Providing Security SLA in Next Generation Data Centers with SPECS: The EMC Case Study

Valentina Casola[1], Massimiliano Rak[2], Silvio La Porta [3] and Andrew Byrne [3]
[1]*Università "Federico II" di Napoli, Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione, Napoli, Italy*
[2]*Seconda Università di Napoli, Dipartimento di Ingegneria dell'Informazione, Aversa, Italy*
[3]*EMC Ireland COE Innovation, Cork, Ireland*

Keywords: Cloud, ngDC, Cloud Security, Security SLA.

Abstract: Next generation Data Centers (ngDC) are the cloud-based architectures devoted to offering infrastructure services in flexible ways: managing in an integrated way compute, network and storage services. This solution is very attractive from an organisation's perspective but one of the main challenges to adoption is the perception of loss of security and control over resources that are dynamically acquired in the cloud and that reside on remote providers. For a full adoption, datacenter customers need more guarantees about the security levels provided, creating the need for tools to dynamically negotiate and monitor the security requirements. The SPECS project proposes a platform that offers security features with an as-a-service approach, furthermore it uses Security Service Level Agreements (Security SLA) as a means for establishing a clear statement between customers and providers to define a mutual agreement. This paper presents an industrial experience from EMC that integrates the SPECS Platform and their innovative solutions for ngDC. In particular, the paper will illustrate how it is possible to negotiate, enforce and monitor a Security SLA in a cloud infrastructure offering.

1 INTRODUCTION

Storage services, like many IT services, are increasingly moving toward the virtualized, distributed cloud model. Indeed, recent concepts like ngDC or Software-Defined Data Centers (SDDC) (Davidson, 2013) are grounded in the ideas of virtualization, offering the capability to run multiple independent virtual servers using a set of shared, physical resources. Resource Pooling is another significant advantage of the ngDC and SDDC solutions, enabling the automatic allocation of storage, network and compute resources to meet the demand of incoming requests. This is one of the foundational concepts cloud computing is built on. In fact, through ngDC provisioning models, a Cloud Service Provider (CSP) may offer on demand, scalable, secure and cost effective cloud infrastructures or services upon which Cloud Service Customers (CSC) can develop their own services.

However, one of the key limiting factors holding back larger adoption of the cloud services is *trust*. In cloud computing the tangible assets of the CSC become intangible, virtual resources, that are dynamically acquired via a 3rd Party provider. With these provisioning models, the loss of control over their own services and assets (data), CSCs are naturally hesitant to place critical business applications or sensitive data in the cloud. A possible solution to this challenge could be the adoption of SLAs, clearly stating what services are provided by the CSP and the related responsibilities in case of violation.

Despite the intense research efforts into developing standards and frameworks for SLAs (Theilmann et al., 2008), (Morin, 2011),(EC, 2011), (CSCC, 2012), (International Organization for Standardization, 2014), at the state of the art few solutions allow CSPs to offer practical, implementable Security SLAs. Moreover, there are very few services able to concretely monitor the security features which would enable CSCs to verify the status of guaranteed SLAs.

In such a context, the SPECS project[1] proposes a framework which aims to facilitate the automated negotiation, monitoring and enforcement of Security SLAs. This paper illustrates how the SPECS framework is used in order to enhance a ngDC storage service with security features based on customer's requirements. In particular, we integrate SPECS with

[1]http://www.specs-project.eu/

Casola, V., Rak, M., Porta, S. and Byrne, A.
Providing Security SLA in Next Generation Data Centers with SPECS: The EMC Case Study.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 2*, pages 138-145
ISBN: 978-989-758-182-3

the ViPR storage controller[2], a commercial product offered as a service by EMC, in order to fully implement the ngDC paradigm by offering storage services protected by Security SLAs.

The implementation of security capabilities, enforced and monitored through SPECS demonstrates the effectiveness of Security SLAs as a concrete solution that can be adopted in commercial products. The effectiveness and adaptability of this approach is further strengthened by use of standardized security metrics to identify capabilities delivered by SPECS to support the storage service. The outcome of this process is to improve trust in the capabilities of the CSP to protect and guarantee their assets services in the cloud.

The remainder of this paper is organized as follows: Section 2 introduces the SPECS framework for the provisioning of cloud services guaranteed by Security SLAs. Section 3 describes the main features and limitations of ngDC that motivate the need for more flexible and secure Data Centers. Section 4 introduces our proposal of enhancing the ngDC with Security SLAs based on the adoption of SPECS. In particular, this section focuses on EMC storage solutions. Section 5 describes the architecture of the ngDC storage testbed and the enhanced security features. Finally, Section 6 gives an overview of related work on frameworks and guidelines for SLAs, while Section 7 summarizes the conclusions and provides direction for future work.

2 THE SPECS FRAMEWORK

The SPECS framework provides services and tools to build applications offering services with security features defined in, and granted by a Security SLA (Casola et al., 2014),(Rak et al., 2013).

The framework addresses both CSPs' and users' needs by providing tools for 1) enabling user-centric negotiation of security parameters in a Security SLA; 2) providing a trade-off evaluation process among CSPs; 3) real time monitoring of the fulfilment of SLAs agreed with CSPs; 4) notifying both End-users and CSPs in the event that an SLA is violated; 5) enforcing agreed SLAs in order to maintain the agreed security levels. The SPECS framework is also able to "react and adapt" in real-time to fluctuations in the security level by applying the required countermeasures.

In order to provide security capabilities granted by Security SLAs, a SPECS Application orchestrates the so called *SPECS Core Services* dedicated to the *Negotiation*, *Enforcement* and *Monitoring* of an SLA. Through these core services, the cloud service is enhanced with security capabilities guaranteed by the signed SLA

In SPECS, four primary actors have been defined:

- **End-user:** The CSC of a Cloud service;
- **SPECS Owner:** The Cloud service provider;
- **External CSP:** An independent (typically public) CSP, unaware of the SLA, providing only basic resources without security guarantees;
- **Developer:** Supports the SPECS Owner in the development of SPECS applications.

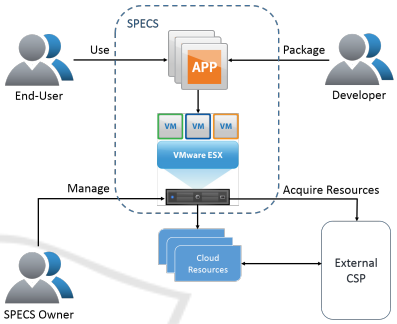


Figure 1: SPECS Entity Relationships.

As illustrated in Figure 1, the interactions among the parties are very simple: the End-user uses the Cloud services offered by the SPECS Owner, which acquires resources from External CSPs, enriched with capabilities to meet the End-user's security requirements. SPECS then monitors and enforces the End-user's security requirements to ensure the agreed security levels and alert the End-user of any breaches in the terms of the Security SLA.

3 NEXT GENERATION DATA CENTER STORAGE

The ngDC is a highly efficient and optimized data center that allows organisations to achieve more within the confines of the available resources (physical servers, power, cooling, facilities, etc.). The key advantage of the ngDC is its agility and ability to adapt rapidly to changes in an organizations business and workload requirements.

This efficiency is achieved in a ngDC by consolidating the physical resources, in other words virtualizing it. As illustrated in Figure 2, we view the classical data center model as one in which there are dedicated physical resources for each application. The

[2]http://www.emc.com/vipr

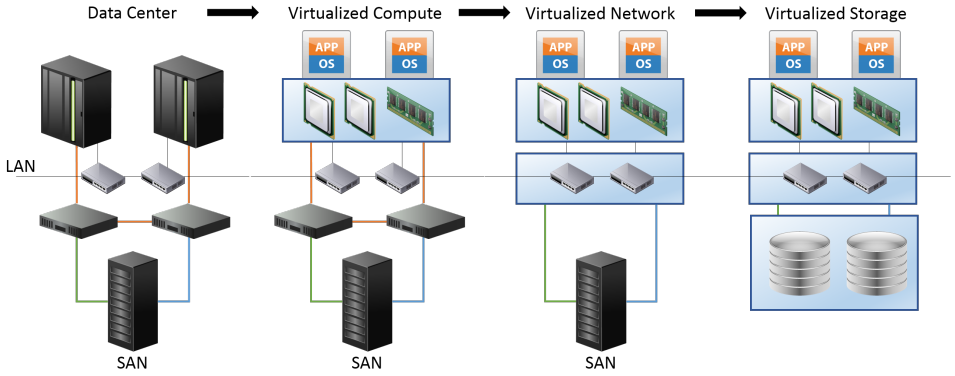


Figure 2: Evolution of the data center towards a fully Virtualized environment.

first step in evolving towards the ngDC is to move away from dedicated resources to consolidated resources virtualizing the physical compute resources though the use of Hypervisor technologies.

The second evolutionary step consists of virtualizing the network resources, dividing them into discrete segments to isolate and segregate the traffic and/or the service by creating virtual networking components (e.g. virtual LANs, virtual SANs, virtual switches, etc.) that are part of a Hypervisor, logical links, and even converged networks.

The final phase before achieving a completely virtualized data center is to abstract out the physical storage resources. In the classic storage model, an Intelligent Storage System is used to group disks together and then partition those physical disks into discrete logical disks. These logical disks are assigned a Logical Unit Number (LUN), and are presented to a host, or hosts, as a physical device. Redundancy of the data stored on the disks is provided by RAID (Redundant Array of Independent Disks) technology, which is applied at either the physical disk layer or the logical disk layer.

This classic model has several limitations however. For example, there is an upper limit to the maximum number of physical disks that can be combined to form a logical disk. Another issue is that often the amount of storage provisioned for each application is greater than what is actually needed in order to prevent application downtime. Both of these situations results in inefficient usage of the physical storage resources that needlessly remain idle.

These kinds of inefficiencies can be resolved by introducing Software Defined Storage (SDS) applications such as EMC's ViPR in order to virtualize the tiered storage resources. The outcome is a more efficient usage of resources which result in reduced power and space costs in the data center as well as reduced workloads for storage and server administrators. The power of these SDS solutions is the abstraction of the physical resources by creating resource pools designed to support more generalized workloads across applications. This enables the capacity usage and requirements to be more closely monitored and aligned to the available resources - further reducing the operational costs.

But what about software-defined security? Most (or all) of the security controls can be automated and managed through software, depending on how virtualized the infrastructure is. Such an approach requires any service to be *controlled* under some security policy. The innovative idea proposed in SPECS to enhance the ngDC, is to provide Security-as-a-Service (SecaaS) according to agreed Security SLA. To achieve this, in following sections, the integration of the ngDC with the SPECS framework is proposed such that the full Security SLA life cycle can be managed.

4 INTEGRATING SPECS WITH ngDC

In a ngDC, the infrastructure is virtualised, delivered as a service and controlled by management applications. This shift in the architectural approach for the data center offers a more agile, flexible and scalable model. The core idea is the decoupling of the hardware from the software layer. Indeed, services (OSs, applications and workloads) view these abstracted, virtual resources as though they were physical compute, storage and network resources. Figure 3 illustrates the relationships between the infrastructure layer, including different physical resources, and the service and application layers.

Despite the multitude of benefits available when leveraging a Cloud infrastructure, wide scale Cloud adoption for sensitive or critical business applications

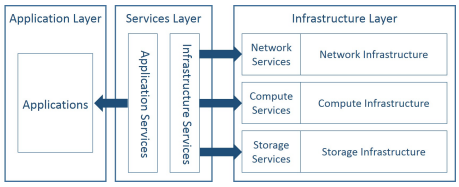


Figure 3: Next Generation Data Center Architecture.

still faces resistance due to concerns over the privacy and security of the data, workloads and applications outsourced to the Cloud provider's data centers. Cloud providers typically offer a set of security measures advertised to potential customers, however without the ability to provide assurance of those security measures or to maintain visibility over the service, the Cloud customer has no way to verify the service is being provided as described.

Integrating SPECS with the ngDC offers a SecaaS solution, not only by establishing a process to negotiate and monitor services running in the data center, but also building on the native security features present by providing additional security features delivered through virtual machines dynamically allocated and instantiated on the data center to meet the security requirements. Combined with the guarantees provided through a Security SLA, these security features improve the confidence with which end users can migrate their applications and data to the Cloud.

Figure 4 illustrates where the SPECS platform integrates with a typical ngDC architecture. In EMC's use case, ViPR is used to offer software defined storage management for the ngDC storage resources.

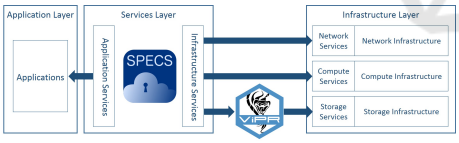


Figure 4: SPECS Enhanced Data Center Architecture.

4.1 Providing ngDC using SPECS Core Services

In Figure 5 the usage of SPECS to provide ngDC services is illustrated: the SPECS platform is used to negotiate an SLA for storage resources provided by ViPR. On receipt of the SPECS negotiated offer, the End-user can sign the SLA which will trigger the Enforcement phase of SPECS, making the newly acquired resources available to the End-user. In parallel to this, the Monitoring module is configured so that the resources are continuously monitored. The three phases are described in detail in the following subsections.

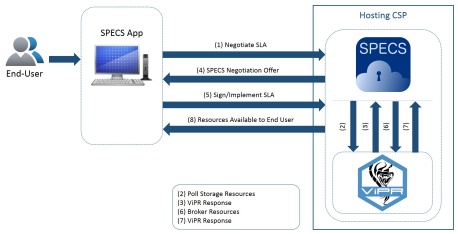


Figure 5: SPECS Service Negotiation/Brokering Service.

4.1.1 Negotiation

Formatted according to the SPECS Security SLA format (De Benedictis et al., 2015), security features are represented using few simple concepts: *Security capabilities*, the set of security controls (NIST, 2013) that a security mechanism is able to enforce on the target service; *Security metrics*, the standard of measurement adopted to evaluate security levels of the services offered; *Security Level Objectives (SLOs)*, the conditions, expressed over security metrics, representing the security levels that must be respected according to the SLA.

Security-related SLOs are negotiated based on the SPECS Customer's requirements. A set of compliant offers, each representing a different supply chain to implement, is identified and validated. The agreed terms are included in a Security SLA that is signed by the SPECS Customer and the SPECS Owner.

4.1.2 Enforcement

Once the SLA has been successfully negotiated, it is implemented through the Enforcement services, which acquire resources from External CSPs and activate the appropriate components (that implement security capabilities). This approach provides security capabilities *as-a-Service* to fulfil the SLOs included in the signed Security SLA.

Each identified security capability is implemented by an appropriate security mechanism able to cover a set of pre-defined security controls. In SPECS, a security mechanism is a piece of software dedicated to implementing security features on the target service. The information associated with a security mechanism is included in the mechanism's metadata, prepared by the mechanism's developer and includes all information needed to automate the security mechanism's deployment, configuration and monitoring.

Cloud-automation tools, such as Chef[3], can be used to automatically implemented the security capabilities required in the SLA through the Enforcement services.

[3]https://www.chef.io/chef/

4.1.3 Monitoring

In the Enforcement phase, the appropriate monitoring components are also configured and activated. The activation of monitoring components includes the launching of services and agents that are able to monitor the specific parameters included in the Security SLA. These services and agents, which may be represented by existing monitoring tools integrated within the framework, generate data that is collected and processed by the SPECS Monitoring module (Casola et al., 2015).

Under specific conditions, the Monitoring module generates monitoring events, which are further processed to verify whether they reveal a violation of the SLA or indicate a possible incoming violation. As a consequence, if a violation occurs, corrective countermeasures may be adopted consisting of reconfiguring the service being delivered, taking the appropriate remediation actions, or notifying the the End-User and renegotiating/terminating the SLA.

5 THE SPECS ENHANCED ngDC STORAGE TESTBED

A core objective of the SPECS framework is to deploy cloud services with user defined security capabilities guaranteed by a Security SLA. SPECS allows the End-user to express the desired capabilities in the Security SLA using a reference standard for guidance and clarity (e.g. Cloud Control Matrix (CCM) 3.0(CSA, 2015) and NIST SP 800-53 (NIST, 2013)).

This section describes the testbed used to integrate SPECS and ViPR, the ViPR usage model and the additional security features delivered *as-a-Service* and guaranteed by a Security SLA.

5.1 Physical and Software Testbed

The core components of the architecture, illustrated in Figure 6, are: (i) ESXi server; (ii) Cisco Switch; (iii) VMAX array; (iv) Management Server.

The management server, running Windows Server 2008 R2 (W2K08), is used to set up and manage the network to which the VMAX array is connected. Additionally, EMCs SMI-S provider[4] must be installed on this system in order to enable the management of VMAX via ViPR. The VMAX array itself consists of the VMAX controller and two VMAX bays equipped with 800 disks for a total available storage space of 200TB. ESXi[5] is VMware's bare-metal hypervisor that virtualizes servers and is installed directly on top of the physical server, partitioning resources into multiple virtual machines. These core components are connected via high speed fiber channel managed by a Cisco switch.

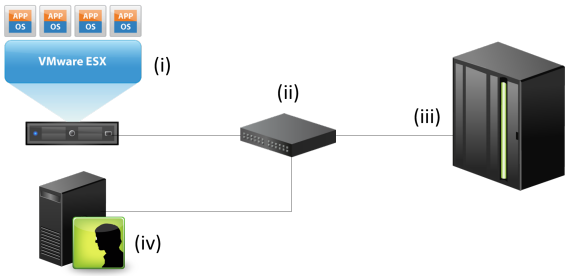


Figure 6: Physical Architecture.

In addition to these core components, the following technologies are also used to support the test environment:

- VCenter Server: Provides a centralized and extensible platform for managing virtual infrastructure.
- EMC ViPR Controller: Storage automation software
- Chef: Powerful automation platform that is able to automate the configuration, deployment, and management of VMs across different networks.

Figure 7 illustrates the high level configuration of the Chef Server alongside the SPECS core provider. In this configuration, Chef is used to install and configure applications, and to deploy VMs. Services selected from the list of available Chef cookbooks via SPECS are deployed from the Chef Server as a Chef recipe, launching a VM preconfigured to execute the security service.

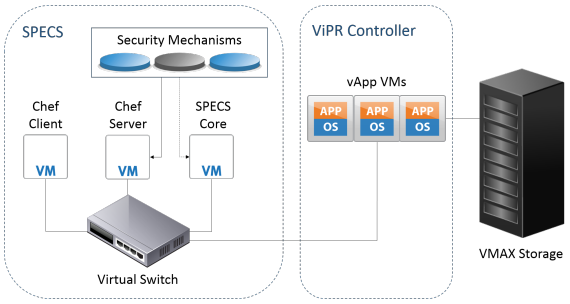


Figure 7: Software Architecture.

As can also be seen in Figure 7, the ViPR controller is run as a virtual appliance (vApp) on the

[4]https://community.emc.com/docs/DOC-19629

[5]https://www.vmware.com/products/vsphere-hypervisor

ESXi server with the VMAX storage in the back-end supplying the physical resources. The ViPR vApp is deployed using the 3+2 configuration file for redundancy purposes (available from EMC support[6]). In this deployment configuration, five virtual machines are used to run the vApp, with two VMs able to fail without affecting the availability of the vApp.

5.2 ViPR Storage Service

The ViPR controller, accessible as a web application running as a vApp on an ESXi server, offers End-users virtual pools of storage resources using the *as-a-Service* model. Using the ViPR REST API to execute commands, the SPECS framework can access all the functionality available through the controller. Furthermore, this enables SPECS to allocate storage services with additional security controls that can be negotiated, for example Business Continuity Management and Operational Resilience (BCR-01, BCR-09 and BCR-11 in the CCM control framework).

While it is possible for the End-user to set up security features for the storage directly via ViPR, this requires significant technical and security expertise and should be restricted to IT or Security administrators. In contrast to this, the SPECS negotiation interface is intuitive to personnel without specific administration expertise, enabling them to select security requirements. Furthermore, the End-user can monitor the enforcement of the security metrics over which the SLOs have been defined.

For the evaluation and testing of the SPECS framework, the security control baselines defined in NIST SP 800-53 were selected to provide a standardised mapping to the security mechanisms offered by SPECS. This paper presents different security controls across categories such as *Access Control*, *Identification and Authentication*, *Physical and Environmental Protection*, and *System and Information Integrity*.

Table 1 shows some of the possible mappings used between the NIST security controls and the security features for Cloud storage services, expressed through security metrics and their description.

On selecting the *EMC ngDC* SPECS application from the SPECS portal, the End-user can choose from different service configuration parameters categorised into the following *Security Capabilities*:

- Secure Storage Capabilities: Security capabilities added to support services offered by storage providers.

[6]https://support.emc.com/downloads/32034_ViPR

Table 1: Sample mappings between NIST Security Controls and SPECS Security Features.

Metric	Description	NIST mapping
RAID Level(s)	Defines the RAID level the volumes in the virtual pool will consist of.	SA-2, SC-6, CP-9, CP-10, SI-17
SAN Multi-Path	The number of paths that can be used between a host and a storage volume.	SC-6, SI-17
Data Geolocation	Defines in which data center the virtual storage and its copies are located.	PE-17, PE-18, PE-20, SI-12
Max Mirrors	Defines the Maximum number of data storage mirrors.	SC-5, SC-6, SI-13

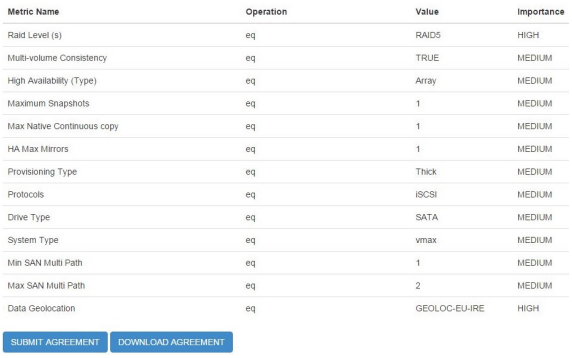
- Availability Capabilities: Capabilities providing redundancy and business continuity in the event of security incidents involving the storage service.

Each type of capability is responsible for a specific security aspect and is associated with a group of security controls. For example, the *Availability Capabilities* are associated with SC-6 (Resource Availability) and SI-17 (Fail-Safe Procedures) as defined in NIST SP 800-53 for Security and Privacy Controls (FORCE and INITIATIVE, 2013).

On selecting the type of capabilities required for the storage service, the End-user is then presented with the available capabilities under the selected categories. For example, the *Availability Capabilities* category includes capabilities such as RAID level, High Availability, Maximum Snapshots, etc.

Once the End-user has specified their requirements, the SPECS portal will display an overview of the capabilities requested for the storage service, as shown in Figure 8. This form displays the metric, the associated value and the importance weight associated with each.

Once the Agreement has been submitted and signed, the Implementation function (of the Enforcement module) implements the signed SLA by making a series of requests via the ViPR REST API to set up the storage service according to the requested capabilities and security mechanisms. Furthermore, during the implementation phase, the ViPR monitoring agents are configured according to the metrics specified in the SLA. The SPECS Monitoring module can then make requests via ViPR's REST API to continuously check the status of the allocated storage and verify if any SLA violation occurs.



Metric Name	Operation	Value	Importance
Raid Level (s)	eq	RAID5	HIGH
Multi-volume Consistency	eq	TRUE	MEDIUM
High Availability (Type)	eq	Array	MEDIUM
Maximum Snapshots	eq	1	MEDIUM
Max Native Continuous copy	eq	1	MEDIUM
HA Max Mirrors	eq	1	MEDIUM
Provisioning Type	eq	Thick	MEDIUM
Protocols	eq	iSCSI	MEDIUM
Drive Type	eq	SATA	MEDIUM
System Type	eq	vmax	MEDIUM
Min SAN Multi Path	eq	1	MEDIUM
Max SAN Multi Path	eq	2	MEDIUM
Data Geolocation	eq	GEOLOC-EU-IRE	HIGH

Figure 8: SLA negotiated through SPECS.

Once the enforcement process is successfully completed, the resources are available through the ViPR administration interface. The capabilities requested through SPECS are reflected in the provisioned storage.

6 RELATED WORK

The drive towards the adoption of SLAs by CSPs is an important initiative in strengthening the trust in services. SLA management frameworks like SLA@SOI (Theilmann et al., 2008) associate services with an SLA, detect SLA violations and are even able to recover from them. Many research projects, like Contrail (Morin, 2011), Optimis[7] and mOSAIC include SLAs in their framework.

ENISA ((Dekker, 2012)(Catteddu, 2011)(Marnix Dekker, 2011)) outlined the need for a Security SLA that offers clear guarantees with respect to the security provided by CSPs to services. Projects like CUMULUS (Pannetrat et al., 2013), A4Cloud (Pearson, 2011), SPECS (Rak et al., 2013), SLAReady [8], SLALOM[9], MUSA (Rios et al., 2015) are actively working on this topic, attempting to clearly model and represent security into an SLA.

Security and compliance issues in the ngDC are a primary concern due to the reliance on traditional security models that have not adapted to virtualization. In the ngDC, and cloud computing as a whole, new, significant risks have been introduced to IT services. Organisations who traditionally hosted workloads and data in internal data centres running on their own infrastructure, now face a loss of visibility and control. The trust boundaries that were clearly established in physical infrastructures are now blurred as virtualized resources are increasingly used.

These new security issues have spawned several research activities into novel solutions to address the security of data in the cloud. For example, Nithiavathy proposes a framework to check the data integrity on CSP using homomorphic token and distributed erasure-coded data (Nithiavathy, 2013). Alternatively, a secure multi-owner data sharing scheme for cloud users using group signature and broadcast encryption was proposed in (Marimuthu et al., 2014).

Other works focus on the security of the communication between distributed Data Centers such as (Talpur et al., 2015), that proposed a security framework to manage a large number of secure connections implemented using Kinetic[10] and Pyretic[11] as a centralized middleware tool. Each of these solutions address a part of the problem, but do not offer a platform on which the CSC can combine security requirements that can be addressed in different application layers, or give formal assurance to End-user through SLAs.

7 CONCLUSIONS

Next generation Data Centers provide a significant evolution how resources, such as storage, network and compute, can be dynamically provisioned. The ngDC offers the possibility to virtualize resources and dynamically pool them according to customer needs in an *Infrastructure-as-a-Service* provisioning model.

To achieve broader adoption, datacenter customers need more guarantees about the security levels provided, creating the need for tools to negotiate security requirements and to be able to monitor their enforcement. This paper has investigated the potential of integrating the SPECS platform with the commercially available ViPR storage solution from EMC. This integration was shown to offer security *as-a-service*, enhancing the security provided by the ViPR, and guaranteed by a Security SLA.

In particular, this paper has illustrated, with a real case study, how it is possible to negotiate, enforce and monitor a Security SLA in a ngDC architecture. Potential future directions from this work should focus on the definition of new security metrics that can be easily measured and monitored in order to provide new security capabilities to a storage infrastructure and enable a CSP to enrich its security service offerings.

[7]http://www.optimis-project.eu/
[8]http://www.sla-ready.eu/
[9]http://slalom-project.eu/
[10]http://resonance.noise.gatech.edu/
[11]http://frenetic-lang.org/pyretic/

ACKNOWLEDGEMENTS

This research is partially supported by the EC FP7 project SPECS (Grant Agreement no. 610795).

REFERENCES

Casola, V., Benedictis, A. D., and Rak, M. (2015). Security monitoring in the cloud: An SLA-based approach. In *10th International Conference on Availability, Reliability and Security, ARES 2015, Toulouse, France, August 24-27, 2015*, pages 749–755.

Casola, V., Benedictis, A. D., Rak, M., and Villano, U. (2014). Preliminary Design of a Platform-as-a-Service to Provide Security in Cloud. In *CLOSER 2014 - Proceedings of the 4th International Conference on Cloud Computing and Services Science, Barcelona, Spain, April 3-5, 2014.*, pages 752–757.

Catteddu, D. (2011). Security & resilience in governmental clouds. Technical report, CSA.

CSA (2015). Cloud controls matrix v3.0.

CSCC (2012). The cscc practical guide to cloud service level agreements. Technical report, CSCC.

Davidson, E. A. (2013). The Software-Defined-Data-Center (SDDC): Concept Or Reality? [VMware].

De Benedictis, A., Rak, M., Turtur, M., and Villano, U. (2015). Rest-based sla management for cloud applications. In *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2015 IEEE 24th International Conference on*, pages 93–98.

Dekker, M. (2012). Critical cloud computing a ciip perspective on cloud computing services. Technical report, ENISA.

EC (2011). Unleashing the potential of cloud computing in europe. Technical report, EC.

FORCE, J. T. and INITIATIVE, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800:53.

International Organization for Standardization (2014). ISO/IEC NP 19086-1. Information Technology–Cloud computing–Service level agreement (SLA) framework and technology–Part 1: Overview and concepts.

Marimuthu, K., Gopal, D. G., Kanth, K. S., Setty, S., and Tainwala, K. (2014). Scalable and secure data sharing for dynamic groups in cloud. In *Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on*, pages 1697–1701. IEEE.

Marnix Dekker, G. H. (2011). Survey and analysis of security parameters in cloud slas across the european public sector.

Morin, C. (2011). Open computing infrastructures for elastic services: contrail approach. In *Proceedings of the 5th international workshop on Virtualization technologies in distributed computing*, pages 1–2. ACM.

NIST (2013). SP 800-53 Rev 4: Recommended Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, NIST.

Nithiavathy, R. (2013). Data integrity and data dynamics with secure storage service in cloud. In *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on*, pages 125–130. IEEE.

Pannetrat, A., Hogben, G., Katopodis, S., Spanoudakis, G., and Cazorla, C. (2013). D2.1: Security-aware sla specification language and cloud security dependency model. technical report, certification infrastructure for multi-layer cloud services (cumulus).

Pearson, S. (2011). Toward accountability in the cloud. *Internet Computing, IEEE*, 15(4):64–69.

Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., and Villano, U. (2013). Security as a service using an sla-based approach via specs. In IEEE, editor, *Proceedings of IEEE CloudCom Conference 2013*.

Rios, E., Iturbe, E., Orue-Echevarria, L., Rak, M., and Casola, V. (2015). Towards self-protective multi-cloud applications - MUSA - a holistic framework to support the security-intelligent lifecycle management of multi-cloud applications. In *CLOSER 2015 - Proceedings of the 5th International Conference on Cloud Computing and Services Science, Lisbon, Portugal, 20-22 May, 2015.*, pages 551–558.

Talpur, S. R., Abdalla, S., and Kechadi, T. (2015). Towards middleware security framework for next generation data centers connectivity. In *Science and Information Conference (SAI), 2015*, pages 1277–1283. IEEE.

Theilmann, W., Yahyapour, R., and Butler, J. (2008). Multi-level sla management for service-oriented infrastructures. In *Proceedings of the 1st European Conference on Towards a Service-Based Internet*, ServiceWave '08, pages 324–335, Berlin, Heidelberg. Springer-Verlag.