Sławomir PRZYŁUCKI, Daniel SAWICKI

Lublin University of Technology, Department of Electronics

Resource security in the cloud computing

Abstract. *This paper presents analysis of security issues inside enterprise private clouds. The investigated security tools were: security groups, elastic IPs, virtual machines isolation. All these mechanisms and tests presented in the article base on Eucalyptus cloud structure and give a detailed view on process of securing the resources inside private IaaS cloud structure.*

Streszczenie. *Praca przestawia analizę zagadnień bezpieczeństwa w prywatnych sieciach chmurowych stosowanych w przedsiębiorstwie. Badane były następujące zagadnienia bezpieczeństwa: grupy bezpieczeństwa, elastyczna adresacja IP, izolacja maszyn wirtualnych. Wszystkie mechanizmy i testy prezentowane w artykule są oparte o strukturę chmury wykorzystującą pakiet Eucalyptus, przedstawiającą szczegółowo proces zabezpieczania zasobów w strukturze prywatnej chmury opartej o model IaaS.* **(*Bezpieczeństwo zasobów w środowisku chmurowym*).**

Keywords: Cloud computing, resource security, Eucalyptus.
Słowa kluczowe: Środowiska chmurowe, bezpieczeństwo zasobów, Eucalyptus.

Introduction

Cloud computing has become nowadays a buzzword among IT and industry engineers. The cloud phenomenon is quickly growing towards becoming the de facto standard of computing, storage and hosting, both in industry and Internet. Cloud computing is the access to computers and their functionality via the Internet or a local area network. Users of a cloud request this access from a set of web services that manage a pool of computing resources (i.e., machines, network, storage, operating systems, application development environments, application programs). When granted, a fraction of the resources in the pool is dedicated to the requesting user until releases them. The user cannot actually see or specify the physical location and organization of the equipment hosting the resources they are ultimately allowed to use. That is, the resources are drawn from a “cloud” of resources when they are granted to a user and returned to the ”cloud” when they are released.

Cloud computing model

Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. From an architectural perspective there is much confusion surrounding how cloud is both similar to and different from existing models of computing and how these similarities and differences impact the operational, and technological approaches to network and information security practices. NIST (U.S. National Institute of Standards and Technology) defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models [1]. They are summarized in visual form in figure 1.

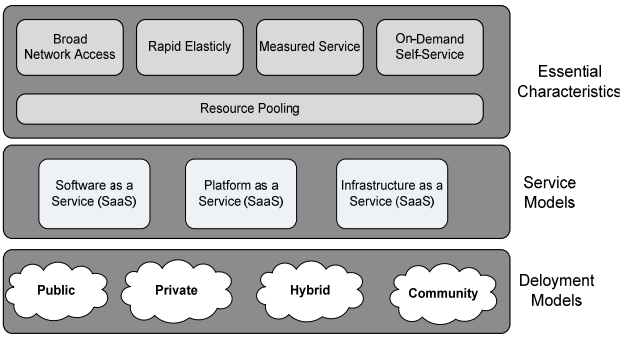

Fig.1. NIST Visual Model of Cloud Computing Definition

Cloud computing characteristics

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches [2]:

- *On-demand self-service*. A consumer can provision computing resources such as server time and network storage as needed automatically, without requiring human interaction with a service provider.
- *Broad network access*. Resources are available over the network and accessed through standard network mechanisms.
- *Resource pooling*. The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- *Rapid elasticity*. Resources can be rapidly and elastically provisioned.
- *Measured service*. Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts).

Cloud computing service styles

Cloud computing is typically divided into three levels of service styles, often referred to as the “SPI Model,” where ‘SPI’ refers to Software, Platform or Infrastructure (as a Service), respectively. These levels support virtualization and management of differing levels of the solution stack. The meaning of cloud service levels are [2],[3]:

- *IaaS style clouds* provide access to collections of virtualized computer hardware resources, including machines, network, and storage. With IaaS, users assemble their own virtual cluster on which they are responsible for installing, maintaining, and executing their own software stack.
- *PaaS style clouds* provide access to a programming or runtime environment with scalable compute and data structures embedded in it. With PaaS, users develop and execute their own applications within an environment offered by the service provider.
- *SaaS style clouds* deliver access to collections of software application programs. SaaS providers offer users access to specific application programs controlled and executed on the provider's infrastructure. SaaS is often referred to as „Software on Demand”.

Cloud deployment models

When categorizing cloud service offerings we often refer to clouds in terms of "service style" depending on the

portion of the software stack delivered as a service. The most common service styles referred to the acronyms IaaS, PaaS, and SaaS. Cloud "types" (including public, private, and hybrid) refer to the nature of access and control with respect to use and provisioning of virtual and physical resources [4].

There are three cloud deployment models [3]:

- *Public clouds* provide access to computing resources for the general public over the Internet. The public cloud provider allows customers to self-provision resources typically via a web service interface. Customer's rent access to resources as needed on a pay-as-you-go basis. Public clouds offer access to large pools of scalable resources on a temporary basis without the need for capital investment in data center infrastructure.
- *Private clouds* give users immediate access to computing resources hosted within an organization's infrastructure. Users self-provision and scale collections of resources drawn from the private cloud, typically via web service interface, just as with a public cloud. However, because it is deployed within the organization's existing data center, and in most cases behind the organization's firewall, a private cloud is subject to the organization's security regulations and thus offers a higher degree of security over sensitive code and data.
- *Community Cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on-premises or off-premises.
- A hybrid cloud combines computing resources (e.g., machines, network, storage, etc.) drawn from one or more public clouds and one or more private clouds at the behest of its users.

Reference model of cloud computing security

The cloud security reference model addresses the relationships of presented above cloud computing model and places them in context with their relevant security controls and concerns. The deployment of cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources and information. It also should take into consideration the types of assets, resources and information being managed, who manages them and how and which controls are selected and how they are integrated [5].

The following figure (fig.2) summarizes above points. The article covers the private cloud security items. We concentrate on the security aspects of the IaaS delivering hardware (server, storage and network), and associated software (usually virtualization technology, distributed file system).

	Infrastructure Managed By	Infrastructure Owned By	Infrastructure Located	Accessible and Consumed By
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization or Third Party Provider	Organization or Third Party Provider	On-Premise or Off-Premise	Trusted
Hybrid	Organization and Third Party Provider	Organization and Third Party Provider	On-Premise and Off-Premise	Trusted and Untrusted

Fig.2. Cloud computing security references model

Eucalyptus cloud implementation

Eucalyptus is an open source Linux-based software architecture that implements scalable, efficiency-enhancing private and hybrid clouds within an enterprise infrastructure. Eucalyptus provides Infrastructure as a Service (IaaS). This means that users can provision their own collections of resources (hardware, storage, and network) via Eucalyptus' self-service interface on an as-needed basis. A Eucalyptus cloud is deployed across an enterprise's "on-premise" data center and is accessed by users over enterprise intranet. Thus, with a Eucalyptus private cloud, sensitive data remains secure from external intrusion behind the enterprise firewall [6]. From the functionality point of view, Eucalyptus covers all IaaS requirements (fig.3).

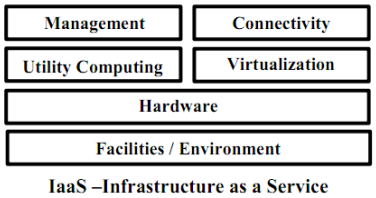

Fig.3. Elements of Eucalyptus IaaS implementation

The architecture of the Eucalyptus system is simple, flexible and modular with a hierarchical design reflecting common resource environments found in many academic settings. The system allows users to start, control, access and terminate entire virtual machines using an emulation of Amazon EC2's SOAP. That is, users of Eucalyptus interact with the system using the exact same tools and interfaces that they use to interact with Amazon EC2. Currently, Eucalyptus support VMs that run atop the Xen and KVM/QEMU hypervisor [7]. There are four components in Eucalyptus installation: Node Controller (NC), Cluster Controller (CC), Storage Controller (Walrus) and Cloud Controller (CLC). The relations among Eucalyptus elements are visualized on figure 4.

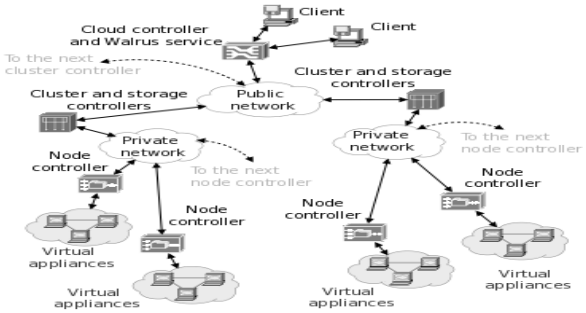

Fig.4. Typical structure of Eucalyptus private cloud

From security point of view, the most important features of Eucalyptus system is multi-tenancy. Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. That is graphically presented on fig. 5.

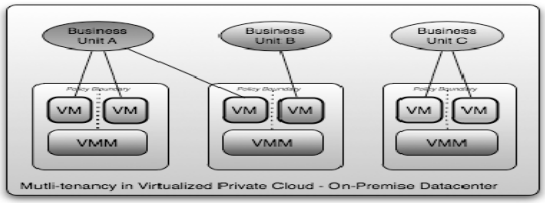

Fig.5. Private clouds with 3 different business units, each with different security policy

Cloud deployment models place different importance on multi-tenancy. However, even in the case of a private cloud, a single enterprise may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. Thus

multi-tenancy concerns should always be considered. Regarding Eucalyptus system, multi-tenancy and security requirement are combined by introducing three mechanisms, described below.

Security Groups: Security groups are sets of networking rules (in effect a firewall) applied to all VM instances associated with a group. In practice a security group defines the access rules for all VM instances associated with a group. For example, a user can specify ingress rules, such as allowing ping (ICMP) or SSH (TCP, port 22) traffic to reach VMs in a specific security group. Note that when you create a VM instance, unless otherwise specified at instance run-time, it is assigned to a "default" security group that denies incoming network traffic from all sources. Thus, to allow login and usage of a new VM instance you must authorize network access to the default security group.

Elastic IPs: With elastic IPs the user gains control over a set of Public IP addresses. Once allocated to the user, those same IPs can be dynamically associated to running instances, thus overriding pre-assigned public IPs. This allows users to run well-known services (e.g., Web sites, etc.) within the Eucalyptus cloud.

VM Isolation: While network traffic between VM instances belonging to a security group is always open, Eucalyptus can enforce isolation of network traffic between different security groups. This is enforced using a VLAN tag per security group, thus, protecting VMs from unwanted eavesdropping by VM instances belonging to other security groups.

Implementation of the isolation mechanisms

One of the most crucial aspects of the resource security in the typical private cloud is the security of the virtualization mechanisms. The ability to provide multi-tenant cloud services at the infrastructure, platform, or software level is often underpinned by the ability to provide some form of virtualization to create economic scale. However, use of these technologies brings additional security concerns. The reality of current practices related to management of virtual operating systems is that many of the processes that provide security-by-default are missing, and special attention must be paid to replacing them. Especially, two aspects are to be mentioned and underlined [8]:

- the efficacy and feasibility of segregating VMs and the possibility to creating security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data on separate physical hardware components such as servers, storage, etc.
- administrative access and control of virtualized operating systems which should include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and isolation tools.

Analyzing above aspects, we tested the instances separation inside private cloud. Within Eucalyptus, the cluster controller handles the set up and tear down of instance virtual network interfaces. The instance's private interface is connected via a bridge to a fully virtual software Ethernet system [7]. Once a VDE network has been created, connections to real Ethernet networks can be established through the Universal TUN/TAP interface, which, in essence, provides Ethernet packet communication from the Linux kernel. To meet VM isolation requirement, each set of instances owned by a particular user is assigned a tag that is then used as a virtual local area network (VLAN) identifier assigned to that user's instances. Once a VLAN identifier has been assigned, all VDE switch ports that are connected to the instance's private interfaces are configured to tag all incoming traffic with the VLAN tag and to only forward packets that have the same VLAN tag. Hence, a set of instances will only be forwarded traffic on VDE ports that other instances in the set are attached to, and all traffic they generate will be tagged with a VLAN identifier at the virtual switch level, thus isolating instance network traffic even when two or more instances are running on the same physical resource [7]. That procedure illustrates the figure 6.

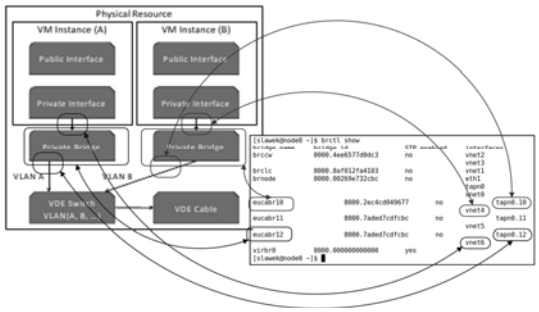

Fig.6. The instances isolation inside the IaaS private cloud

Conclusion

Eucalyptus security tools are very important mechanism because the private clouds are deployed within the organization's existing data center, and in most cases behind the organization's firewall, thus the private cloud is subject to the organization's security regulations. Presented results have proved that:

- single machine approach can easily utilize resources security mechanism.
- developed single machine testbed has all the security features (VM isolation, elastic IP, security groups).
- have the same characteristic as the large cloud systems developed in the distributed environments.

REFERENCES

[1] Mell P., Grance T.: The NIST Definition of Cloud Computing, *National Institute of Standards and Technology*, (2011)

[2] Foster I., Zhao Y., Raicu I., Lu S.: Cloud Computing and Grid Computing 360-Degree Compared, *Grid Computing Environments Workshop*, (2008), 1-10

[3] Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., Zaharia M.: Above the Clouds: A Berkeley View of Cloud Computing, *UC Berkeley Reliable Adaptive Distributed Systems Laboratory* , (2010)

[4] Vaquero L M., Rodero-Merino L., Caceres J., Linder M.: A Break in the Clouds: Towards a Cloud Definition, *ACM SIGCOMM Computer Communication Review*, 39, No.1, (2009), 50–55

[5] Wood L.: Cloud Computing and Compliance: Be Careful Up There, *ITWorld*, (2009) (http://www.networkworld.com/news/2009/013009-cloud-computing-and-compliance-be.html)

[6] Johnson D., Murari K., Raju M., Suseendran R.B., Girikumar Y.: Eucalyptus Beginner's Guide – UEC Edition, *CSS Corp.*, http://www.csscorp.com/eucauecbook, (2010)

[7] Przyłucki S., Sawicki D.: Cloud computing testbed, *Studia Informatica*, 32, No. 3A, (2011), 83-92

[8] Lombardi F., Di Pietro R.: Secure virtualization for cloud computing, *Journal of Network and Computer Applications*, 34, (2011), 1113-1122

***Authors**: dr inż. Sławomir Przyłucki, Politechnika Lubelska, Katedra Elektroniki, ul. Nadbystrzycka 38a, 20-618 Lublin, E-mail: spg@politechnika.lublin.pl; mgr inż. Daniel Sawicki, Politechnika Lubelska, Katedra Elektroniki, ul. Nadbystrzycka 38a, 20-618 Lublin, E-mail: sawi@politechnika.lublin.pl.*