jamk.fi

How to self-assess and audit application deployment in public cloud?

Pinja Koskinen
Vesa Simola

Masters thesis
XXXXX 2018
Cyber security
Master's degree programme in cyber security

<table>
<tr><td rowspan="3">Author(s)
Pinja Koskinen, Simola, Vesa</td><td rowspan="2">Type of publication
Masters thesis</td><td>Date
Month Year</td></tr>
<tr><td>Language of publication:
English</td></tr>
<tr><td>Number of pages</td><td>Permission for web publication: x</td></tr>
<tr><td colspan="3">Title of publication
Title
possible subtitle</td></tr>
<tr><td colspan="3">Degree programme</td></tr>
<tr><td colspan="3">Supervisor(s)
Last name, First name</td></tr>
<tr><td colspan="3">Assigned by</td></tr>
<tr><td colspan="3">Abstract</td></tr>
</table>

Contents

1 Introduction

1.1 Background of the study

1.2 Structure of the study

1.3 Objective of the study

1.4 Methods of the study

2 General overview of cloud

Cloud service is generally understood as a product that consists of services hosted in the Internet. This could include servers, networks, storage systems, software applications and other services. These products could be running from anywhere in the world, in a distributed manner. Cloud allows users to utilize applications without modifications or access to their locally available files and services can be reachable from any location within the Internet. Also, in some cases users may share files, data and information between several systems and other users via the cloud infrastructure. (Suikkanen, 2013 s8)

To name a few higher level motivators that might push companies towards cloud, let us consider the following (Tim Mather, Subra Kumaraswamy, Shahed Latif 2009):

- Initial investment is more manageable than buying complete set of infrastructure.
- Economies of scale provided to the cloud service provider help to keep costs and delivery times down.
- Open standards by open source software are acting as the foundation of the cloud solution.
- Sustainability via means of service provider having already done the major capital investments.

All of the above are beneficial elements of the different categories of different cloud categories. Cloud community uses the following models to categorize their services: Infrastructure as a Ser-

vice (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). (Ahlgren 2012, s7) Cloud hosting can be done in few different manners: Private cloud, public cloud, hybrid cloud and community cloud. (Suikkanen, 2013). Aforementioned deployment and hosting models are discussed next.

2.1 Cloud hosting types

2.1.1 Public cloud

Public cloud is hosted on the service provider facilities and all maintenance, modifications and upgrades are done by the service provider, meaning that the customer has no control over the hosted infrastructure. One exception to this is the fact that certain service providers give customer the options of choosing from several geographical locations from which to run their service. (Juha Ahlgren 2012, s12). The economy of scale can mean that the public clous can offer efficient storage, compute and connectivity at reasonable price. This can be especially true with the charging models where customers are required to pay only for the service they require and use. (Saara Suikka, 2013, s11)

2.1.2 Private cloud

Private cloud is understood as a service that is being operated by a service provider as a service to be used by single customer. Private cloud tends to use the same techniques as public cloud but they are configured to help the customer organization be more responsive and efficient in the IT resource usage than with traditional IT operation model. (Saara Suikkanen, 2013 s11) There are generally two types of private clouds, ones that are hosted on the customer premises and then there are those that are hosted on service provider infrastructure. It should be noted that while cloud infrastructure could be externally hosted, it is still considered a private cloud if the infrastructure is solely used by single customer organization. (Juha Ahlgren 2012, s10). Infrastructure on public cloud on the other hand is shared among the various customers of a service provider. (TAMOU, Aikaterini, 2014, s6).

2.1.3 Hybrid cloud

Combinations of the public and private cloud are called hybrid clouds. These clouds can tie the infrastructures of a private and public cloud together and allow the customer to extend their capacity beyond what is available in the private cloud by additionally utilizing the public cloud on time of need. This is called cloud bursting. Meaning that customer uses private cloud under normal circumstances but during peak load some or all parts of the service can be transported to public cloud.(Juha Ahlgren 2012, s13)

2.1.4 Community cloud

Fourth and final form of cloud is the community cloud. Community cloud is a multitenant cloud setup that is utilized by several organizations that may share a common interest or computing concerns. Such concern could come in a form of a compliance requirement, audit requirement or that the organizations require high speed access to common data, for example research organizations working on a common project. (Saara Suikkanen 2013, s12)

2.2 Cloud deployment models

2.2.1 Infrastructure as a service

Infrastructure as a service is the most basic service in the cloud landscape, it generally means an offering consisting of infrastructure, physical or virtual machines and other related resources like storage of images, networking and security features such as firewalls and load balancers and bundles of software. (Saara Suikkanen, 2013 s13) The benefit of the IaaS cloud for the customer is that certain data center related activities can be abstracted and used from for example a web interface or an API. There is no need to manage all levels of the infrastructure anymore and administative tasks can mostly focus on server side level like operating systems management and maintenance and third party software maintenance. (Kavis, Michael. ”Infrastructure as a Service”. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons.

2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018), Infrastructure as a Service). As in this type of a cloud service only the infrastructure is provided, all software related development and administration responsibilities are left to the customer (Kavis, Michael. ”Infrastructure as a Service”. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018), Infrastructure as a Service). So, it is worth to emphazise that while customer has limited or no control of underlying architecture that is used to provision the cloud based services, customer is still responsible for proper use and care of the cloud resources, for example the configuration of an application. (STAMOU, Aikaterini, 2014,s5)

2.2.2 Platform as a service

As stated above IaaS does not address the various scalability issues or automation challenges faced by organizations especially from the perspective of a software. All the parts of the software infrastructure must be provided by the customer. To ease this task PaaS providers can provide software platforms to certain level. Typical software platforms can be for example databases, logging and payments services, which can be used via various APIs (Kavis, Michael. ”Platform as a Service”. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)) Several PaaS related technologies also aim at automating the provisioning procedures for the virtual machines and containers that actually run the application. Examples of these services could be for example a Kubernetes platform, which would provide an API for containers for automatic scalability. Containers are relatively new concept in computing but they are used to package the application and its dependencies in to a manageable units for distribution and running in cloud platform. (What is a container? Docker documentation 2018). These containers can then be housed in orchestration tools such as the aforementioned Kubernetes or Docker swarm. As a conclusion, PaaS deployment could be considered being one level above the Software as a Service deployment as it eliminated the need for customer owned infrastructure for

the deployment of a software application. (Saara Suikkanen 2013, s14)

2.2.3 Software as a service

Software as a service is a method of delivering software application from cloud via Internet connectivity with the least amount of manual work from the customer. Using SaaS only requires configuration and user management from the customer, leaving everything else for the service provider. The advantages to the customer is the lack of need to maintain the platform and not needing any personnel to execute the maintenance tasks, which is beneficial especially when talking about services that do not belong to the core functionalities of the customer. (Kavis, Michael. "Software as a Service". Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)) Naturally, the SaaS services can not be used for software that require any heavier tayloring than just predefined configuration changes. A real-life example that illustrates the stacking of cloud services and the SaaS could be a email service that has its customer specific frontends running in containers on service provider orchestration tool that utilizes virtual machines housed in service provider facilities and hypervisors somewhere. SaaS services are nowadays very common (Kavis, Michael. "Software as a Service". Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)). Key point to understand the SaaS model is that customer has no control of the underlying software deployment or the computing infrastructure in SaaS model. (STAMOU, Aikaterini, 2014,s5). This is essential differentiator between SaaS and PaaS.

3 Security in cloud

3.1 Common cloud security aspects

As cloud is a relatively new approach to computing it is no wonder there is some uncertainty about how security at its various levels can be achieved. This uncertainty has led to decission makers to state that security is their primary concern with cloud computing. (Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009). Some general level challenges of cloud computing are identified as follows by Ben Halpert in his book Auditing Cloud Computing: A Security and Privacy Guide.

- Availability can be at risk as customers might consume more of the shared resources than expected. This is especially true in public cloud.
- Vast resources of the cloud could be used to launch denial of service attacks.
- Data recidency is a factor as different countries and regions have different requirements for information handling.
- Multitenancy is what allows the economics of scale, it is also a compliance consideration when same infrastructure is shared amongst customers.
- Log management of shared infrastructure might present an issue as information from multiple tenants could be visible in the same log files.
- Performance and service levels of the cloud are based on the services purchased, these metrics can be controlled by service level agreenments.
- Data evacuation process should be addressed as it sets the boundaries how information is removed from shared infrastructure.
- Supervisory access is of interest as service provider has the highest level of access to the infrastructure.

Some of the more detailed security concerns can be seen as shared among all the deployments while others are more tied to specific deployment model. Tim Mather, Subra Kumaraswamy and Shahed Latif describe the following barriers for cloud implementations that are shared amongst the

deployment models.

- Privacy is essential and it may not be obvious if the cloud model meets the current and upcoming requirements to safeguard privacy.
- Connectivity is mandatory to reach the service. High speed and reliability are critical for the user experience.
- Reliability requirements are high as enterprise applications are expected to be available 24/7.
- Interoperability with traditional non-cloud software is not given.
- Reliance on the service provider and vendor lock-in are threats that need to be addresssed on contract level.
- Economic value can be at risk due to hidden costs that are not obvious. It should be also noted that transitioning to cloud is not free.
- IT governance still has to be taken into account to make sure that the cloud deployment is in line with the business needs.
- Political and global boundaries can be factors when considering if it is all right to store for example customer data to outsourced data center.
- Changes in IT organization has to have the skills needed to operate the cloud environment and on the other hand IT organizations role might change due to a major cloud deployment.

Given the suggested flexibility of the cloud deployments and the vast number of threats shown above it is only natural that from an IT manager's perspective the very nature of the cloud architechture bypasses and fights against the well-known tools and frameworks of security. This is illustrated by the ease (and contradiction therein) in which services can be migrated, created and deployed in a cloud environment, but this does not remove the need for compliance and security. (Raghu Yeluri, Enrique Castro-Leon 2014). Next, we'll discuss some of the security concerns of different cloud deployment models.

3.1.1 Division of responsibility

Based on the security concerns identified above it is essential to understand the concept of division of responsibility. Term division of responsibility means that the responsibility of the service and the data therein is shared between the customer and the cloud service provider as defined by Jiafu Wan,Kai Lin,Delu Zeng, Jin Li, Yang Xiang, Xiaofeng Liao, Jiwu Huang and Zheli Liu in their conference papaer on SPNCE 2016. Same paper also clarifies this by stating that this division of work may lead to unexpected consequences and that it may be difficult to clearly define who can be held responsible of what as there are likely multiple factors at play on the same time. Combining the ”many hands working together” -problem with the long list of identified security concerns this is a factor worth considering.

3.2 Security aspects in public cloud

Based on what has been written above it is likely that it is taken as a given that in public cloud there are multiple tenants on the same physical infrastructure. Be that as it may, most public clouds offer software-based separation and permission control to maintain isolation between customers. Hardware level separation might be an option, but with likely additional costs involved. It is essential to understand how the platform-of-choice implements the multitenancy, for example if it supports the concept of having multiple directory services, such as Microsoft Active Directory or LDAP, one for each tenant.(Bond, 2018). Responsibility of patching and updating servers in public cloud generally falls to the service provider, but this can also cause unexpected risks to customer systems and applications. Hence, close interaction with the service provider is required to ensure that no new risks are introduced or availability issues surface due to service provider doing maintenance. (Halpert, 2011).

3.3 Security aspects in private cloud

Unlike with public cloud, multitenancy is slightly less of an issue in private cloud, in fact private cloud on its own could be seen as an approach to solve the multitenancy issue. (Bond, 2018)

3.4 Security aspects in hybrid cloud

As hybrid cloud is stated above being a mixture of both public and private cloud all the same rules apply. It should still be noted that while portions of the service may run in public cloud at times, the same security precautions and metrics should still be met as if the service was running solely in private cloud. (Voiks tallain sanoo ja viitata omaan aikaisempaan tekstiin?)

3.5 Security aspects in Infrastructure as a service

3.6 Security aspects in Platform as a service

3.7 Security aspects in Software as a service

3.8 Methods of improving security and availability in cloud

3.8.1 Service level agreenments

Service level agreenments aka SLAs are sets of condition and terms defined in contracts between customer and the service provider. SLAs can be used to define and agree upon the service levels between provider and customer, including sanctions if the terms are not met. Conditions and terms in SLAs can include various technical, commercial and business service level objectives (SLOs) combined with mechanics of how to measure that the agreed upon services levels are met. (Stamou,2014)

To succesfully utilize SLA as a way to improve service availability and security the SLA life-cycle could be split into four parts as follows: (Stamou,2014)

- Creation of the SLA including contract
- Implementing the SLA
- Enforcement and monitoring of the SLA
- Termination of the SLA

Generally speaking the first step consists of service provider predefining a set of various SLA levels for customer to choose from and to bind the contract upon. These could be considered as templates for the SLA. Customer then reviews these templates, selects one possibly modifying it and sends it back to the service provider for a review. Service provider then accepts, declines or sends modified version to the customer for a review. (Stamou,2014 s 13). Rest of the SLA life-cycle consists of implementation, regular reviews and eventually ending of the SLA as stated above.

What makes the SLA for cloud specially tricky is the fact that currently SLAs for cloud lack standardization. This is not optimal as standardization would lead into more structured content of SLAs. In a perfect world the SLA should take into account the individual risk requirements of the customer but this can lead into highly tailored SLAs. (Stamou,2014 s14).

3.8.2 Overcoming the reliance to connectivity

Once an application is running in the remote location it is obvious that connectivity is of paramount importance, in essence, having no connectivity in the campus means having no application and this can mean having no business. While many organizations have Internet connectivity these days it is still surprisingly uncommon for organizations to have backup connectivity if the unthinkable disruption happens. Fiber cuts are not all that uncommon (Teddy Hayford-Acquah and Ben Asante, 2017). To reduce the impact of a last mile failure it is a common practice to have two physically separate lines from a service provider, terminated to two separate customer premises routers in two separate equipment rooms. (Gunnar Bøe, Vidar Faltinsen, Einar Lillebrygfjeld, 2011) Two routers using VRRP protocol act in active-passive manner to provide so-called first-hop redundancy (rfc5798, 2010). This approach, when combined with physically separate lines, provides protection from fiber cuts on the last mile and this also protects from power supply failures in the customer premises router and also acts as a backup connection during router software upgrades and some configuration changes. However, this method does not protect against catastrophic failures in the service provider network. To accomplish this, it is required to have similarly separated lines and routers from two separate service providers. Assuming that the customer has some IP block(s) to announce over BGP and that the service providers are accepting the customer IP block(s) for transit it is possible to create fully

redundant last mile connectivity. All these relatively complex and expensive requirements are likely the reason why organizations won't purchase redundant connectivity but instead accept the risk of significant business impact and downtime. (Packetworks, 2016).

Similarly, if cloud application is running in a "stretched" network infrastructure, e.g. data center interconnect, it is essential that the interconnect is built in a redundant fashion. While redundancy is all good it can also cause failures of different kind, but with equally potential for catastrophe (Pepelnjak, 2011). This problem with location redundancy could be solved by making the application layer not so reliant on the underlying IP layer, this could be done for example by decoupling the service IP - address that end users connect to - and advertising it to data center routers via BGP over only locally significant subnet. Even while there are tools for this sort of decoupling (RIPE 2010), this kind of approaches have apparently been deemed as non-trivial and time consuming tasks so currently it would appear that the accepted solution is to introduce more complexity outside the application to hide the underlying already existing complexity of IP transport. One such method is overlay networking, such as VXLAN, that builds up a streched OSI layer 2 domain over routed network (rfc7348). While there are quite a few methods of implementing encryption in network it should be questioned if it is a sustainable choice to outsource application security to network layer. Implementing encryption using IPSEC (rfc4301) commonly indicates that OSI layer 3 routing should be implemented between data centers, while doing routing is a healthy choice for data center interconnect in terms of limiting failure domains. It also means that an overlay networking is likely required if OSI layer 2 transparency is insisted upon. To implement both OSI layer 2 transparency and encryption one could choose to do encryption on OSI layer 2 via MACSEC (Juniper, 2018), VXLAN over IPSEC or by utilising encryption in DWDM (Arista, 2018) level. It should be noted that both MACSEC and IPSEC have impact in the capacity of performance in terms of payload transferred versus the capacity utilized. Running VXLAN over IPSEC may have an impact in the net payload as well, or atleast MTU should be carefully considered. Many public cloud providers such as Amazon (Amazon 2018), Google (Google 2018) and Microsoft (Microsoft 2018) support IPSEC tunnels to tenant specific virtual routing and forwarding instances that are logically separated from one another. Still, it is worth mentioning that even if the data center interconnect from customer data center to cloud provider is encrypted this does not mean that the internal data center traffic inside

the service provider facility is encrypted in any fashion. This is one reason why it might be a good idea not to rely on network level to implement the encryption, instead utilize sufficient encryption in the application level, just to be sure.

4 Self-assessment of cloud security posture

Self-assessment means observation and evaluation of oneself or activities, viewpoints and performance of one's capability, performance or ability at a given task in relation to on objective standard. The important bit here is that self-assessment is done by oneself, not by an external party (Oxford dictionaries, 2018). This is a key differentiatior to audit and compliance, as described next.

Prior to going deeper into self-assessment of cloud security posture we need to define what is meant by compliance and audit, and how they differ from self-assessment. The classical definition of compliance is to meet a requirement, yet in the context of security compliance is a security blueprint for certain type of data. Organization that owns the data defines the minimum level of security. Audit on the other hand is the process that measures how the organization is aligned with the given compliancy requirement at a given point in time. (Prashant Priyam, 2018) Another definition of the term auditing refers to the accounting of user activity on data. This can mean read and write operations, who did them and when. Cloud offers multitude of options to provide security, yet it largely depends on the requirements and talent available to implement those security features in practice. It is key to understand that the implementation of security in cloud is slightly different from what it is with on-premise or traditional deployments. (Prashant Priyam, 2018) Oxford dictionary definition of audit states that the audit is an official inspection of entitys accounts by an independent auditor. (Oxford dictionaries, 2018). Another definition of audit is given by Ben Halpert in his book Auditing Cloud Computing: A Security and Privacy Guide as follows: Audit is an method of assuring that certain standard or practice is implemented and this is done by the auditor systematically examining the evidence for the compliance against given criteria. (Halpert 2011). We believe that the aforementioned statements highligh the difference of audit and self-assessment.

5 Conclusions