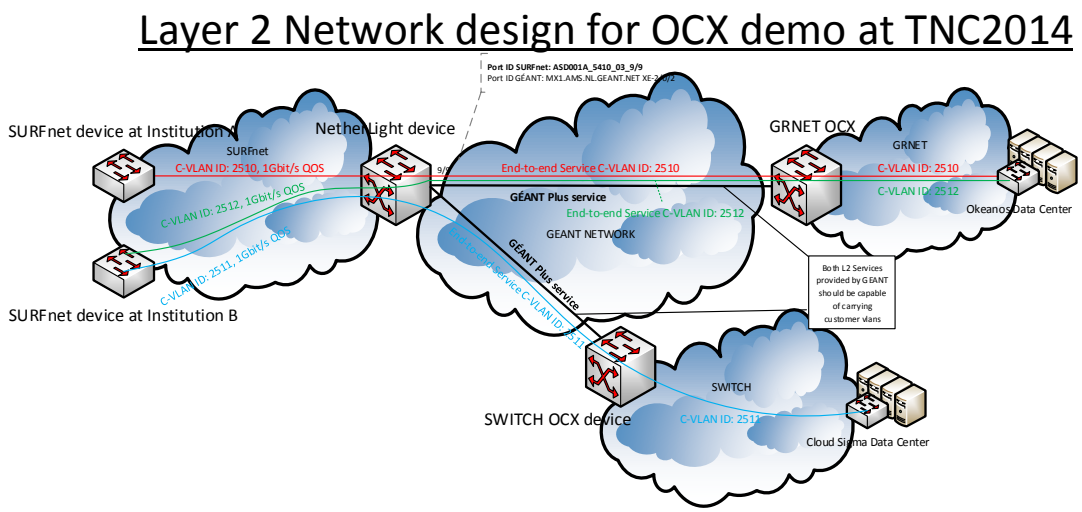

Figure A.1: gOCX demo scenario (the end-to-end services that will be provisioned are shown in red and green). For detailed information on the hardware, links and configuration please refer to section A.1.1

The input data (image set) is the 4K (4096x1720 pixels) version of the 10-minute open source movie Sintel. The application deployment configuration is controlled by the user via a web application (GUI). The scheduler uses a straightforward self-scheduling policy to distribute the tasks to provisioned resources.

The web interface to the application is divided into three main areas: a) preview: where the user can view in real time the result of the transcoding, b) control and status, and c) configuration area. In the configuration area the user can select the resources which would then be used to execute the application. The workload parameters, that is, what image to use and what transformations to apply to it, are also configured in this area. Each CSP offers different types of VMs with varying CPU and memory capacities, and the interface allows the users to select the amount and type of resources to be requested from each CSP. To showcase the advantages gOCX offers, the interface allows users to also select the network resources to be used by the application. Two options are available: the Internet, or the high-speed gOCX network. Once the application and the required resources have been configured, the execution phase may begin. As images are processed, the preview area starts displaying the last processed image together with real-time network statistics.

Institution A and institution B, both under the SURFnet network administrative domain, want to obtain IaaS services (VMs) from Okeanos (part of GRNET) as well as CloudSigma. The steps to accomplish this are as follows:

1. All scenario participants setup L2 connections from their premises via the NREN towards the nearest OCX instances (located at SURFnet, GRNET and SWITCH);

[2]An inherent limitation is that when the L2 GÉANT Services are used in order to interconnect OCX instances running at the periphery, only one VLAN ID can be transported per service (unless IEEE802.1ad is used which then limits this number to 4096 VLANs).

2. Once connected, the institutions request connections from their local OCX instance to the two CSPs in order to be able to use the services these offer. At this stage, the clients (institutions) can browse a service directory from which they can choose to subscribe to services offered by the various CSPs. The TTP role is used for the service publishing and service subscription actions.

3. The local OCX, to which the institutions are connected, establishes L2 VLANs to the remote OCX instances in order to provide direct virtual connections for his clients based on their subscription choices. Upon completion of this step, an end-to-end connection between the clients and the CSPs is established and ready to use. In this case the connection is established between the two institutions (A and B), NetherLight, GRNET and SWITCH. The VLANs that are put in place are configured between the NetherLight OCX via the GÉANT network towards the OCX instances in GRNET and SWITCH respectively. The OCX instances at GRNET and SWITCH configure a VLAN between Okeanos and CloudSigma. All VLANs are trunk lines to the ports interconnecting the institutions and the CSPs.

4. Okeanos accepts the assigned VLAN and terminates it on the Ethernet Segment A. Ethernet Segment A is attached to all VMs that are assigned to Institution A, or a CSP, e.g. CloudSigma.

5. The same procedure (for the new VLANs only, without the need to set up L2 connections again as these will be already in place) is carried out for Institution B. A second institution is included to demonstrate that it is not necessary to repeat the complete procedure as long as the OCX infrastructure is in place.

A.1.1 gOCX Configuration Setup

A.1.1.1 *Network configuration at UvA, SURFnet and NetherLight OCX*

The workload data source and destination are stored on FIONA at UvA. This appliance has 1.4TB of flash backed with 18T of hard disk storage, and is designed to be a source for high quality video streams at speeds above 10 Gbps.

The total amount of data transferred during one execution is approximately 160GB. Similar types of VMs are used at both CSPs. These comprise 4 CPU cores running at 2GHz and 4GB of RAM.

The connection between Okeanos and UvA consists of 802.1q VLANs with IDs in the range of 3301-3310 set on a 1G Ethernet service. These VLANs were mapped to 10 predefined networks in the Okeanos cloud interface. The connection between UvA and CloudSigma is made using Q-in-Q tagged VLAN 2611 on a 10G Ethernet service. CloudSigma used the 50-1000 range as inner VLANs, which are randomly assigned to virtual networks created via its cloud API. However, the actual mapping cannot be queried via the cloud API, and CloudSigma's support department has to be contacted to verify which VLANs are actually mapped to the virtual networks.

The OCX device implemented at NetherLight premises is a Ciena5410 that provides 10 Gbps bandwidth on all connected links. All services at NetherLight for this demo were configured as an EVPL point-to-point connections with a high degree of transparency. The 10G Ethernet service from Netherlight connects to a network switch (Juniper EX4500) at the UvA. The switch strips the outer Q-

tag and forwards the inner VLANs 50-1000 together with the 3301-3310 VLAN range from Okeanos to FIONA, which was connected at 10 Gbps.

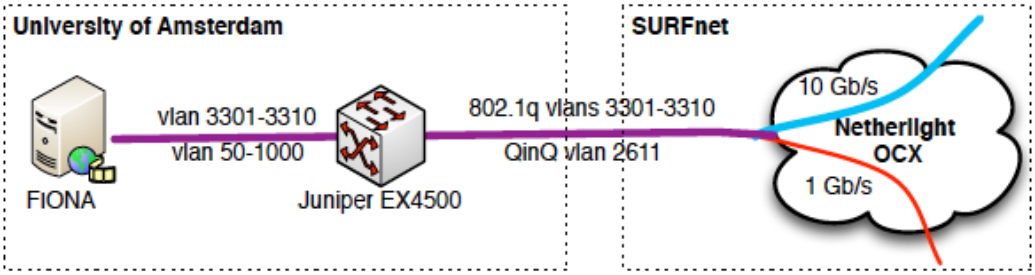

Figure A.2: Network configuration at UvA

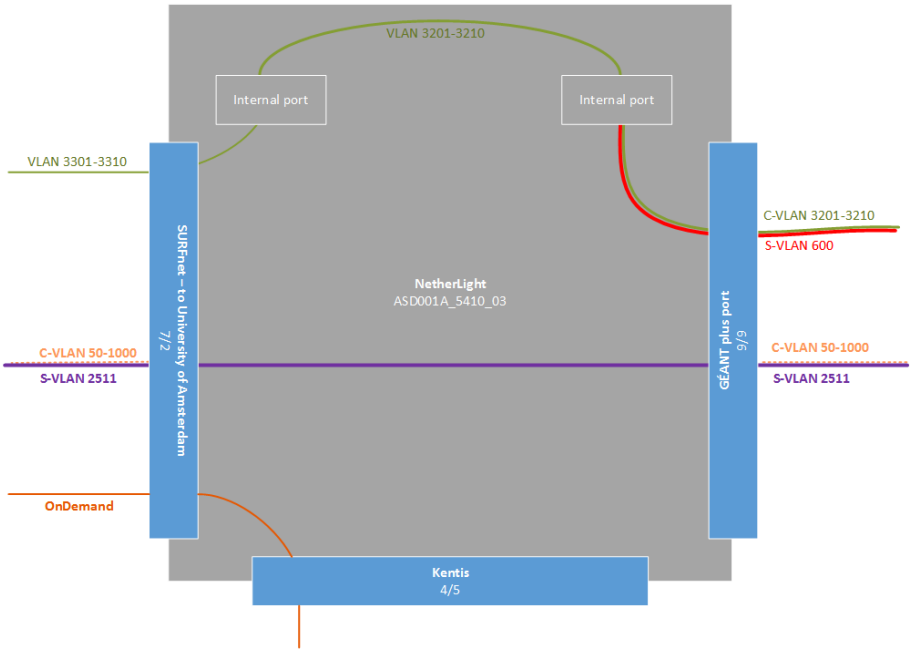

Figure A.3: Network configuration at NetherLightThe VLANs used for the demonstration are combined on FIONA in a Linux network bridge. In this way, a transparent Ethernet domain is created between the UvA and the different cloud sites. This offers the advantage of running a DCHP server that assigns IP addresses and (possibly) other configuration options to the VMs from both cloud providers.

A.1.1.2 *Network configuration at SWITCH OCX and CloudSigma*

At SWITCH, three links that span over two routers needed to be set up in order to provide connectivity to CloudSigma (link 1) via Equinix (link 2); and towards the OCX instance at NetherLight (link 3):

1) Cloud Sigma <==> Equinix Zurich- Cross connect Cloud Sigma to SWITCH (Equinix) - Configuration of the virtual network on the Cloud Sigma account for the 3 VMs that were used for the demo:

   a. tnc_demo12 b32e354-8832-428a-82c4-26975b344c72 = ID 882
   b. tnc_demo22 b8f7ef9-a697-48c3-82b1-bd7590383e76 = ID 983

c. tnc_demo32 b92e513-168e-406c-a2f9-bf7afc18d88b = ID 924

2) Equinix Zurich <==> CERN (SWITCH PoP) with Cross Connect SWITCH-PoP to GEANT PoP at CERN, this is the OCX setup Cloud Sigma to GEANT within SWITCH

a. Router Equinix Zurich (swiIX1) - port Te3/1 10GE single-mode fiber to Cloudsigma DC with EoMPLS transport to swiCE3 in Geneva (no priority, route the same as normal IP traffic)

```
swiIX1#traceroute 130.59.255.29
Tracing the route to swiCE3-L2.switch.ch (130.59.255.29)
VRF info: (vrf in name/id, vrf out name/id)
1 swiZH2-10GE-1-3.switch.ch (130.59.36.130) [MPLS: Label 308
Exp 0]
2 swiCE3-10GE-3-1.switch.ch (130.59.36.1)
```

b. Router at CERN, Geneva (swiCE3) - port Te3/5 10GE single-mode to GEANT router

```
swiCE3#traceroute 130.59.255.51
Tracing the route to swiIX1-L1.switch.ch (130.59.255.51)
VRF info: (vrf in name/id, vrf out name/id)
1 swiZH2-10GE-1-1.switch.ch (130.59.36.2) [MPLS: Label 34 Exp
0]
2 swiIX1-10GE-3-3.switch.ch (130.59.36.129)
```

3) CERN (SWITCH PoP) <===> OCX SURFNetherLight – GEANT Link

```
Description: GEANT Hardware is Force10Eth, address is
00:01:e8:8b:4a:d7
Pluggable media present, SFP+ type is 10GBASE-LR
Medium is MultiRate, Wavelength is 1310nm
SFP+ receive power reading is -2.2323dBm
Interface index is 35193858
Internet address is not set
*MTU 9000 bytes, IP MTU 8982 bytes*
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:30:46
Queuing strategy: fifo
```

A.1.1.3 *Network configuration at GRNET OCX and Okeanos*

In GRNET, the local OCX instance was created on top of the Carrier Network as a virtualized Private LAN instance. Taking advantage of GRNET's architecture, a Virtual Private Lan Service (VPLS) was created in all carrier network elements that serve GRNET's Data Centers and that are interconnected with GEANT's mx1.ath.gr.geant.net router that terminates all VPN services. This VPLS instance was configured to switch all vlans that it was agreed would participate in the demo. The following network diagram outlines the OCX architecture in the GRNET network.

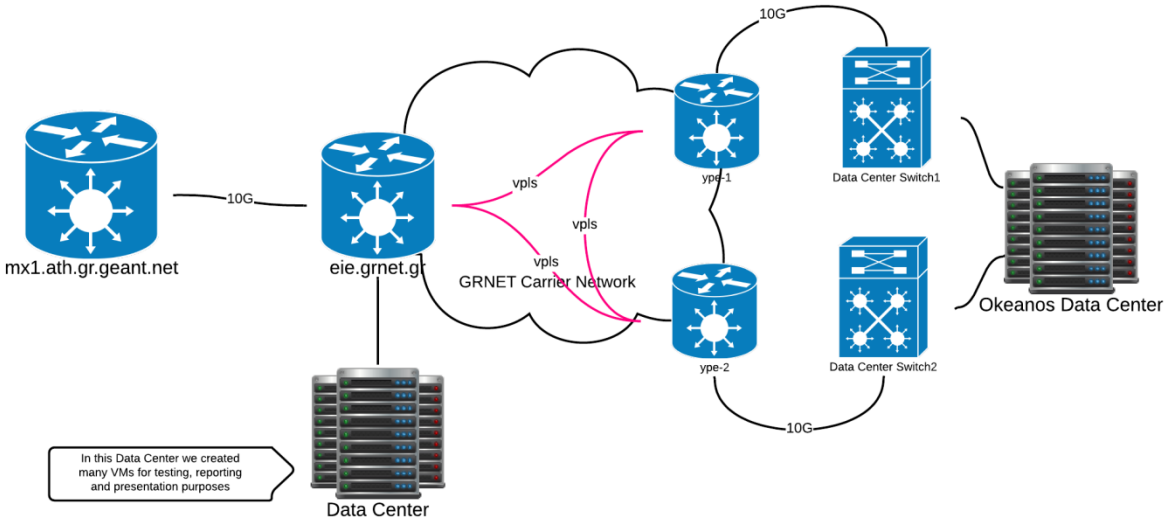

Figure A.4: Network configuration at GRNET and Okeanos

All Carrier Network Elements involved in the OCX network in GRNET are Juniper MX960s and 480 series. Geant'smx1.ath.gr.geant.net is also a Juniper 480 Router. The Data Center elements are Cisco Nexus 7K Switches. All links are 10G Ethernet or bundles of 10Gs in the backbone.

A.2 Demo Scenario II

For this demonstration, the Vampires [Vampires] cloud scheduler and execution engine for data-intensive, Bag-of-Tasks applications was used. Bag-of-Tasks applications (BoTs) are a type of workload consisting of independent jobs which can be executed in any order. Typical examples include image processing, parameter sweeps, design space exploration or any other type of batch jobs which have no interdependency. The provisioning component was built using the jclouds Java library, which provides a common API for multiple cloud providers. The user-specified resources were provisioned from the selected cloud providers and the application was then deployed onto them.

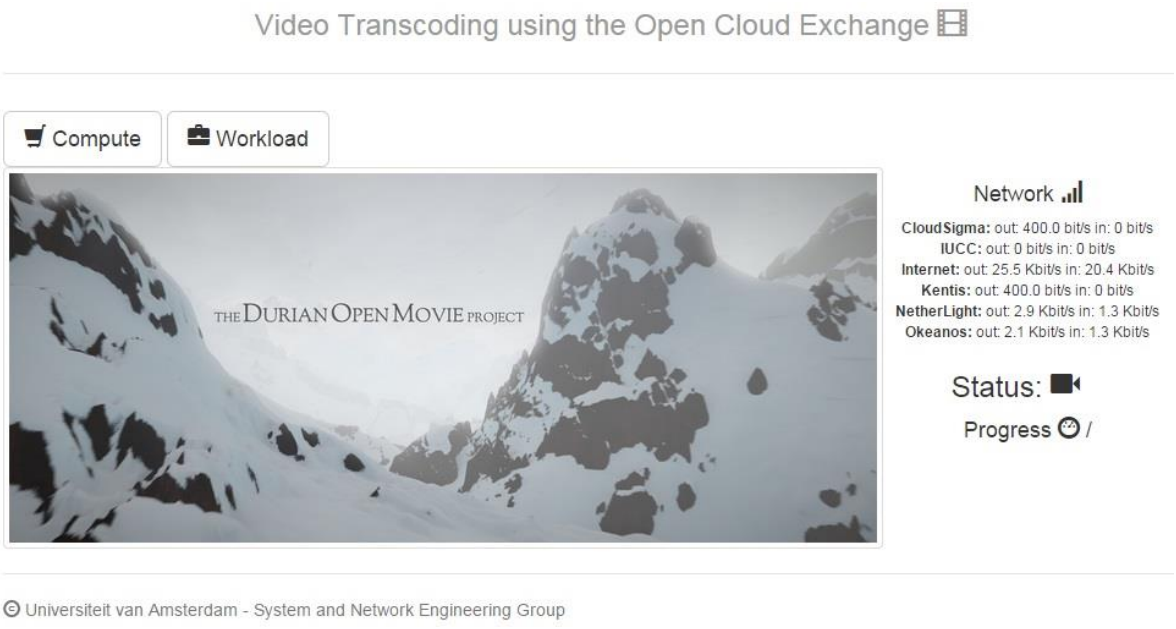

Figure A.5: Demo scenario user GUI

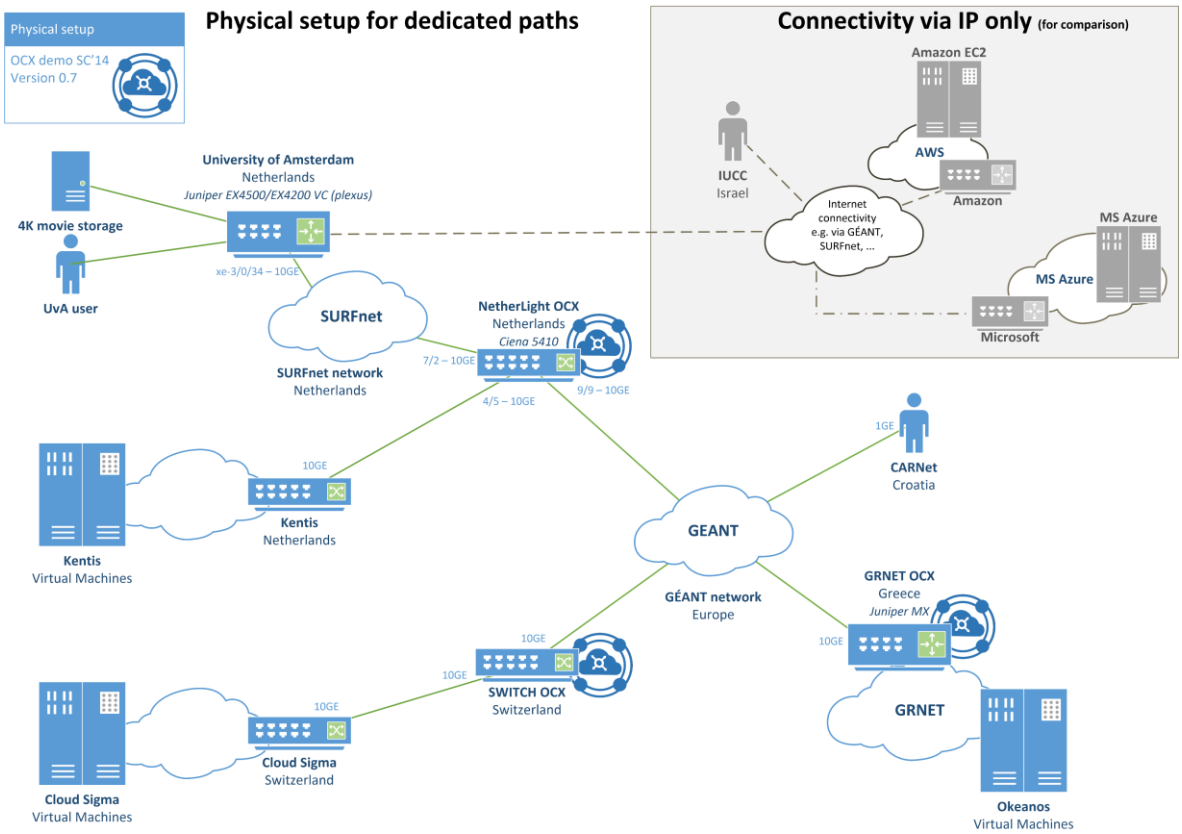

Figure A.6:gOCX demo scenario II – physical links setup

Figure A.7: Network statistics during the demo scenario

Appendix B Monitoring and Mapping

The near real-time OPerator Time Optimized decision Support System for ICT and Cloud infrastructures (OPTOSS) is being developed by Opt/Net in collaboration with institutions of the European R&E community. It consists of OPTOSS NG-NetMS and OPTOSS NG-CloudMS tools, which share the same base source code.

Next Gen Cloud Management System (NG-CloudMS) is a new web-based, end-to-end management tool developed to support the OCX concept. This prototype provides near real-time visibility of the networks and cloud infrastructures and interconnected computing and data storage resources that are part of the OCX-enabled Intercloud architectures. It can therefore assist participating operators to localise the causes of potential incidents for the cloud services. The main benefit of the NG-CloudMS tool is that it provides end-to-end visibility into the Cloud Services that are delivered through several networks and many different service providers.

The NG-CloudMSruns on Ubuntu 14.04 LTS and can run on just one core in the virtual machine. It only requires 1GByte of RAM (at the very minimum) as was shown during the SC14 demo. The larger networks require more computing power and storage. The NG-CloudMS may be deployed on the real server hardware or virtualized into the cloud as one of the services.

NG-CloudMS is connected to the OCX server and automatically maps and monitors the addition and deletion of the CSP’s network links and nodes to the managed architecture. It is precise, quick and efficient in collecting the most complete information about the OCX Cloud network's inventory, topology, mapping of IP address space and, most importantly, the analysis of syslog events and SNMP alarms both in near real-time and from historical archives.

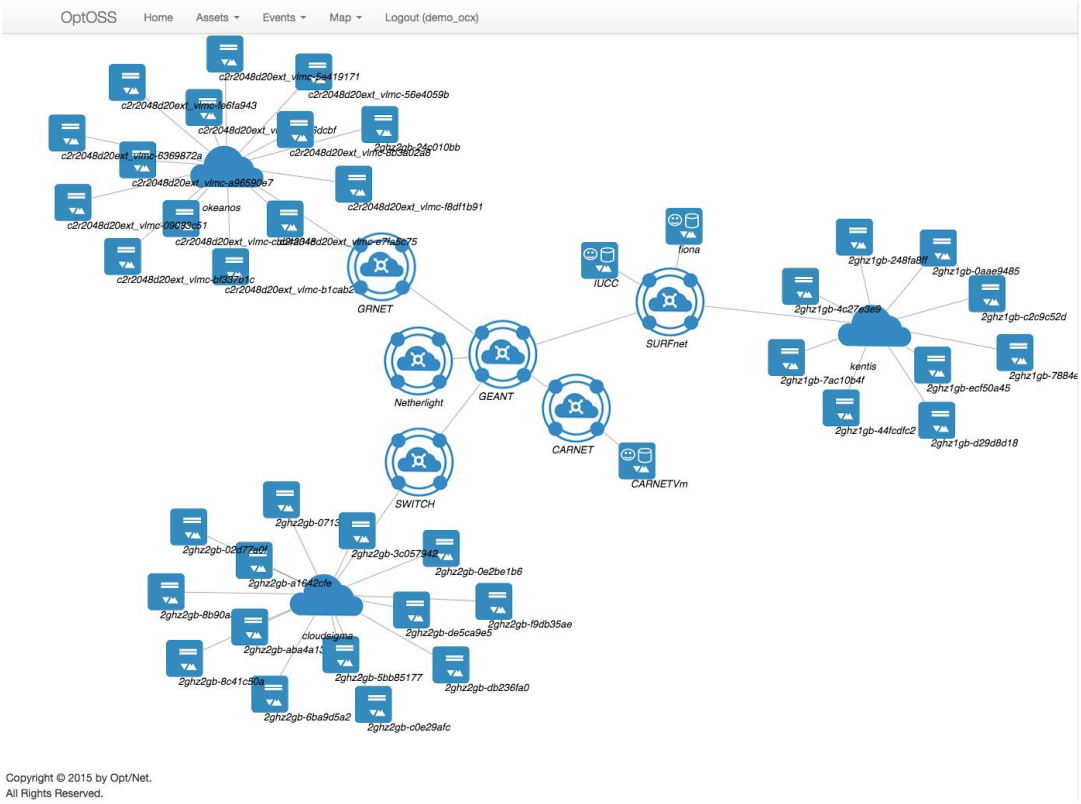

Figure B.1:Real-time map of the OCX enabled Intercloud network used during SC14 demo

NG-CloudMS is a fully autonomous and dynamic system once it has been initiated and configured by the OCX operator. It consists of the following modules:

- Network audit and Host polling modules
- Device specific plugin modules
- Central database
- Event collector modules
- Web GUI

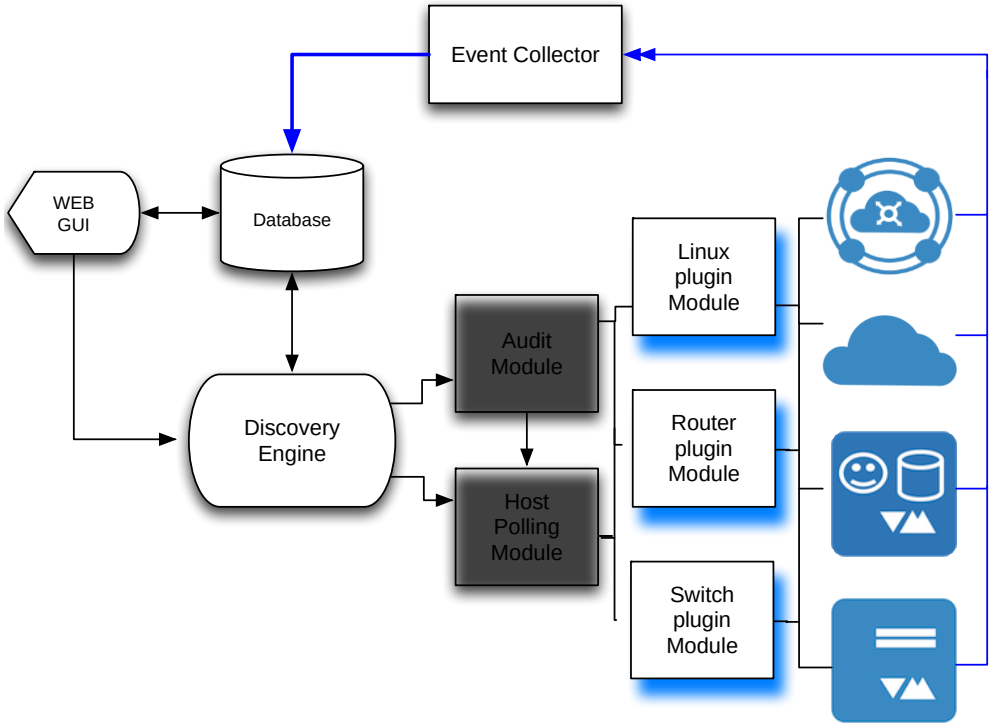

Figure B.2: NG-CloudMS Architecture

The operators perform the initialisation and basic configuration of NG-CloudMS via Web GUI. The system should be configured with authentication methods for the whole managed domain. Also, the active feedback loop from all managed components should be established.

All Intercloud components are configured to send syslog messages to the NG-CloudMS via UDP or TCP network protocols, where these messages are processed and profiled by event collector modules in near real-time. All VM templates contain this configuration and authentication settings.

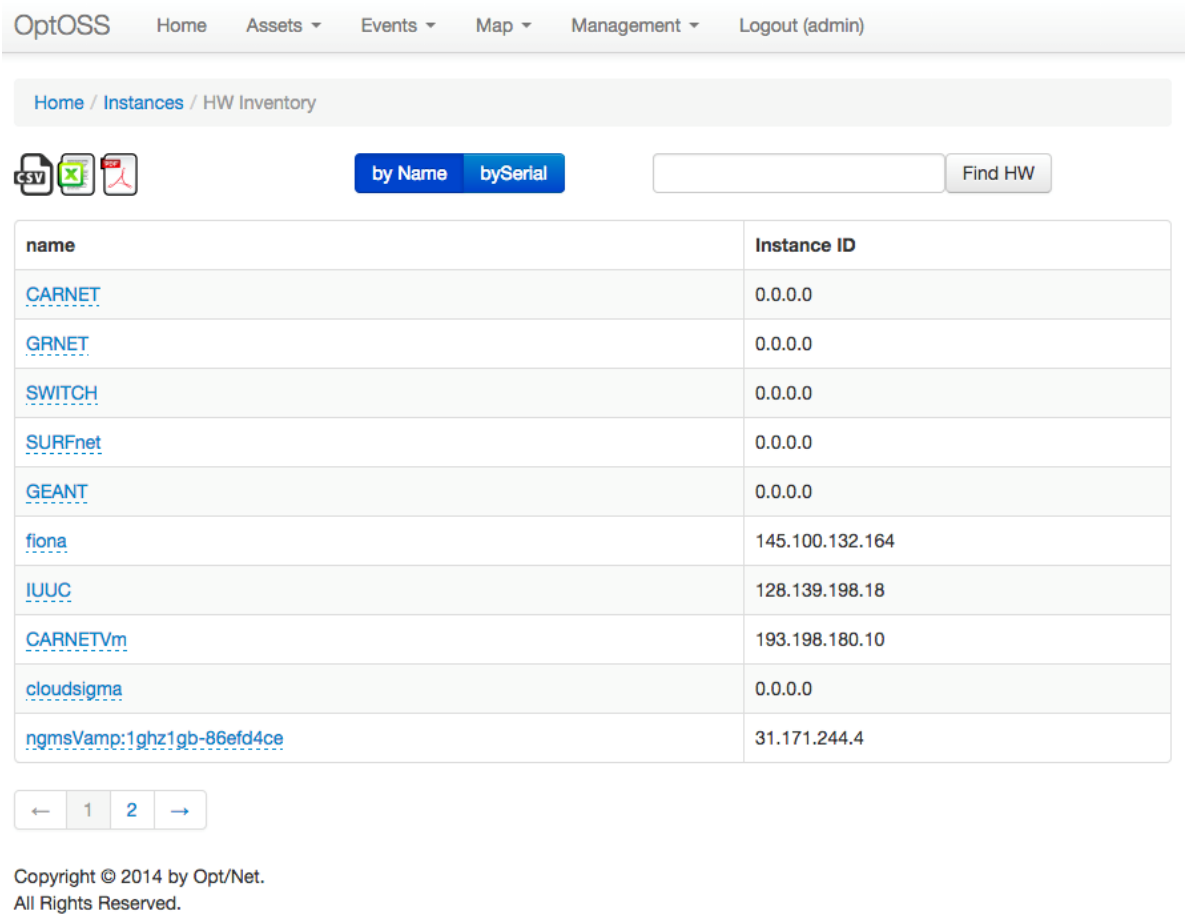

Figure B.3: Inventory data

In order to discover and conduct a complete inventory of the Intercloud infrastructure, NG-CloudMS needs network topology information, which is created and maintained by the Vampire Application Workflow Management/Optimization System (VAWMOS). As new VMs are dynamically spawned by the VAWMOS, the infrastructure update cycle is triggered. The information is provided in JSON table format and is retrieved by NG-CloudMS automatically, as soon as it receives a defined message that signifies that the Intercloud infrastructure has changed. NG-CloudMS will then initiate the network audit cycle and rediscover the entire cloud topology. The network discovery may be partial or complete, depending on the type of change that took place.

Web GUI provides access to inventory information and has reporting capabilities. Information such as system software version and network interfaces, IP addresses and hardware details is presented and could be exported in a number of reports.

The IPv4 address tree provides information about IP addresses used and names of the interfaces which use them.

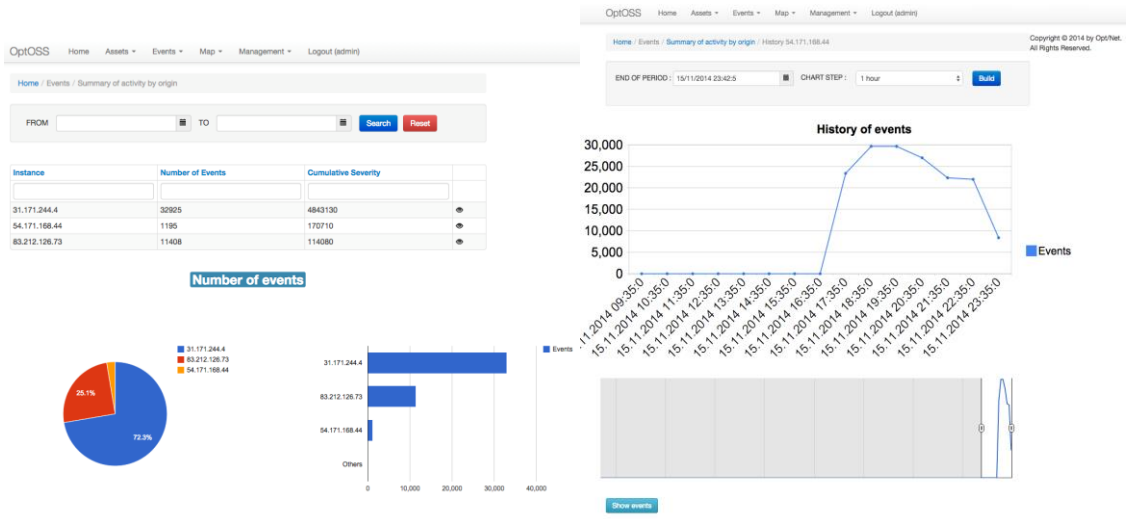

Figure B.4: Event analytics and historical events view

All discovered nodes are monitored continuously and a periodic inventory of the complete network takes place. Events from managed nodes are continuously received by collectors and stored in the central database for archival purposes and analysis. The cumulative severity of the received messages may be plotted with Web GUI. This graphical representation facilitates interpretation of the network and device activity and simplifies searching for the causes of different events. The historical view may be used for data analytics and also to search for the root causes of events. Often, it helps with troubleshooting of different problems on the network and associated cloud services.

Web GUI provides analytics for all collected events. There are two kinds of analytics reports available at this time:

- Cumulative severity of events by origin
- Cumulative severity of events by facility

It is easy to detect top sources of events on the network based on these high level reports. Top sources could be investigated further once enough statistics become available through the historical and detailed event views.

OPTOSS NG-CloudMS is a scalable and modular tool and was selected for this reason for the visualisation of OCX enabled Intercloud infrastructure by the GN3plus project. NG-CloudMS is an Open Source project and is hosted on SourceForge [SourceForge]. Opt/Net distributes most of its code under GPL3.0 license. This guarantees that NG-CloudMS will benefit free software and research and education communities.

The OPTOSS suite of products is being developed by Opt/Net under a business incubation grant from the European Space Agency (ESA). The commercial version of this product (NG-CloudMS Pro) will use intellectual property developed by ESA in the area of advanced operations concepts. The ESA patents are used by Opt/Net under a R&D license agreement signed in 2014 by Opt/Net and ESA.

References

[Affiniti]	"Affiniti WAN services", Affiniti, 2014 http://www.affiniti.com/documents/upload/doc/1/Affiniti%20WAN%20Services%202014.pdf
[AWS]	http://aws.amazon.com/grants/
[BoD]	GÉANT Bandwidth on Demand Service, http://services.geant.net/bod/Pages/Home.aspx
[Brocade]	Brocade, "Cloud Service Delivery Architecture Solutions for Service Providers", Technical Paper for Network Engineers http://www.brocade.com/downloads/documents/technical_briefs/csda-for-network-engineers-tb.pdf
[CloudSigma]	https://www.cloudsigma.com/
[Dumitru]	C. Dumitru et al.:**"**Enabling User-Centric Data-Intensive Application Deployment in Clouds Using the Open Cloud Exchange", SC14, New Orleans, USA, November 2014
[Equinix]	http://www.equinix.com
[FlowVisor]	R. Sherwoodet al.**: "**FlowVisor: A Network Virtualization Layer", Technical Report, 2009
[GEANTCloudCatalogue]	https://catalogue.clouds.geant.net/#/
[GEANTOpen]	http://www.geant.net/Services/ConnectivityServices/Pages/GEANTOpen.aspx
[gOCX]	D. Regvart at al., **"**Network Architectures for Cloud Services White Paper: gOCX", MS101 (MJ1.2.1), GN3+ http://www.geant.net/Resources/White_Papers/Documents/MS101_MJ1-2-1_Network-Architectures-for-Cloud-Services.pdf
[gOCXSC14]	Y. Demchenko at al.: "GÉANT Open Cloud eXchange (gOCX): Architecture, Components, and Demo Scenario", SC14, New Orleans, USA, November 2014
[GRNET Demo]	http://sc14-ocx-demo.grnet.gr/demo.html
[Helix Nebula]	http://www.helix-nebula.eu
[HNI]	http://cordis.europa.eu/news/rcn/122783_en.html
[ICAF]	Y. Demchenko, M. Makkes, R.Strijkers, C.Ngo, C. de Laat, Intercloud Architecture Framework for Heterogeneous Multi-Provider Cloud based Infrastructure Services Provisioning, The International Journal of Next-Generation Computing (IJNGC), Volume 4, Issue 2, July 2013.
[Kentis]	http://www.kentis.nl/diensten/cloud-services/
[NGCMS]	http://ngcms.sourceforge.net

[NFV] White paper on "Network Functions Virtualization" http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[NISTdef] NIST SP 800-145, "A NIST definition of cloud computing" http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[NISTarch] NIST SP 500-292, "Cloud Computing Reference Architecture, v1.0." http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[NSI] Network Service Interface working group in Open Grid Forum https://redmine.ogf.org/projects/nsi-wg

[Okeanos] https://okeanos.grnet.gr/home/

[OpenFlow] "OpenFlow Switch Specification", ONF, ver. 1.4, October 2013 https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf

[SDN] White paper on "Software-Defined Networking: The New Norm for Networks" https://www.opennetworking.org/

[SourceForge] https://sourceforge.net/projects/ngcms/

[TNC2014] Y. Demchenko at al., "Open Cloud eXchange (gOCX): Bringing Cloud Services to NRENs and Universities", TNC, Ireland, 2014

[Vampires] C. Dumitru at al.:"A queuing theory approach to pareto optimal bags-of-tasks scheduling on clouds", Euro-Par 2014 Parallel Processing, pages 162–173. Springer, 2014.

[VPLS] "Implementing VPLS for Data Center Interconnectivity", Juniper Networks, 2011http://www.juniper.net/us/en/local/pdf/implementation-guides/8010050-en.pdf

Glossary

a/pCSP	academic/public Cloud Service Provider
API	Application Programming Interface
AWS	Amazon Web Services
CSP	Cloud Service Provider
gOCX	GÉANT's Open Cloud Exchange
IaaS	Infrastructure as a Service
ICADI	InterCloud Access and Delivery Infrastructure
MPLS	Multi-protocol Layer Switching
NBI	North Bound Interface
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NREN	National Research and Education Network
NSI	Network Services Interface
OCCI	Open Cloud Computing Interface
OGF	Open Grid Forum
OFN	Open Networking Foundation
PaaS	Platform as a Service
QoS	Quality of Service
R&E	Research and education
REST	Representational state transfer
SaaS	Software as a Service
SBI	South Bound Interface
SDN	Software Defined Networking
SLA	Service Level Agreement
SSO	Single Sign On
TTP	Trusted Third Party
UvA	University of Amsterdam
VM	Virtual Machine
VPLS	Virtual Private LAN Service
VPRN	Virtual Private Routed Network