The Challenge of Private Cloud for the Digital Business

Eugen Petac
Faculty of Mathematics and Computer Science
"Ovidius" University of Constanța, Romania
epetac@univ-ovidius.ro
Andreea-Oana Petac
Faculty of Mathematics and Computer Science
"Ovidius" University of Constanța, Romania
andreea.petac@gmail.com

Abstract

For various organizations, a Private Cloud represents a stepping stone to a fully public model, while others consider it to be the ideal solution. Organizations such as the governmental institutions that have stringent data security needs might choose the Private Cloud model. Its qualities such as availability, security, compliance may convince other organizations to look at a private cloud model as well. In this paper we propose an integrated solution within the private cloud area, based on open source software. In section 2 we provide brief characterizations of the existing types of Clouds, focusing then on Private Cloud. In section 3 we address the security issues in Private Cloud. In section 4 we present and analyze different open source software solutions within Private Cloud. Section 5 encompasses some conclusions regarding the benefits and downsides of this technology, along with some detail information on how to set up an organization that runs in a Private Cloud.

Key words: Digital Business, Private Cloud, Information Security, Cloud computing
J.E.L. classification: L8, M1, M3

1. Introduction

We are in the Digital Age (Rosenquist, 2015, p.66), a historical period that is characterized by the existence of digital technology. The business activities are based on transmission, processing and storage of information. Lopez (2015, p.1) defines digital business "as the creation of new business designs by blurring the digital and physical worlds". Those new models are based on complete integration of business concepts and technological concepts. Any company within the digital business will be a technology company.

Social media, mobile, (data) analytics and cloud (SMAC) (Accenture, 2015, p.4) are the four technological categories underlying the digital transformation. They are pushing the business field towards innovation, the consumer having the opportunity to be better informed and better connected. The SMAC categories support new business model to deliver solutions and services in a contextual manner to customers anytime and anywhere within an optimized price structure. Using a cloud platform should be the first choice of the user, or at least for him to be acknowledged that is made available. The access to a product or service must be designed primarily for mobile or, at least, it should be optional. Companies need intelligent solutions for data analysis in order to be able to deliver predictions and be based on social data including information from social media.

Cloud computing is a modern concept in the computing field, representing an ensemble of distributed computing services, applications, access to information and data storage, the user not needing to know the location and physical configuration of the systems which provide these services.

There are many definitions of what cloud computing is. One that is worth mentioning is stated

by the National Institute of Standards and Technology (NIST): " Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Grance, Mell, 2011, pp.2-3).

The idea behind the term "Cloud" can be derived even from the nature and purpose of this technology: the system works for users even if they have no clue about its complexity. Users do not realize that while they are using this technology, huge amounts of data are processed globally in real time, so that applications work for them, the proportions of this action being simply stunning. The only thing that users should be concerned about is linked to the terminal through that they connect to the cloud and whether or not this is connected to the internet so that they can have access to the tools that the cloud offers.

What many users may not know is that much of the structure of today's information technology industry is already in the cloud computing or migrates to it. A slow migration is performed for several years, mainly due to the infrastructure support costs and to the economy of large proportions of data centers that provide necessary performance and processing power. This delay can be attributed to the ongoing development of the internet technology towards the vast amounts of data that needs to be extracted, analyzed and organized for users to easily manage data for processing.

In the Digital Age there are stated a number of trends (Accenture, 2015, p.9): Internet of Me (DuBravac, 2015, p.1), Outcome Economy, Platform (R)evolution, The Intelligent Enterprise, Workforce Reimagined. *People First: The Primacy of People* (Accenture, 2016, p.3) it is stating to be the new strategy. This will enable organizations to create new business models that support Digital Age, based on the following trends: Intelligent Automation, Liquid Workforce, Platform Economy, Predictable Disruption, Digital Trust. Cloud Computing technology is an integral part of these trends and will become increasingly prominent in the latter half of this decade.

2. Important Aspects on Private Cloud

Cloud services fall into three broad categories: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) (Grance and Mell, 2011, pp.2-3). The SaaS is designed to provide software to the user, usually via a web portal. While the user is free to use the service from anywhere, the companies pay some fees. Through the PaaS, the provider offers the solutions package along with specific characteristics. The services offered by PaaS include all phases of the System Development Life Cycle (SDLC) and can use Application Program Interfaces (APIs), web portals or gateway software. IaaS is a way of delivering the cloud infrastructure (servers, storage, networks) and their associated resources via dashboard and/or API. It has already purchased the software needed. This model is alike to running a virtual server on a device, only now is single server running virtual disk, being similar to the concept of "pay only what you use."

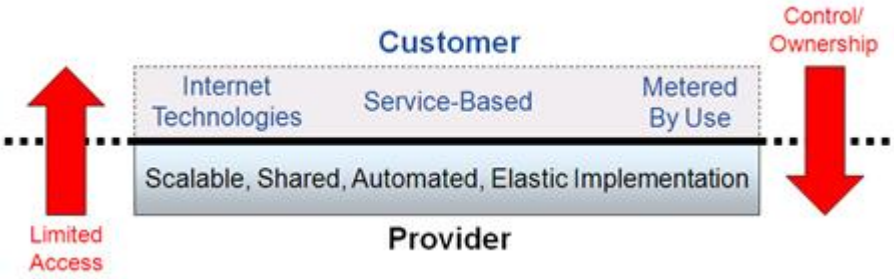
Taking into consideration the implementation methods, there are three basic Cloud Computing models: Public Cloud, Private Cloud and Hybrid Cloud. To this it can also be added Community Cloud which can be characterized by a multi-administrative domain involving different deployment models – public, private and hybrid (Velte, 2010, pp.91-172). Personal Cloud (Forrester, 2012, pp.3-5) can be defined as a place where one can store, stream, synchronize and share various content which is actively moving from one platform, screen and location to another. Through this, a new trend has been started – the Internet of Me – in which the end user is placed at the center of every digital experience.

While Public Cloud relies on third parties to provide IT services over the Internet, through Private Cloud the information and processes are managed internally. Hybrid Cloud is a mixture of the other two types of Cloud, having the possibility to extend its capabilities to be used in public Cloud. Private Cloud is similar to the public one, but their resource-providing model is limited within the boundaries of an organization. It can also be represented by several different departments within the same company. Virtualization is used on existing servers in the company in order to improve the use of workstations. A Private Cloud also involves sourcing and measurement of its components, enabling rapid deployment and change of components where appropriate. The

private model usually uses virtualization technologies in order to increase the hardware utilization and to abstract computation, memory, network, and storage component from its consumers (Shinder, 2012). Private Cloud integrates Personal Cloud when the services and infrastructure are maintained on a private network.

An organization is able to choose between two types of private cloud: the On-Premise Private Cloud (OPPC), which is hosted within an organization's own data center and the Externally-Hosted Private Cloud (EHPC), which is hosted by an external cloud computing provider. A comparison between the OPPC and the EHPC is shown in the following figure.

Figure no. 1. OPPC vs EHPC



Source: (Bittman, 2010)

Upfront capital cost, time, resources, the needs and size of an organization are only a few of the reasons that need to be taken into consideration when one chooses a solution for Private Cloud Computing. To these are added the security requirements, the backup and disaster-recovery procedures, movement of the legacy applications to the cloud, the influence over the IT&C team and the management of the organization.

Private Cloud represents the solution that is recommended when the following situations happen: the ability to use shared resources is limited due to the security and regulatory requirements, the computing budget is not limited or the computing demand is stable over time, the business growth being predictable. It can also happen a limitation to the feasibility of shared resources demanded by the industry or the government or an acceptance of higher costs in order to be ensured that the dedicated resources are strongly desired.

The new trends included in the strategy People First: The Primacy of People together with Internet of things (IoT) (Vermesan and Friess, 2011, pp.7-206), Internet of Everything (IoE) (Bradley, Barbier and Handler, 2013, pp.1-17), Internet of Me (Accenture, 2015, p.9) and Big Data (Zikopoulos, et al., 2012, pp.3-52) make Private Cloud a topic of major interest.

3. Security Issues in Private Cloud

Although it resembles the public Cloud, the private Cloud has the big advantage of having the core business operations in-house by relying on the existing IT infrastructure and reducing the responsibility of maintaining it once the cloud has been set up. By using this method, the security concerns become less critical, sensitive information not going out of the private infrastructure.

However, there are some issues towards this Cloud model, the first one being represented by its security architecture. Its security perimeter is not always configured in order to protect the information and resources from attacks within the organization (Shinder, 2012). Another way for the resources to be better protected is by placing them in separate security zones, differentiating them by type and sensitivity level (Stawowski, 2009, p.35). Although one may think that because it is on the internal network it is secure, attacks are still possible (Pfleeger, Irvine, Kwon, 2012, pp.19-23). Security standards are a necessity and are not to be lowered (Bloomberg, 2012).

When the private model is implemented, the idea of having control on specific devices is not going to be possible because the virtual machines are not related to specific hardware devices. Also, the implemented security policies must not be linked to trusted zones based on any physical hardware. A compromised hypervisor can allow an attack to each virtual machine on a virtual host. This results in an increase in the resources usage of a virtual machines that causes a denial of

service across the host or even across a collection of servers. The solutions based on Intrusion Detection and Intrusion Prevention Systems (IDS/IPS) (Pathan, 2014, pp.3-258) are the ones that are recommended in these scenarios.

A key concept is that security "is an enabler, not a disabler" (O'Hanley and Tiller, 2010, p.146). In the same time, nothing about information security is ever black or white. The security policies for Private Cloud must be adapted to its essential characteristics: on-demand self-service, a broad network access, resource pooling, rapid elasticity and measured service. A first step consists of determining the roles and responsibilities based on a RACI Matrix (Responsible, Accountable, Consulted, and Informed) (Smith and Erwin, 2015, pp.2-14). All the actors involved must understand them very well and document the scenario.

Attack surface analysis is used in order to deduce the cyber security control methods through which the vulnerabilities of physical entities (Humans, Datacenters, Servers and Storage, Networks, Operating Systems, Hypervisor/hosting operating systems, Cloud management consoles, tools & APIs.) or virtual entities (virtual network devices, Virtual (Guest) Operating Systems, Hypervisors, Management Consoles and APIs) can be eliminated or mitigated.

The formal process for making different changes to the Private Cloud services is called change management. For the NIST change management model (Johnson, et al., 2011, pp.16-46) to be used, various steps are required: request the change, record the request, determine if change control is required, analyze for security impact, test for security impact, approve the change, implement the change, verify the implementation, close the request. For a successful deployment to happen, an effective logging, monitoring, measuring and event management strategy are required. The incident management and recovery provide assistance within the cycle of the incident. The NIST security incident framework (Cichonski, et al., 2012, pp.21-51) reports four distinct stages for managing security incidents: preparing for the incident, detecting and analyzing the incident, containing, eradicating and recovering from the incident and performing post-incident activities.

Implemented private Clouds can be a successful action within various business activities, such as healthcare or financial sector. However, one must take notice that the security procedures have been properly implemented.

4. An Approach on Building a Private Cloud Solution

The GNU General Public License (GPL) projects have made great progress in recent years. They are thought to be a viable alternative for the construction of Private Cloud. OpenStack, CloudStack, Eucalyptus and OpenNebula are the most important open source cloud computing software (Barkat, Diniz dos Santos and Ikken, 2015, pp.187-204).

Initially presented as an Infrastructure as a Service (IaaS) solution, through a number of improvements the OpenStack models type approached to those of Platform as a Service (PaaS) and Software as a Service (SaaS) models. OpenStack provides a broad set of possible configurations and integration within the existing systems. It can also control a large number of computational and storage resources and network. OpenStack infrastructure virtualizes the hardware structure and it optimizes both the physical and human resources within an organization.

CloudStack enables the creating, managing, and deploying infrastructure of cloud services. It can support multiple types of virtualization, including the LXC (Linux Containers), being able to run multiple instances of hypervisor type. CloudStack requires: a management server, placed outside the virtual infrastructure and provides the control's cloud, virtual hosts that will run in virtualized environment, primary storage where they will be physically stored files and a secondary storage where one can make the savings.

Eucalyptus provides a way of managing a large number of physical machines that run virtualized instances. It consists of the following modules: the cloud controller, storage controller, storage controller elastic cluster controller, controller node. Eucalyptus Private Cloud solution is fully compatible with the offered Amazon Cloud model. This allows the movement between Amazon Cloud platform created our private and even use as a hybrid Cloud, without any modifications.

OpenNebula is a software that uses existing network interconnected for creating virtual environments and has the advantage that it resizes easily to the demands of new services. It

integrates into any existing environment. OpenNebula allows private infrastructure expansion with remotely infrastructure and is able to create isolated virtual data centers. In these datacenters virtual user groups can create and control virtual machine instances.

OwnCloud is a software package for file storage, being an IaaS private personal cloud service. From a functionality point of view it can be compared to Dropbox or Google Drive. However, the main difference is that OwnCloud is free and open-source. It allows access to storage from mobile devices, desktops, or Web browsers.

Xen and KVM solutions (Jaikar, Kim and Noh, 2013, pp.118-131) are open source virtualization software used above. They add a number of commercial options including VMware or Microsoft Hyper-V.

Containers-as-a-Service(CaaS) is essentially a Private Cloud solution (Pahl, 2015, pp.24-31). Docker, Kubernetes, Rkt are a few of software solutions. CaaS offers full security control, direct data access, direct integration ability, full ownership date, integrated single sign-on and complete cost transparency. AppScale, OpenShift, Cloud Foundry are some of PaaS open-source software solutions.

The best SaaS applications from a Private Cloud must be integrated within social, mobile and analytical parts. The SaaS solutions open source available target areas of interest such as (Krishna, Nandimandalam and Choi, 2016, pp.53-62): Network Monitoring, Cloud Backup and Storage, Big Data, Business Process Management, Content Management, Customer Relationship Management (CRM), Document Management Systems, E-Commerce, E-mail/ Collaboration/ Groupware, E-mail Marketing, Enterprise Resource Planning (ERP), Human Resource Management (HRM), Invoicing, School Management/Learning Management Systems, Time Tracking, etc.

Private Cloud solutions based on open source software have been gaining more and more ground. The intellectual property policies must be evaluated and updated in order to meet the obligations that are associated with the Private Cloud environment. With the help of specifically designed tools, the organizations can detect the open-source code, providing then a list of the license obligations that accompany each component. In order to define the acceptable intellectual property license policies for the organization, audit the current software portfolio and incoming code, and ensure compliance through all of the software development and procurement stages, an Open Source Software Adoption Process (OSSAP) can be used (Protecode, 2016, pp.1-5).

5. Conclusions

For a number of institutions, a Private Cloud will be a stepping stone to the public model, and for others this will represent the ideal solution. Organizations with higher data security needs or organizations with the right scale might pursue a private cloud model. Availability, security, compliance etc. may be the qualities that will drive other companies to look at a private cloud model as well. However, cloud computing represents an exciting evolutionary step in computing and organizations will be able to choose between private, public or hybrid cloud offerings based on their unique needs and concerns.

The implementation of a Private Cloud aims to avoid many of the objections regarding cloud computing security. Because its setup is implemented safely within the corporate firewall, a Private Cloud provides more control over the company's data, ensuring security, though with greater potential risk for data loss due to natural disaster. The organization that is implementing the private cloud is responsible for running and managing the IT resources instead of passing that responsibility on to a third-party cloud provider.

In order to have a Private Cloud implemented, an organization needs to follow various steps. Doing research of the needs and benefits of this type of Cloud is the first step. After analyzing that the proper processes and policies are in place to successfully build a secure Private Cloud, it is highly important the way that it is developed and tested within a non mission-critical environment. The IT staff must be trained appropriately on how to manage the Private Cloud and employees and partners on how to access and use the Cloud. Based on all of these aspects of Private Cloud, we propose an integrated solution that is based on open source software.

Within the Private Cloud deployment model, once roles and responsibilities are determined they must be rigorously documented, and all of the actors involved must have a thorough understanding

of them. It is required an understanding of the risks that are related to: Application Design, Architecture, Business Continuity, Data Location, Funding, Legal and Regulatory, Privacy and Reputation, Human Capital, Security and Standards.

6. References

1. Accenture, 2015. Digital Business Era: Stretch Your Boundaries. [online] Available at: <http://techtrends. ccenture.com/s-en/downloads/Accenture_Technology_Vision_2015.pdf> [Accessed 20 April 2016].
2. Accenture, 2016. People First: The Primacy of People in a Digital Age. [online] Available at: <https://www.accenture.com/us-en/insight-technology-trends-2016.aspx > [Accessed 20 April 2016].
3. Barkat, A., Diniz dos Santos, A.-R. and Ikken, S., 2015. Open Source Solutions for Building IaaS Clouds. Scalable Computing: Practice and Experience, [online] Available at: < http://www.scpe.org/index.php/scpe/ rticle/iew/1089 > [Accessed 25 April 2016].
4. Bittman, T., 2010. Clarifying Private Cloud Computing. [online] Available at: <http://blogs.gartner.com/ thomas_bittman/2010/05/18/clarifying-private-cloud-computing/> [Accessed 25 April 2016].
5. Bloomberg, J., 2012. Why Public Clouds are More Secure than Private Clouds. [online] Available at: <http:// apthink.om/012/02/07/why-public-clouds-are-more-secure-than-private-clouds/> Accessed 25 April 2016].
6. Bradley, J., Barbier, J. and Handler, D., 2013. Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion. [online] Available at: < https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_ Economy.pdf [Accessed 25 April 2016].
7. Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer Security Incident Handling Guide. [online] Available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [Accessed 25 April 2016].
8. DuBravac, S., 2015. The “Internet of Me”. [online] Available at: <http://www.cta.tech/i3/Grow/2015/March April/The-Internet-of-Me%E2%80%9D.aspx> [Accessed 25 April 2016].
9. Forrester, 2012. Personal Cloud Services Emerge To Orchestrate Our Mobile Computing Lives. [online] Available at: <https://www.sugarsync.com/media/sugarsync-forrester-report.pdf> [Accessed 25 April 2016].
10. Grance, T., Mell, P., 2011. The NIST Definition of Cloud Computing. [online] Available at:
11. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [Accessed 25 April 2016].
12. Jaikar, A., Kim, G.-R. and Noh, S.-Y., 2013. Performance Trade-off between Xen and KVM. Journal of Next Generation Information Technology (JNIT), 4(8), pp.118–131.
13. Johnson, A., Dempsey, K., Ross, R., Gupta, S. and Bailey, D., 2011. Guide for Security-Focused Configuration Management of Information Systems. [online] Available at: <http://nvlpubs.nist.gov /nistpubs/Legacy/SP/nistspecialpublication800-128.pdf> [Accessed 25 April 2016].
14. Krishna, M., Nandimandalam, V. and Choi, E., Comparison of Open-Source PaaS Architectural Components. In: D. C. Wyld and J. Zizka ed. 2016. CCSEA, CLOUD, DKMP, SEA, SIPRO - 2016. Chennai: AIRCC. pp.53-62.
15. Lopez, J., 2015. Digital Business Key Initiative Overview. [online] Available at: <https://www.gartner.com/ doc/3098425/digital-business-key-initiative-overview > [Accessed 20 April 2016].
16. O’Hanley, R. and Tiller, J. S., 2010. Information Security Management Handbook. 6nd ed. New York: CRC Press.
17. Pahl, C., 2015. Containerisation and the PaaS Cloud. IEEE Cloud Computinf, 2(3), pp.24–31.
18. Pathan, K. A., 2014. The State of the Art in Intrusion Prevention and Detection. New York: CRC Press.
19. Pfleeger, L. S., Irvine, C. and Kwon, M., 2012. Guest Editors' Introduction. IEEE Security and Privacy Systems Journal, 10(2), pp.19–23.
20. Protecode, 2016. Open Source Software Adoption Process (OSSAP). [online] Available at: < http://www. protecode.com/open-source-software-adoption-process-ossap/> [Accessed 25 April 2016].
21. Rosenquist, M., 2015. Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc.
22. Shinder, T., 2012. Security issues in the Private Cloud. [online] Available at: <http://social.technet. microsoft.com/wiki/contents/articles/security-issues-in-the-private-cloud.aspx> [Accessed 25 April 2016].
23. Smith, L., M. and Erwin, J., 2015. Role & Responsibility Charting (RACI). [online] Available at: <https://pmicie.starchapter.com/images/downloads/raci_r_web3_1 .pdf> [Accessed 25 April 2016].

24. Stawowski, M., 2009. Network Security Architecture. [online] Available at: <http://www.clico.pl/services/ Network_Securite_Architecture.pdf> [Accessed 25 April 2016].
25. Velte, A., 2010. Cloud Computing - A Practical Approach. New York: McGrow-Hill.
26. Vermesan, O. and Friess, P., 2011. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. Aalborg: River Publisher.
27. Zikopoulos, P., Eaton, C., deRoos, D., Deutsch, T. and Lapis, G., 2012. Understanding Big Data Analytics for Enterprise Class Hadoop and Streaming Data. New York: McGrow-Hill.