Security SLA in Next Generation Data Centers, the SPECS Approach

Massimiliano Rak[1], Valentina Casola[2(✉)], Silvio La Porta[3], and Andrew Byrne[3]

[1] Dipartimento di Ingegneria dell'Informazione, Seconda Università di Napoli, Aversa, Italy
massimiliano.rak@unina2.it
[2] Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione, Università di Napoli Federico II, Napoli, Italy
casolav@unina.it
[3] EMC Ireland COE Innovation, Cork, Ireland
{silvio.laporta,andrew.byrne}@emc.com

Abstract. Next generation Data Centers (ngDC) provide a significant evolution how storage resources can be provisioned. They are cloud-based architectures offering flexible IT infrastructure and services through the virtualization of resources: managing in an integrated way compute, network and storage resources. Despite the multitude of benefits available when leveraging a Cloud infrastructure, wide scale Cloud adoption for sensitive or critical business applications still faces resistance. One of the key limiting factors holding back larger adoption of Cloud services is trust. To cope with this, 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 use case from EMC that integrates the SPECS Platform with their innovative solutions for the ngDC. In particular, the paper illustrates how it is possible to negotiate, enforce and monitor a Security SLA in a cloud infrastructure offering.

Keywords: Cloud · ngDC · Cloud security · Security SLA

1 Introduction

Storage services, as many IT services, are increasingly moving toward the virtualized, distributed cloud model. Indeed, recent concepts like ngDC or Software-Defined Data Centers (SDDC) [6] 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 a significant advantage of the

M. Helfert et al. (Eds.): CLOSER 2016, CCIS 740, pp. 151–169, 2017.
DOI: 10.1007/978-3-319-62594-2_8

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.

This solution is very attractive from an organisation's perspective offering economic benefits as well as providing increased resilience and accessibility of services. However, one of the main challenges hindering broad-scale 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.

This is primarily due to concerns over the privacy and security of the data, workloads, and applications, outsourced to the Cloud provider's data centers. 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. 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 that the service is being provided as described. 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.

For example, Amazon and Google offer, on their Cloud storage services, an SLA that details the remediation process (partial reimbursement of payment, credit for extended service period, etc.) available to the customer, in the event that the monthly uptime of their services does not meet the 99.9% offering. However, customers are unable to request more specific requirements and are reliant on the CSP itself to report the actual measurement of the service uptime.

Despite the intense research efforts into developing standards and frameworks for SLAs [5,9,11,14,23], 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 enforce and 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. In this paper, we aim to address both the needs of the CSP (offering secure services on an ngDC to customers according to an agreed SLA), and the CSC (negotiating the level of security granted by providers). In particular, we integrate SPECS with vSphere[2] and ViPR storage controller[3], two commercial products offered as a service by EMC to fulfil the ngDC components by offering

[1] http://www.specs-project.eu/.
[2] https://www.vmware.com/it/products/vsphere.
[3] http://www.emc.com/vipr.

virtual machines running services on top of storage resources. The acquisition and configuration of these services are managed through SPECS and are formally defined in Security SLAs which guarantee the performance and security requirements of the services.

The implementation of security capabilities, enforced and monitored through SPECS demonstrates the effectiveness of Security SLAs as a concrete solution that can be adopted by commercial products and services. 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: Sect. 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, Sect. 6 gives an overview of related work on frameworks and guidelines for SLAs, while Sect. 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 [1,20].

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.

As illustrated in Fig. 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

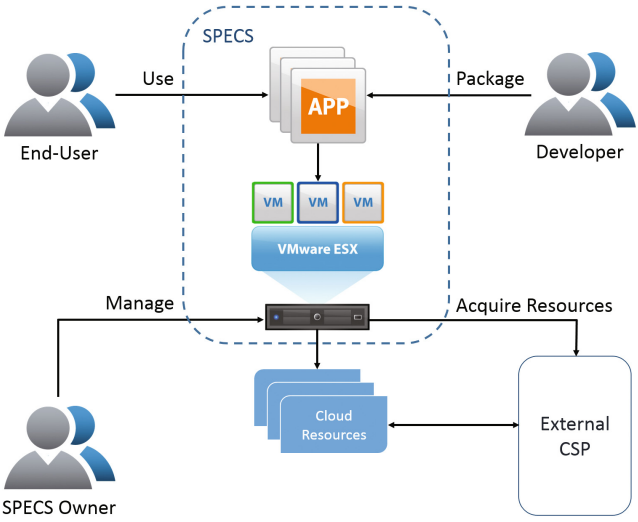

Fig. 1. SPECS entity relationships.

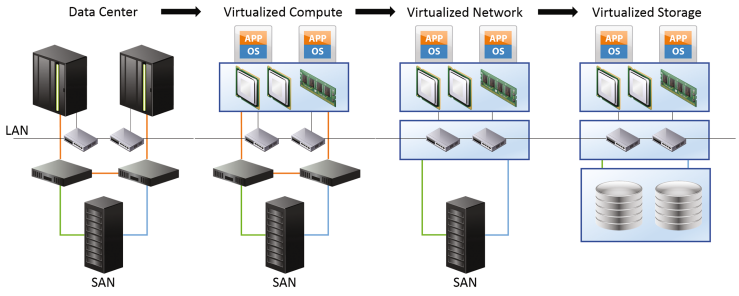

Fig. 2. Evolution of the data center towards a fully virtualized environment.

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 Fig. 2, we view the classical data center model as one in which there are dedicated physical resources for each application. The 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 in the management of storage 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 an 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.

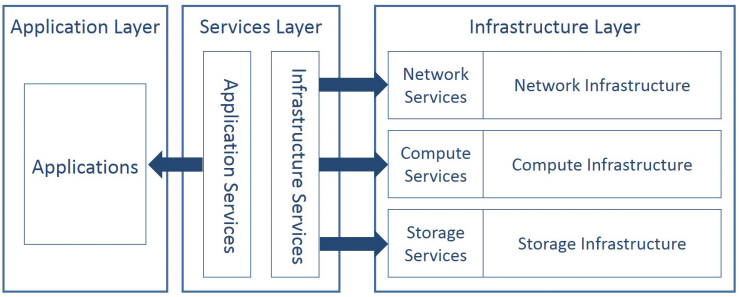

Fig. 3. Next generation data center architecture.

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

To provide validation of the SPECS platform as a solution to address these concerns, through the use of Security SLAs to guarantee services, the use case illustrated in Fig. 4 was established. This use case represents a typical scenario in which an End-user wishes to deploy a service on a Virtual Machine on storage configured to their performance and security requirements. The candidate technologies used here are vSphere and ViPR storage controller. While the technologies are effective in achieving their objectives, they require advanced technical expertise in order to deploy services correctly. Typically, this requires dedicated management from IT personal to handle End-user requests for resources and services.

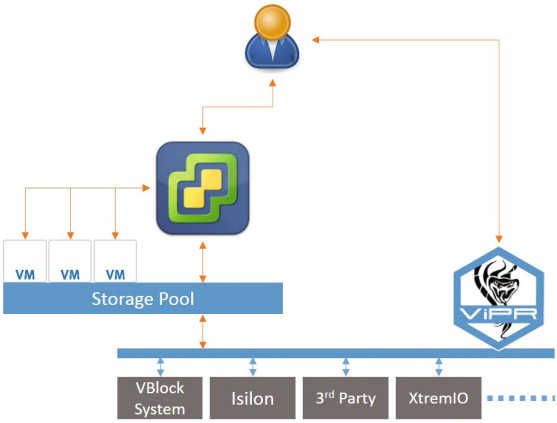

Fig. 4. EMC ngDC use case.

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 5 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 while vSphere provides central management of the compute resources.

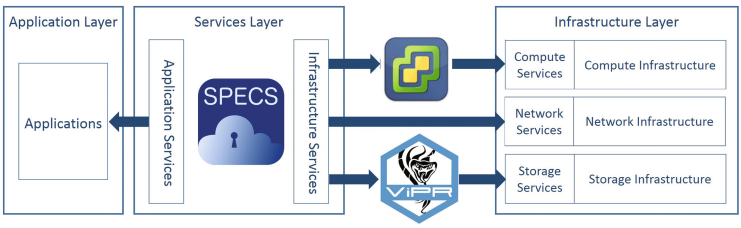

Fig. 5. SPECS enhanced data center architecture.

The SPECS framework provides the core functionality (negotiation, enforcement and monitoring) and the interface between the SPECS application presented to the End-user and the services they are requesting (e.g., storage service through ViPR). Operating at this level in the overall architecture, additional

security mechanisms (such as End-to-End Encryption, AAA-as-a-Service and Data Geolocation) can be added through SPECS to the storage service that enhance the security offerings available natively by the storage service.

To enable the integration of SPECS with ViPR, an adaptor component was developed to make use of the ViPR REST API to manage the service. The adaptor allows the Enforcement and Monitoring modules to send requests and receive response from the ViPR Controller relating to available resources, performance options and security mechanisms.

The new End-user interactions with the ngDC, via SPECS, are illustrated in Fig. 6. It can be clearly seen that the interactions with individual tools have been abstracted from the End-user by SPECS, enabling them to quickly and easily define requirements, negotiate the SLA and deploy their service. A new component, Chef[4], has been added to the use case. Chef provides End-user with an extensible set of services that can be deployed on the acquired resources.

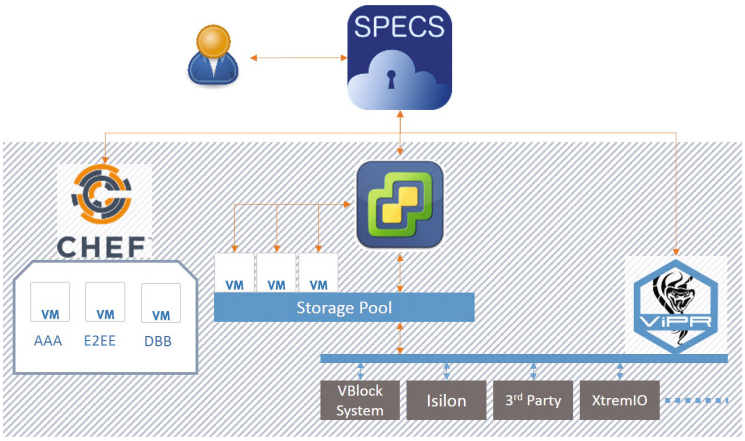

Fig. 6. SPECS service negotiation/brokering service.

For an End-user to instantiate a service on top of SPECS, first, the End-user negotiates the storage requirements through SPECS, resulting in the acquisition of cloud storage according to the Security SLA. In order to deploy services (running on Virtual Machines provisioned on the storage acquired in the previous step), the End-user then selects from the security services available through SPECS. The following subsections provide more detail on these processes.

4.1 Providing Storage Service Using SPECS Core Services

Figure 7 outlines the End-user interactions with SPECS, and subsequent interactions between SPECS and ViPR, to provide cloud storage resources. The initial step involves the negotiation of the SLA for storage resources through the

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

SPECS platform. Here, we consider only ViPR to provide storage resources though SPECS is capable of support other providers such as AWS S3. Once the SLA has been negotiated and submitted, SPECS queries the storage services, namely ViPR, to determine if the End-user requirements can be satisfied. SPECS returns the negotiated offer to the End-user, who can sign the SLA, triggering the Enforcement phase of SPECS. This phase brokers the resources and makes 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.

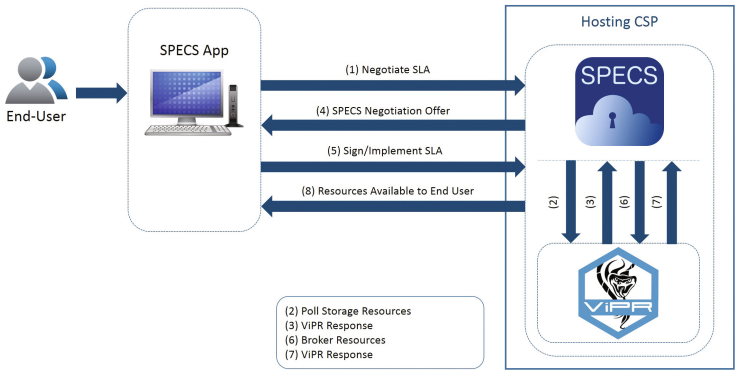

Fig. 7. SPECS service negotiation/brokering service.

Negotiation. Formatted according to the SPECS Security SLA format [7], security features are represented using few simple concepts: *Security capabilities*, the set of security controls [15] 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 and feasible 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.

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, can be used to automatically implemented the security capabilities required in the SLA through the Enforcement services.

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 [2].

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 End-User and renegotiating/terminating the SLA.

4.2 Providing SPECS Applications on Top of ngDC

In order to illustrate the process of offering services through SPECS on top of ngDC we focus on a simple example related to the acquisition by a web developer (the End-user) of a web container enhanced with a set of security features (refer to [19] for a deeper description of the SPECS application development).

It is reasonable to suppose that the End-user is not a security expert, in that he/she is aware of the technologies that may be involved (SSL, authentication and authorization protocols, etc.), but has no detailed knowledge of the best practices and of how to protect their application from malicious attacks. For this reason, the acquisition of VMs hosting the web container and the enforcement of security features are accomplished through SPECS.

It should be noted that, at the state of the art, even if the web developer acquires VMs from a public CSP, he/she is the only person responsible for setting up any security configuration. Existing appliances offer predefined services (for example, a pre-configured web server), but checking and comparing the security features offered by different CSPs is not an easy task. The web developer has to (i) manually find the security features provided by each CSP, (ii) evaluate and compare existing offers, (iii) apply a suitable configuration, if not natively supported, and (iv) implement a monitoring solution to verify at runtime the respect of the security features.

The SPECS ecosystem provides a turnkey solution to the above issues, as it (i) offers a single interface to choose among multiple offerings on multiple providers, (ii) enables the web developer to specify explicitly the needed security capabilities on the target web container, (iii) automatically configures the VMs in order to enforce the security controls requested, (iv) offers a set of security metrics to monitor the respect of the security features requested, (v) enables continuous monitoring of the security metrics negotiated, and (vi) can automatically remediate to (some of the) alerts and violations that may occur to the SLA associated to the web container.

Moreover, running on top of the ngDC it is possible to negotiate the storage pool on top of which the Web Container will run, granting that the web server files will reside on a storage that have a set of security features agreed through the SLA.

In order to deliver web servers, pre-configured according to security best practices, we developed a mechanism named *WebContainerPool* devoted to automatically deploying and configuring a pool of web servers over a set of Virtual Machines acquired on the hosting ngDC. The developed mechanism not only provides the web server cloud service, but it also offers some reliability features, measured in terms of the two metrics (i) `LevelofRedundancy` and (ii) `LevelofDiversity`. The former ensures resiliency to failures through replication of the web container instances (used transparently by the End-user), while the latter ensures resiliency to vulnerability-based attacks by employing different software and/or hardware instances of the same web container.

In practice, the *WebContainerPool* mechanism has been developed as a security mechanism, and includes a set of pre-configured web servers (at the state of the art, Apache and Ngnix) and a load balancer (based on HAProxy). Web servers are synchronized through Memchached, so that the accesses to the web application are synchronized. The Chef cookbook associated to the *WebContainerPool* can be used also independently of the SPECS framework. It is worth pointing out that, if the aim is to apply the same process to a different cloud service (e.g., a Secure CMS), it is first necessary to develop a Cloud service cookbook dedicated to offer the CMS, and later on to select the security mechanisms that can be offered for it, possibly developing custom ones.

The proposed service (web container), as outlined above, relies on (a pool of) virtual machines, hosting synchronized web servers. The service offers some integrated security features (redundancy and diversity), but a lot of additional security capabilities can be provided. In SPECS three main security mechanisms are already available:

- **TLS:** it is a preconfigured TLS server, configured according to security best practices.
- **SVA (Software Vulnerability Assessment):** it regularly performs vulnerability assessment over the virtual machines, through software version checking and penetration tests.
- **DoSprotection:** it consists in a solution for denial of service attacks detection and mitigation based on the OSSEC tool.

5 The SPECS Enhanced ngDC 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 [4] and NIST SP 800-53 [15]).

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 Fig. 8, 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[5] 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 200 TB. ESXi[6] 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.

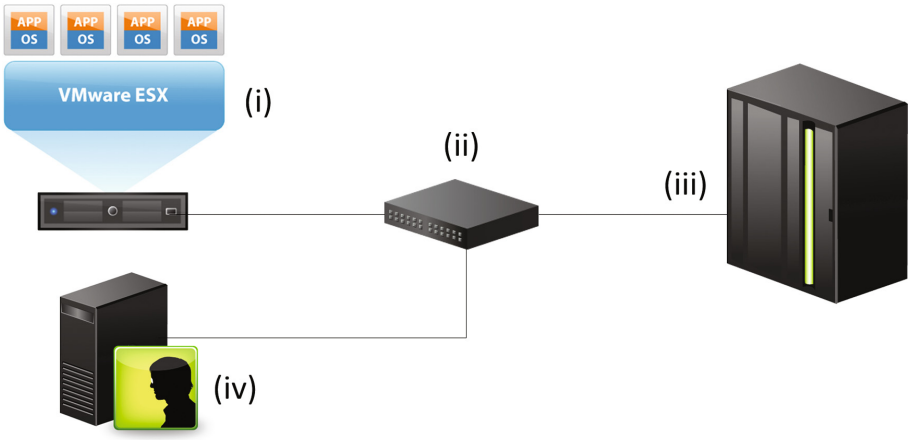

Fig. 8. Physical architecture.

[5] https://community.emc.com/docs/DOC-19629.
[6] https://www.vmware.com/products/vsphere-hypervisor.

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

- VMWare vSphere ESXi: Delivers industry-leading performance and scalability with benefits including improved reliability and security, streamlined deployment and configuration, higher management efficiency, simplified hypervisor patching and updating. It is the platform in which the entire system runs.
- VCenter Server: Provides a centralized and extensible platform for managing virtual infrastructure. vCenter Server manages VMware vSphere environments, giving IT administrators simple and automated control over the virtual environment to deliver infrastructure with confidence.
- EMC ViPR Controller: Storage automation software based on the open source development project CoprHD[7]. It centralizes and transforms multi-vendor storage into a simple and extensible platform. It abstracts and pools resources to deliver automated, policy-driven storage services on demand via a self-service catalogue. With vendor neutral, centralized storage management, customers can reduce storage provisioning costs up to 73%[8], provide greater choice and deliver a path to the cloud through storage-as-a-service. It is used to abstract the physical layer and to manage the storage resource of the data center.
- Chef: Powerful automation platform that is able to automate the configuration, deployment, and management of VMs across different networks.

Figure 9 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.

As can also be seen in Fig. 9, the ViPR controller is run as a virtual appliance (vApp) on the 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[9]). 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

[7] https://github.com/CoprHD.
[8] https://www.emc.com/collateral/data-sheet/h11750-emc-vipr-software-defined-storage-ds.pdf.
[9] https://support.emc.com/downloads/32034_ViPR.

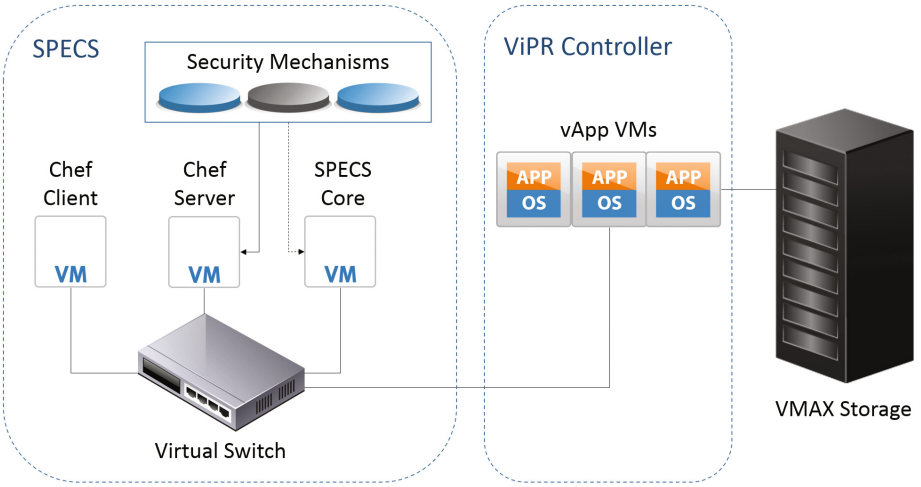

Fig. 9. Software architecture.

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

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

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 [10].

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 Fig. 10. This form displays the metric, the associated value and the importance weight associated with each. The *importance* is an additional specifier, selected by the user, that enables SPECS to make more informed decisions about the service a provider is offering.

The final step in the negotiation process is for the End-user, on review of the negotiated SLA, to sign and, then, implement the SLA. 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. Once the resources have been acquired through SPECS and the SLA has been signed and implemented, End-users can observe the implemented SLAs. 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

SUBMIT AGREEMENT DOWNLOAD AGREEMENT

Fig. 10. 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 [23] associate services with an SLA, detect SLA violations and are even able to recover from them.

Many research projects, like Contrail [14], Optimis[10] and mOSAIC include SLAs in their framework.

ENISA ([3,8,13]) outlined the need for a Security SLA that offers clear guarantees with respect to the security provided by CSPs to services. Projects like CUMULUS [17], A4Cloud [18], SPECS [20], SLAReady[11], SLALOM[12], MUSA [21] 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

[10] http://www.optimis-project.eu/.
[11] http://www.sla-ready.eu/.
[12] http://slalom-project.eu/.

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 [16]. Alternatively, a secure multi-owner data sharing scheme for cloud users using group signature and broadcast encryption was proposed in [12].

Other works focus on the security of the communication between distributed Data Centers such as [22], that proposed a security framework to manage a large number of secure connections implemented using Kinetic[13] and Pyretic[14] 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.

By integrating the ViPR Controller API with SPECS, End-users may negotiate the performance and security capabilities of a Cloud storage service with resources managed transparently through ViPR. The Storage Adaptor created for this integration is platform agnostic and also supports Amazon S3 and the open source CoprHD project. In addition to negotiating capabilities that are native to the target service (e.g. ViPR), the SPECS application offers new security capabilities that enhance the overall security of the target service.

The application described in this paper fully implements the ngDC paradigm by offering storage services protected by Security SLAs through the negotiation, enforcement and monitoring phases.

[13] http://resonance.noise.gatech.edu/.
[14] http://frenetic-lang.org/pyretic/.

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.

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

References

1. Casola, V., De Benedictis, A., Rak, M., Villano, U.: Preliminary design of a platform-as-a-service to provide security in cloud. In: Proceedings of the 4th International Conference on Cloud Computing and Services Science, CLOSER 2014, Barcelona, Spain, 3–5 April 2014, pp. 752–757 (2014)
2. Casola, V., De Benedictis, A., Rak, M.: Security monitoring in the cloud: an SLA-based approach. In: 10th International Conference on Availability, Reliability and Security, ARES 2015, Toulouse, France, 24–27 August 2015, pp. 749–755 (2015)
3. Catteddu, D.: Security and resilience in governmental clouds. Technical report CSA (2011)
4. CSA: Cloud controls matrix v3.0 (2015). https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/
5. CSCC: The CSCC practical guide to cloud service level agreements. Technical report, CSCC (2012)
6. Davidson, E.A.: The Software-Defined-Data-Center (SDDC): concept or reality? [VMware] (2013). http://blogs.softchoice.com/advisor/ssn/the-software-defined-data-center-sddc-concept-or-reality-vmware/
7. De Benedictis, A., Rak, M., Turtur, M., Villano, U.: Rest-based SLA management for cloud applications. In: 2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 93–98, June 2015
8. Dekker, M.: Critical cloud computing a CIIP perspective on cloud computing services. Technical report, ENISA (2012)
9. EC: Unleashing the potential of cloud computing in Europe. Technical report, EC (2011)
10. Force, J.T., Initiative, T.: Security and privacy controls for federal information systems and organizations. NIST Spec. Publ. **800**, 53 (2013)
11. ISO: ISO/IEC NP 19086–1, Information Technology-Cloud computing-Service level agreement (SLA) framework and technology-Part 1: Overview and concepts (2014)
12. Marimuthu, K., Gopal, D.G., Kanth, K.S., Setty, S., Tainwala, K.: Scalable and secure data sharing for dynamic groups in cloud. In: 2014 International Conference on. Advanced Communication Control and Computing Technologies (ICACCCT), pp. 1697–1701. IEEE (2014)
13. Dekker, G.H.M.: Survey and analysis of security parameters in cloud slas across the European public sector (2011). http://www.enisa.europa.eu
14. Morin, C.: Open computing infrastructures for elastic services: contrail approach. In: Proceedings of the 5th International Workshop on Virtualization Technologies in Distributed Computing, pp. 1–2. ACM (2011)
15. NIST: SP 800–53 Rev 4: Recommended Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, NIST (2013)

16. Nithiavathy, R.: Data integrity and data dynamics with secure storage service in cloud. In: 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), pp. 125–130. IEEE (2013)
17. Pannetrat, A., Hogben, G., Katopodis, S., Spanoudakis, G., Cazorla, C.: D2.1: security-aware SLA specification language and cloud security dependency model. Technical report, certification infrastructure for multi-layer cloud services (cumulus) (2013)
18. Pearson, S.: Toward accountability in the cloud. IEEE Internet Comput. **15**(4), 64–69 (2011)
19. Rak, M., Ficco, M., Battista, E., Casola, V., Mazzocca, N.: Developing secure cloud applications. Scalable Comput. Pract. Exp. **15**(1), 49–62 (2014)
20. Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., Villano, U.: Security as a service using an SLA-based approach via specs. In: IEEE Proceedings of IEEE CloudCom Conference 2013 (2013)
21. Rios, E., Iturbe, E., Orue-Echevarria, L., Rak, M., Casola, V.: 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, pp. 551–558 (2015)
22. Talpur, S.R., Abdalla, S., Kechadi, T.: Towards middleware security framework for next generation data centers connectivity. In: Science and Information Conference (SAI), pp. 1277–1283. IEEE (2015)
23. Theilmann, W., Yahyapour, R., Butler, J.: Multi-level SLA management for service-oriented infrastructures. In: Mähönen, P., Pohl, K., Priol, T. (eds.) ServiceWave 2008. LNCS, vol. 5377, pp. 324–335. Springer, Heidelberg (2008). doi:10.1007/978-3-540-89897-9_28