Chapter 82
Securing the External Interfaces of a Federated Infrastructure Cloud

Philippe Massonet
Centre d'Excellence en Technologies de l'Information et de la Communication, Belgium

Syed Naqvi
Centre d'Excellence en Technologies de l'Information et de la Communication, Belgium

Arnaud Michot
Centre d'Excellence en Technologies de l'Information et de la Communication, Belgium

Massimo Villari
University of Messina, Italy

Joseph Latanicki
Thales Services, France

ABSTRACT

This chapter describes an open source solution for securing the Claudia service manager and the OpenNebula virtual execution environment manager when combined in a federated RESERVOIR architecture. The security services provide confidentiality, authentication, and integrity by securing the external API. The chapter describes how to integrate the security solution in an open source cloud computing system, how to install it, and provides an illustrative case study showing its potential for the community. The aim of the chapter is to help those who want to build their own secure infrastructure clouds. The open source security code provides mutual authentication between clients and the Claudia service manager, and secures the SMI interface with role based access control. The same security services can also secure the VMI with role based access control and X509 certificates. Finally the federation can be secured by combining an LDAP server to manage the federation and XACML security policies, and using policy matching to guarantee the respect of security policies within the federation.

DOI: 10.4018/978-1-4666-2919-6.ch082

INTRODUCTION

Large infrastructure clouds such as Amazon EC2 (Amazon, 2011) are becoming increasingly popular. Such clouds rely on a large shared and scalable infrastructure that is accessible through the public internet to a large customer base. Many different types of applications are being deployed on such infrastructure clouds. They range from enterprise applications from multiple domains such as publishing (New York Times, 2008) down to distributed file systems (Hendrickson, 2008). Many successful cloud projects have been initiated individually within companies and corporations. These successes have raised questions about the generalized usage of cloud computing within companies and corporations. One of the main issues that have been debated is the security risks that are faced when deploying applications on shared infrastructure clouds. Several studies have recommended the use of a risk management approach to deal with the security risks of deploying an application on a cloud. The risk management approach aims to clearly identify the security requirements of the application to be deployed, and identifying a cloud provider with the adequate security measures (Hogben & Catteddu, 2009). To remain competitive in the cloud market, infrastructure providers need to secure their infrastructure clouds so that they can meet their customer's outsourcing policies and their associated security requirements.

To provide Infrastructure as a Service (IaaS) with an infrastructure cloud that has a sufficient level of security some important security threats must be addressed. The level of security that is required will depend on the kind of infrastructure cloud that is being developed: a private cloud will require a lower level of security than a public cloud that is accessible to a large community via the public internet. Infrastructure clouds face the same threats as current data centers, plus new cloud specific threats. The main threats that must be addressed can be classified as external or internal threats. The main external threats are linked to man-in-the-middle, TCP hijacking (spoofing), malicious service manifest, identity theft/impersonation, false migration and security policies, denial of service (DoS or Distributed DoS), flooding, buffer overflow and peer to peer attacks. Internal infrastructure cloud threats are related to runtime isolation, network isolation and storage isolation.

This chapter explains how to secure the external interfaces of a federated infrastructure cloud using open source components. It explains how to install the security services for securing the external API of a federated infrastructure cloud. This chapter assumes that the federated infrastructure cloud implements the RESERVOIR architecture API (Rochwerger, et al., 2009). The RESERVOIR architecture (Rochwerger, et al., 2009) is used as a reference for federated clouds. The architecture introduces a virtualized infrastructure layer on top of the physical infrastructure: every site is partitioned by a virtualization layer into virtual execution environments (VEEs). These environments are fully isolated runtime modules that abstract away the physical characteristics of the resource and enable sharing. A RESERVOIR cloud has three different layers described as follows:

- Service Manager (SM) is responsible for the instantiation of the service application.
- Virtual Execution Environment Manager (VEEM) is responsible for the placement of VEEs onto VEE hosts.
- Virtual Execution Environment Host (VEEH) represents a virtualized resource hosting a certain type of VEEs.

The security services allow securing the service manager and the federation that is managed by the virtual execution environment manager of a cloud based on the RESERVOIR architecture.

This chapter is organized as follows: the "background" section describes the RESERVOIR architecture, describes the public API, and in-