CERTIFIED IT SERVICES IN-A-BOX FOR CLOUD COMPUTING ENVIRONMENTS

Ethan Hadar[1] and Debra J. Danielson[2]
[1]*CA Technologies, Inc., Herzelia, Israel*
[2]*CA Technologies, Inc., Ewing, New Jersey, U.S.A.*

Keywords: Compliance, Cloud Service Marketing and Management, Service Composition, Service Monitoring and Control, IT Financial Management.

Abstract: Certified IT Services in-a-box position paper describes a conceptual architecture and a debatable approach to increasing trust between cloud players, as well as increasing accountability of cloud services providers. The presented conceptual system is comprised of a combination of contemporary IT management services that provide modeling, assembly, automation, assurance and security of IT services, coupled with insurance-based financial remedies. The integrated system constantly conducts auditing and reporting that will be available upon demand in case of a defined incident, by insurance adjustors. This evidence is provided while maintaining the cloud encapsulation and abstraction premise. Business models that increase cloud services consumption; as well as enterprise level compliance fulfillment are among the offerings of this conceptual system. As a result, this paper leads to a hypothesis on the ability of integrated technologies to increase trust and reduce security concerns in cloud consumption, without detracting from the value proposition for cloud services.

1 INTRODUCTION

In the Cloud Computing domain, specifically through Infrastructure as a Service (IaaS) and Software as a Service (SaaS), IT organizations can offload IT capabilities from the organization's internal datacenter and IT resources to public cloud services [9]. Some human resource-related solutions can be outsourced to an external agency to handle difficult issues and to provide service desk solutions. However, lack of trust (Habib, 2010) and external transparency (Ko et al., 2011) are the primary obstacles for cloud usage by enterprise IT organizations. Specifically, data protection, compliance needs by the consumers, and liability are major obstacles (Brandic et al., 2010). Such consumers can not even consider using the provided cloud services, without clear understanding of the target service's compliance. Namely ensuring that the consumed cloud services are compliant to regulation, and in case of a failure, that liability and remedy will be achieved.

Such remedy may be provided by an insurance provider. This agency must have proof that an event has occurred that constitutes a valid claim against the policy (Insurance Event) to proceed with the remedy; this evidence usually found on audit logs, transactions monitoring or other reporting tools of the IT activities. Insurance events are defined within a written policy, and are limited only to that which can be agreed upon by the consumer and supplier and to what can be measured and proved.

The introduction of an insurance remedy into the cloud consumer / provider relationship limits the damage to the cloud consumer caused by failures of the cloud provider and changes the risk equation for adoption of the cloud service.

Today's on-premise IT management toolsets can provide all these monitoring tools, and provide reporting and auditing as well as identity and access enforcement (Heiser and Nicolett, 2008). Connecting these existing solutions to certification and insurance authorities, as well as providing recorded evidence on demand, addresses the needs for trust, transparency, and compliance (Blakley, 2011; Blum et al., 2011; Brandic et al., 2010) on demand between providers and consumers of cloud services.

This position paper illustrates a conceptual system that solves the certification needs that increase trust and compliance transparency within cloud environments.

Hadar E. and Danielson D..
CERTIFIED IT SERVICES IN-A-BOX FOR CLOUD COMPUTING ENVIRONMENTS.
DOI: 10.5220/0003897202110215
In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science* (CLOSER-2012), pages 211-215
ISBN: 978-989-8565-05-1

2 ADVANTAGES OF THE PROPOSED SYSTEM

The *Certified IT Services in-a-Box* system collects reports, data transaction logs, access usages and infrastructure changes. These changes include but are not limited to virtualization structural changes, hybrid connectivity to remote servers or fully public infrastructure.. The information is stored (locally or remotely) at a secured electronic vault by the IT management tools vendor as a trusted third party. When there is a possibility of an insurance event, the information is provided to the service consumer, provider, and the insurance provider.

Existing infrastructure services may have enhanced security or monitoring tools. The modification in this system is the binding of the reported information with contractual financial agreements and risk mitigation through an insurance provider. Evidence in the form of logs, reports and auditing, that testify whether or not a failure (data leak, data roaming, service level failure or infrastructure un-authorized change (Blakley, 2011; Blum et al., 2011) occurred, is the differentiator.

Our Certified IT Services in-a-Box system delivers reports and logs to the insurance provider and other involved parties, archives these logs for a period based on applicable regulations and/or any relevant event or breach, and provides them to the stakeholders on demand.

Cloud services vendors can increase the trust and thus the usage of their offered services by proposing Insurance Level agreements (ILA) through the proposed system, with different pricing models relevant to "non-insured" services. Moreover, providers may sell their entire portfolio hardened and enforced with insured technology.

Consequently, several advantages emerge from this IT management service with certification:

- A new business model integrated with systems and technology that bundles insurance, monitoring, and remedy. It opens large-scale business opportunities for billable value added services for IT Insurance.
- Lack of transparency and trust between consumers and providers may be overcome by inserting financial remedies or other ramifications to the loss of data or lack of functionality due to security or availability issues.
- Economic models are main drivers to cloud usage, as well as the ability to provide scaled-up transient loads on the cloud. Degraded functionality or complete lack of service in these peak times has more financial impact than non-peak times. Risk mitigation is critical, and as in the case of any insurance issue, proven evidence and facts are needed by an auditing and measuring agency.
- Our assumption is that a cloud service provider would opt to purchase insurance and coverage for loss of data and protection for malfunction. The presented approach suggests that the provider can charge more for "trusted and secured liable services" dependent upon the ability of the provider to show, after an incident has occurred, the root cause and history stored at a third party vaults for a certain period of time.
- The system enables the service consumer to select different types of services, and add different insurance premiums, based on the type of risk associated with the data. Accordingly, data activity, or performance will be monitored to collect logs in case on a breach on security or segregated service level agreement (SLA).
- On demand, service consumers may require that the service provider will show evidence of using security and auditing tools, approved by the consumers, and embedded in the providers infrastructure.
- The audit, monitoring and system availability data can be extended to cover and enforce compliance and regulation, using the intercepted activity data as evidence. In this case, the evidence is shown as part of a certification process, validating that a potential lawsuits from a third party will not occur.
- The consumers can get quarterly reports of all the changes done to the infrastructure, as well as all the data relocation done within the infrastructure. Such reports, provided by the "Certified IT service in a box" for both sides, enable transparency and increase trust, while maintaining usage abstraction levels.

3 CONCEPTUAL ARCHITECTURE OF THE SYSTEM

Figure 1 depicts the conceptual architecture of the "Certified Services in a Box", based on integrations with IT management tools as well as several conceptual modules. Each component is numbered, and referenced accordingly in the text.

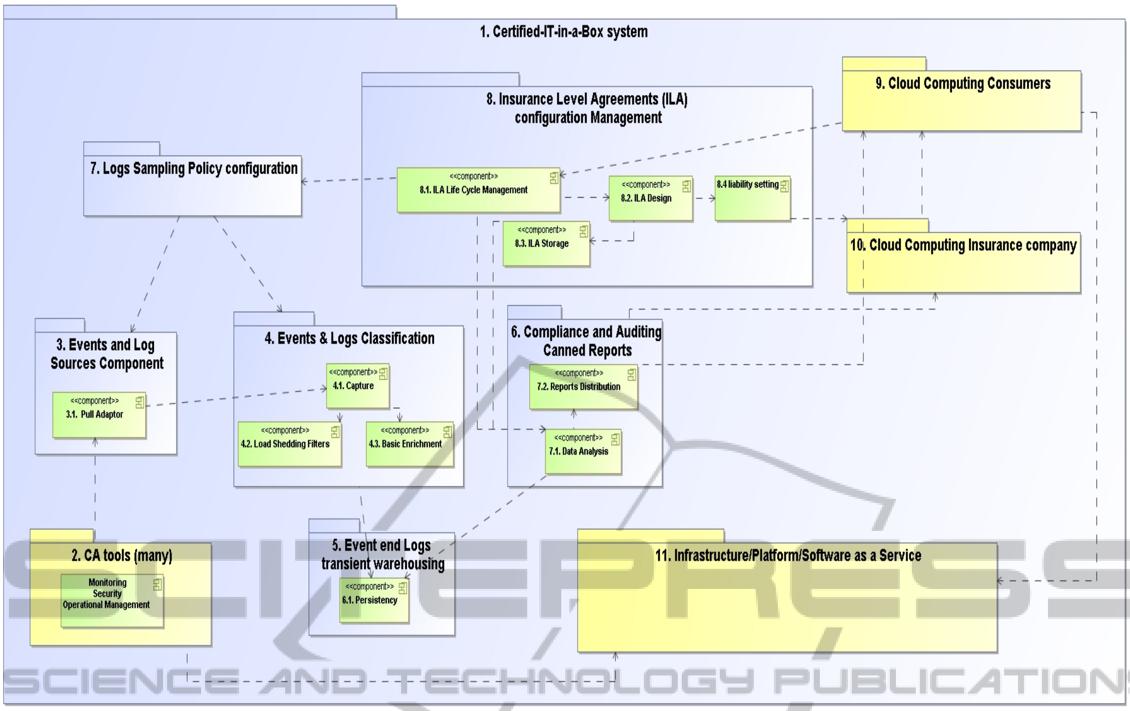
1. Certified-IT-in-a-Box system
7. Logs Sampling Policy configuration
8. Insurance Level Agreements (ILA) configuration Management
<<component>> 8.1. ILA Life Cycle Management
<<component>> 8.2. ILA Design
8.4 liability setting
<<component>> 8.3. ILA Storage
9. Cloud Computing Consumers
10. Cloud Computing Insurance company
3. Events and Log Sources Component
<<component>> 3.1. Pull Adaptor
4. Events & Logs Classification
<<component>> 4.1. Capture
<<component>> 4.2. Load Shedding Filters
<<component>> 4.3. Basic Enrichment
6. Compliance and Auditing Canned Reports
<<component>> 7.2. Reports Distribution
<<component>> 7.1. Data Analysis
2. CA tools (many)
Monitoring
Security
Operational Management
5. Event end Logs transient warehousing
<<component>> 6.1. Persistency
11. Infrastructure/Platform/Software as a Service

Figure 1: “Certified Services in a box” conceptual architecture.

3.1 Conceptual Architecture

Events and Log Sources (3). These are a set of components that can access any of the IT management, operation, and security teams in order to extract logs of activities in a common format, from the underlying vendor tools, such as CA Technologies’ IT Management and Security products: e.g. CA Application Performance Management, CA Service Operations Insight, CA SiteMinder® (CA Technologies’ tools) (2).

Events & Logs Classification (4). This set of systems normalizes the data originating from the collective set of *CA Technologies’ tools (2),* as well as deciding which elements to log and which to not, based on a configuration defined by the **service consumers (9)**.

Event end Logs Transient Warehousing (5). As part of the insurance provider requirements, the defined logs are stored for future analysis, based on needs of the **insurance provider (10)**, the consumers or the service providers. The data in the warehouse is archived and periodically sent to the relevant parties. In addition, the data collected may be purged or removed to off-line permanent storage in compliance with defined retention policies.

Predefined Compliance and Auditing Reports (6). Based on demand or other polices, the components analyze the data collected in the *warehouse component (5)*, and produce predefined reports to the relevant players such as the insurance provider, Cloud Provider or Cloud consumers.

Log Sampling Policy Configuration (7). This component defines which events and logs are going to be collected, based on the type of insurance defined for each user. The *Certified-IT-in-a-Box service (1)* is configured differently for each consumer since different insurance policies and types of assets to be protected may be applied. Thus, the service provider can define different pricing models to its consumers, based on the level of reporting and evidence needed.

Insurance Level Agreements (ILA) Configuration Management (8). This component defines the overall periodic scans that will provide evidence of normal operations according to contracts, or violation. Since each insurance policy defines different scanning needs, each need should be provided with a report that is executed on the gathered data. These settings enable definition of the insurance level agreements (ILA) between the service consumer and service provider. The system can offer a single ILA for all, multiple types of ILA and different pricing models, or customized ILA. These definitions trigger the relative reports and logs provided periodically to the players. This component interacts with the insurance provider as well, in order to define the liability contract (agreement) between the provided ILA to the consumers, and its coverage by the *insurance provider (10)*.

3.2 Prototypical Usage Pattern

A typical example for a scenario of the system and method is as follows:

When a consumer of an IT services (9), approaches a Provider (11) (either for IaaS/PaaS/SaaS), it is offered with modified service that includes insurance element. The insurance includes liability in case of data security issue, breach of a service level agreement or lack of operational services. This offering can be part of the basic service (without any negotiation and amendment), or the consumers can select different Insurance Level Agreements (ILA) from the provider (11). The ILAs are predefined and determined by the *service provider (11)* negotiating a liability service from the *insurance provider (10)*, and either offers readymade ILAs to its *consumers (9),* or builds a new definition (design) for an ILA, using the *ILA configuration management component (8)*. The defined ILA are monitored and managed by *CA Technologies' tools (2)* according to the type of services needed. For example, when the ILA provider sets security enforcement, *CA Technologies' tools (2)* will monitor Identity Access Management and provide Privileged Access Management to server administrators. If roaming limitations insurance is needed, *CA Technologies' tools (2)* will enforce network zone protection, and physical roaming policies, enabling supervised automatic provisioning by the provider datacenter. Setting an ILA does not preclude the service provider from protecting its private or public cloud, rather that evidence or remedy of these activities will not necessarily be provided

However, when such ILA do apply, *CA Technologies' tools (2)* will monitor and control, as well as provide dedicated logging options for further analysis by the *reporting tools (6)*. Nevertheless, ILA setting might be also partially configured, enabling *CA Technologies' tools (2)* to monitor just part of the data, thus reducing data monitoring capacity and aggregated reports.

Since the ILA is defined between the consumers and providers, periodic monitoring and report generation is conducted. These reports are delivered either as a service, on-demand, periodically, or even off-line. The recipients of these reports can be the service providers, the consumers, and the insurance provider, according to business arrangements.

4 CONCLUSIONS

In this position paper, we presented a novel approach for providing certified cloud services, by means of insurance provider, technology, and a new business model for cloud services. Auditing and reporting tools, when connected to IT management tools, enables a centralized "evidence vault" for future use. These reports and logs may be used for insurance claims, certification and/or compliance needs. We suggest that combining IT monitoring and security tools with a reporting layer, alongside risk mitigation and remedy from an insurance provider, will increase trust and transparency, while maintaining cloud computing abstraction concepts.

We argue in this position paper that certified services with financial backup will provide a more appealing approach for commerce relationship, and will generate a significant market opportunity for insurance providers, as well as for IT management technology.

REFERENCES

Blakley B., "2012 Planning Guide: Identity and Privacy", G00217746 Burton IT1 Research, 1 November 2011

Blum D., Schacter P., Maiwald E., Krikken R., Henry T., Boer M., Chuvakin A., "2012 Planning Guide: Security and Risk Management", G00224667, Burton IT1 Research, 1 November 2011

Brandic, I.; Dustdar, S.; Anstett, T.; Schumm, D.; Leymann, F.; Konrad, R.; "Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds", 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, USA, 5-10 July 2010

Glazer I., "Identity and Access Governance." Gartner. 21 Jul 2010.

Habib, S. M.; Ries, S.; Muhlhauser, M.; "Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation", Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), Xian, Shaanxi, 26-29 Oct. 2010

Heiser H, Nicolett M, "Assessing the Security Risks of Cloud Computing", Gartner Research Report G00157782, 3 June 2008

Ko, R. K. L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Qianhui Liang; Bu Sung Lee; "TrustCloud: A Framework for Accountability and

Trust in Cloud Computing”, , 2011 IEEE World Congress on Services (SERVICES), Singapore, Singapore, 4-9 July 2011

Pearson, S., “Taking account of privacy when designing cloud computing services”, ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09. Vancouver, BC, 23-23 May 2009Reeves D., "2012 Cloud Computing Planning Guide: From Hybrid IT to Hybrid Clouds." Gartner. 1 Nov 2011