國立政治大學資訊科學系
Department of Computer Science
National Chengchi University

碩士論文

Master's Thesis

雲端運算環境下檔案更新管理之安全性研究

A Study on the Security of Patch Management in a Cloud Computing Environment

研 究 生：簡禎儀

指導教授：左瑞麟

中華民國一百零二年一月

January 2013

雲端運算環境下檔案更新管理之安全性研究

A Study on the Security of Patch Management in a Cloud Computing Environment

研究生：簡禎儀　　Student： Chen Yi Chien

指導老師：左瑞麟　　Advisor： Ray-Lin Tso

國立政治大學
資訊科學系
碩士論文

A Thesis
submitted to Department of Computer Science
National Chengchi University
in partial fulfillment of the Requirements
for the degree of
Master
in
Computer Science

中華民國一百零二年一月
January 2013

A Study on the Security of Patch Management in a Cloud Computing Environment

Abstract

As cloud computing techniques advance, Virtual Machines (VM) seems to be an appropriate solution than physical machine deployment. Having multiple instances of virtual machines cause more efficient use of computing resources to achieve the aim of energy consumption and cost effectiveness. In this thesis, Virtual Machine Image Catalogue (VMIC) is designed for helping users search and acquire expected virtual machine images promptly. Nevertheless, security of VMIC is also a crucial task to keep systems up-to-date and defends against security attacks. Pakiti is adopted to monitor patch status of physical and virtual machines, and schedules the warning information to remind security staffs to update the patches.

Keywords

Cloud security, Virtual machine image, Patch management

雲端運算環境下檔案更新管理之安全性研究

摘要

隨著雲端運算盛行，企業採用大量虛擬主機來取代實體機器，虛擬主機有效率的模擬實體機器達到企業減少能源耗損與提高成本效率目標。 文中提及虛擬主機映像檔目錄系統(VMIC)主要讓使用者能有效率搜尋期望的檔案並獲得下載的實體位置，故本論文研究重點著重在改進安全性在原 VMIC 系統，應用 Pakiti 監控系統來掌握更新檔狀況於實體機器或虛擬機器環境，使資安人員能在短期間內獲得正確資訊，及時升級更新檔避免攻擊災害發生。

關鍵字

雲端安全，虛擬主機映像檔，更新檔管理

Acknowledgement

終於寫到誌謝辭部分，也代表我的論文即將劃下句點。 當論文寫完的當下，真的很開心很感動，我終於可以放下心中的大石，領取那張期待已久的畢業證書。 從開始念書以來，因為外派瑞士工作的緣故，我的論文也擱置了很久，非常感謝左瑞麟老師這段時間的指導，讓我能夠在回國後，順利完成這份論文。 也非常感謝我的口試委員蔡國裕教授和葉國暉教授，針對我的論文給予很多寶貴的建議，獲益良多。

這三年來，經歷了很多事情，我的朋友們常常鼓勵我，讓我可以作學業兼顧。 也感謝政大的同學們，針對論文撰寫給我很多建議，節省許多寶貴時間。 CERN的朋友和國外的朋友，謝謝你們一直為我打氣。 一個曾經很重要的法國人，因為你的緣故給我最大的動力在短期間完成這任務。最後我要把這篇論文獻給我的家人，尤其是我親愛的弟弟，感謝他針對我的英文部分給我很多指導糾正，我的家人在這三年來給我最大的支持與鼓勵，謹以這三年來的成果，獻給我最親愛的家人。

TABLE OF CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Introduction

Cloud computing is one of the most influential technologies in the Information Technology (IT) industry and is revolutionizing the way IT resources are managed and utilized in the 21st century. Cloud computing is to scale the resource up and down flexibility. Customers request the resource depends on their usage amount. Cloud provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure [1].

The University of California, Berkeley gave a broader definition of cloud computing: cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The data center hardware and software is what we will call a cloud [2]. All cloud clients can just request resources without maintenance effort, and will be charged only when they really use such resource on-demand services.

In cloud computing, both software and hardware resources are distributed, which can be allocated and extended dynamically as services. To achieve better performance, the service providers have to prepare such great number of machines which will increase business cost. Therefore, the current trend is deploying virtual machines to reduce cost called virtualization. Virtualization improves scalability and optimizes hardware-resource. With virtualization, operating systems can be run in parallel on a single central processing unit (CPU). This parallelism utilizes hardware resources and tends to reduce overhead costs.

What cloud clients also emphasize on is service reliability and security issues. Since virtualization will be greatly used in the future, the cloud providers need to ensure that their infrastructure is secure and that their clients' data and applications are protected. Virtual machine is extensively utilized and expected to reduce the physical machines in usage. However, deploying a virtual machine is not strict as a physical machine; its security should not be undervalued and underpaid. In this thesis, we will discuss security issues with virtual machines.

1.2 Thesis Architecture

The paper is organized as follows. Section II we introduce the current background and related work of cloud computing security and virtualization. And also mentions the motivation to study about virtual machine image security. Section III we discuss about the approach of virtual machine image catalogue system consists of the essential components. Section IV it mentions security improvement and solution of the approach. Section V discuss about the future work to achieve. Finally conclusions are drawn in section VI.

2 Background and Related Work

2.1 Cloud Computing

Since Internet is coming, users can search the information via the browsers. The browsers interact with Domain Name Server (DNS) and network servers to capture the information to represent on the client's browsers. It is not necessary for users to understand the middle process; users only care about the performance of service providers (servers) and service requesters (clients). As the result of Internet is popular and the bandwidth is raised, many kinds of equipments that can access the Internet are developed, it means users can use not only personal computer but also other equipments to access the Internet. Application will not be limited to read web pages or receive e-mails; users want to provide electronic commerce, customization or high-performance computing processing on the Internet. Therefore cloud computing is caused. In figure 2-1, we can understand the cloud involves network, computing, storage and many services. Ian Foster mentioned the definitions for cloud computing in 2008, cloud computing is a large-scale distributed computing paradigm that is driven by economies of scale in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet [3].

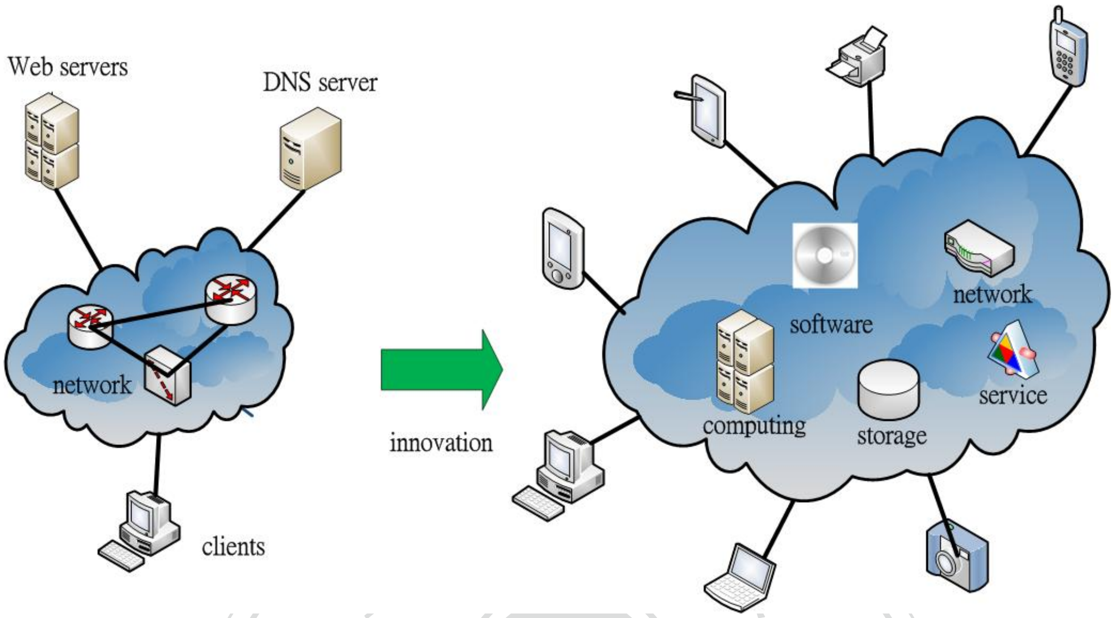


Figure 2-1 Cloud Computing.

2.1.1 Cloud Service Models

There are three layers of the typical cloud fundamental models in figure 2-2: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [1]. According to Cloud models, The National Institute of Standards and Technology (NIST) provides the details definition below [4]. Our approach is based on IaaS.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components Amazon Elastic Compute Cloud

(Amazon EC2) is a typical example.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, but has control over the deployed applications and possibly application hosting environment configurations. This kind of consumer is a software programmer.

Software as a Service (SaaS). The capability provided to the consumer is to use the service provider's applications running on a cloud infrastructure. The applications are accessible from various client devices such as a web browser or mobile phones. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

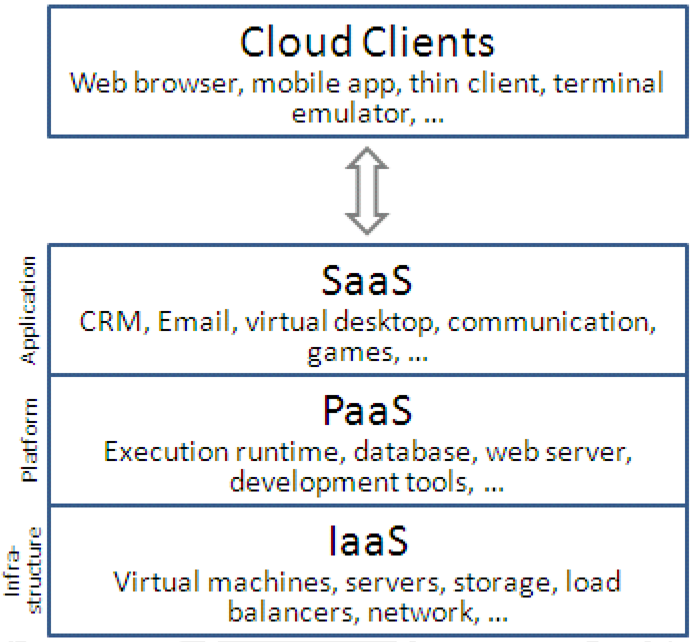

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 2-2 Cloud computing layers [1].

2.1.2 Cloud Computing Security

Security is one of the largest urgent concerns of cloud computing. Cloud computing security, simply speaking is to refer to a number of policies, technologies, and controls deployed to protect valuable data, applications, and the associated infrastructure of cloud computing. Cloud Service provider should make effort in ensuring the data is safe and protected [5]. Regarding the concept of cloud computing security has following definition.

Identity management

Every enterprise has its specific Identity Management System to control access to information or computing resources. Hence, cloud providers integrate the customer's Identity Management System into their infrastructure, using federation or Single-Sign-On (SSO) technology, or according to the requirement to provide the solution.

Physical and personnel security

Cloud service providers ensure the physical machines are under completely security protection and that access to these machines as well as relevant customer data is not only restricted but the access record is traced.

Availability

Cloud service providers ensure customers are able to access the data and applications regularly.

Application security

Cloud service providers ensure their available applications are secure via the cloud by implementing testing and acceptance procedures for outsourced or packaged application code.

Privacy

Cloud service providers ensure that all sensitive and critical data are masked (for example: credit card numbers) and that only authorized users can access to data in its entirety. In addition, digital identities and credentials must be protected.

As the convenience of cloud computing, a number of services are tended to support cloud development. Many enterprises provide cloud applications and services. It means some sensitive and customer information will published on the Internet. Enterprises must ensure these data be secure not to access from irrelevant people. Security is the important field in IT, people always need to consider security issue to avoid the terrible accident happened, especially virtualization application in Cloud.

2.2 Virtualization

Virtualization, simply speaking is the creation of a virtual version of hardware platforms, operating systems, storage device, and network resources [6].

The virtualization concept was initially discussed since 1950, in recent years the popularization of server virtualization technique, it brings a brand-new data center deployment and management method to assist managers earning high efficiency and convenient management experience. Virtualization is to upgrade resource utilization and reduce energy consumption as well. Figure 2-3 is shown the overall virtualization [7].

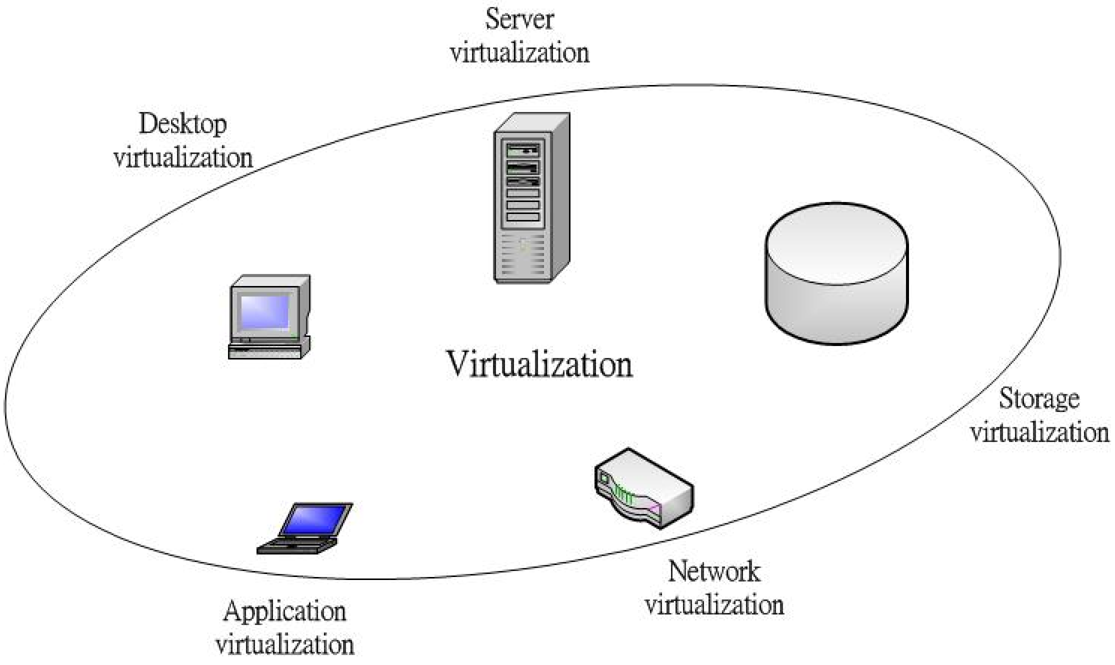


Figure 2-3 Virtualization.

Enterprises trend to virtualization generally, the mostly reason is the advantage they can gain.

1) **Cost reduction:** to reduce procurement, maintenance cost and operating expenses.
2) **Improvement of application compatibility:** many services and programs can apply

on different platform.

3) **Acceleration of deployment:** deploying a System-in-Package service to reduce time and cost.

4) **Improvement of service availability:** extension of continual and stable service. Even if system failure or hardware failure, the service can recover at the short time.

5) **Improvement of resource utilization:** system administrator integrates many virtual machines into one physical machine to increase resource utilization.

6) **Resource on dynamic scheduling:** real-time adjustment of resource.

7) **Energy consumption reduction:** close idle physical servers to reduce the sum of running machine.

In virtualization, many enterprises use a large number of virtual machines to replace physical machines; it will reduce considerable enterprise cost. See figure 2-4 shown after virtualization, one physical machine can install more virtual machines and run the same services. Hence enterprises must to create or gain virtual machine images to deploy their cloud environments. Because of many virtual machine images, people start to take account of the image security.

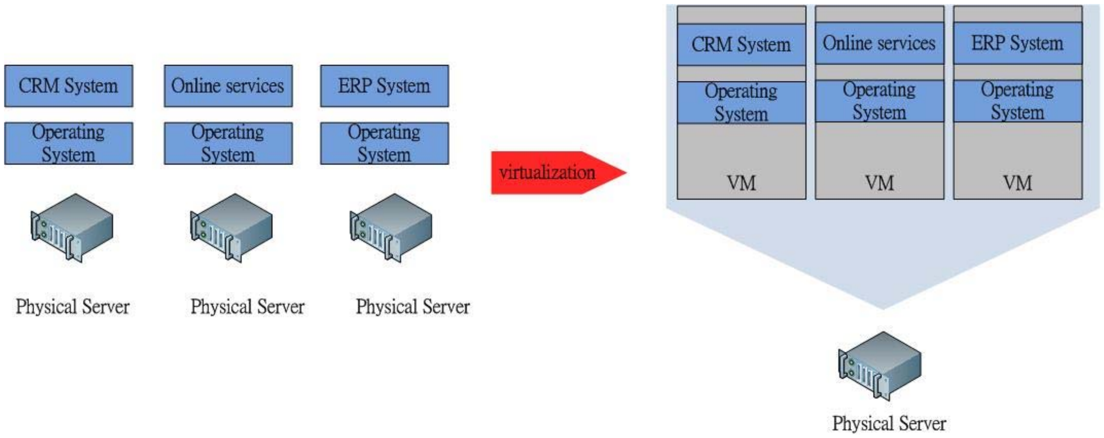


Figure 2-4 Server virtualization.

The following topics will introduce virtual machine image application and security. The approach is the development of a software tool to facilitate the distribution of virtual machine images between different sites. It also points out the security improvement according to the current system.

2.2.1 Virtual Machine Infrastructure

Follows the cloud computing applications popularly, plenty of enterprises want to reduce the assets cost but keep the available requirement; they try to use virtual machines to execute in the environment. In General, current cloud platform consists of a large number of virtual machines. A virtual machine, an efficient, isolated duplicate of a real machine [8], is a software implementation of a machine that executes programs like a physical machine. Modern virtual machines are implemented with either software emulation or hardware virtualization or (in most cases) both together [9]. Thus, a virtual machine provides a complete system platform that supports the environment of an operation system and expects to run multiple operation systems at the same time on one physical machine. Our approach is about the application of virtual machine image, the first draft implementation was published at The High Energy Physics Unix Information Exchange (HEPiX) meeting, and we will also have more details of virtual machine image security below.

List of System Virtual Machine

Name	Developer	Operation System
KVM	Read Hat , Inc	Linux kernel
Oracle VM VirtualBox	Oracle Corporation	Microsoft Windows, Mac OS X, Linux and Solaris
VMware	VMware, Inc.	Microsoft Windows, Linux, and Mac OS X
Xen	The Xen Project XenSource, Inc.	Linux, and other Unix-like, *BSD, OpenSolari, Microsoft Windows.

- **KVM** Kernel based Virtual Machine, an open-source software, is a full virtualization infrastructure for Linux on x86 hardware containing virtualization extensions [10][11].

- **Oracle VM VirtualBox** is a powerful x86 and AMD64/Intel64 virtualization software package for enterprise. It created by software company Innotek GmbH, purchased by Sun Microsystems, and now developed by Oracle Corporation. At present, Oracle VirtualBox executes on Windows, Linux, Macintosh, and Solaris hosts [12][13].

- **VMware** , a company providing virtualization software, delivers customer-proven solutions that accelerate IT by reducing complexity and enabling more flexible, agile service delivery. VMware's desktop software runs on Microsoft Windows, Linux, and Mac OS X, while VMware's enterprise software hypervisors for servers, VMware ESX and VMware ESXi are bare-metal embedded hypervisors that run directly on server hardware without requiring an additional underlying operating system [14][15].

- **Xen**, an open-source industry standard for virtualization, is a virtual-machine monitor providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently. Xen offers an efficient and secure feature set for virtualization of x86, x86_64, IA64, ARM, and other CPU architectures. In the beginning, the University of Cambridge Laboratory developed the first versions. Since 2010, the Xen community develops and maintains Xen as free software, licensed under the GNU General Public License (GPLv2) [16][17].

2.2.2 Virtual Machine Image Catalogue

The European Organization for Nuclear Research (CERN) started in 1954. It is the world's largest physics laboratory and its location on Swiss and French border. The famous World Wide Web was birthed from CERN. All the time, CERN IT involves in different computer science's fields and is developing a different set of tools to import the cloud computing infrastructure. In 2009, CERN IT and HEPiX Virtualization Working Group published a proposal about the virtual machine image management in HEPiX conference.

Simply speaking, VMIC is a catalogue of virtual machine images. It can subscribe images list from other sites and easily export an image list for other sites. Sites can choose to trust only specific endorser or even a single image. All virtual machine images files and metadata are preserved for traceability. A trusted endorser can maintain a set of valid virtual machine images. The set is maintained the latest with security patches and updated regularly. All trusted virtual machine images are managed via VMIC and only trusted endorsers can publish and maintain images from VMICs [18]. Each site can setup their personalized VMICs. Sites may decide to trust endorsers and all the virtual machine images. All endorsers and sites should comply with the security policies from the SPG.

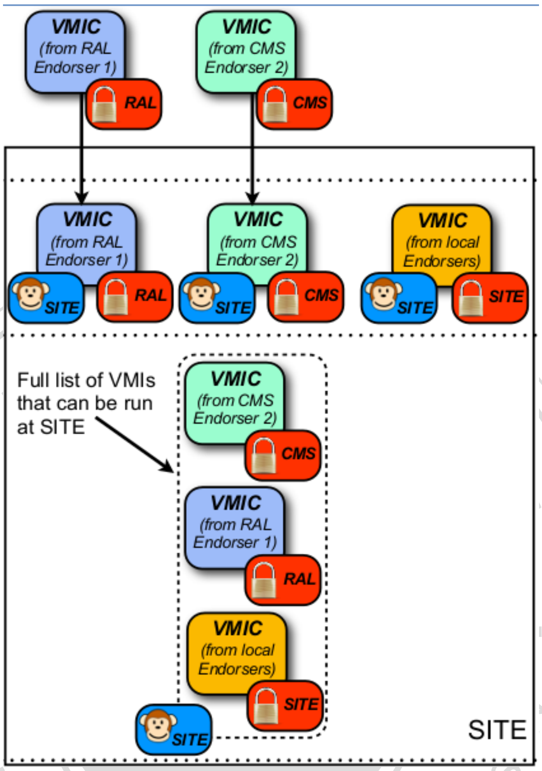

VMIC (from RAL Endorser 1)
RAL
VMIC (from CMS Endorser 2)
CMS
VMIC (from RAL Endorser 1)
SITE
RAL
VMIC (from CMS Endorser 2)
SITE
CMS
VMIC (from local Endorsers)
SITE
SITE
Full list of VMIs that can be run at SITE
VMIC (from CMS Endorser 2)
CMS
VMIC (from RAL Endorser 1)
RAL
VMIC (from local Endorsers)
SITE
SITE
SITE

Figure 2-5 VMIC architecture and concept [18].

Figure 2-5 showed in VMIC this diagram several scenarios of image trust are depicted. Two endorsers from RAL and CMS have published a VMIC. A site approved those VMICs as well as its local one from a local endorser. This populates a list of virtual machines that can be used at the site. The local image distribution system can be hooked onto the local listing of approved VMIs to automatically pre-stage the images [18].

Academia Sinica Grid Center (ASGC) [19] applies VMIC as the component of their distributed cloud computing environment [20]. As shown in Figure 2-6, when a site approves a virtual machine image from an endorser, the virtual machine image information will be imported to the site VMIC database. Then this site can do a real subscription of an approved image. When approved images are stored in a site, it is published a new image list as well as redistribute and re-endorse those on-site images. VMIC works with many replications in different sites and different communication protocols such as gridftp, bit torrent Peer to Peer ...etc. Therefore sites can always pick up their best access method to subscribe images.

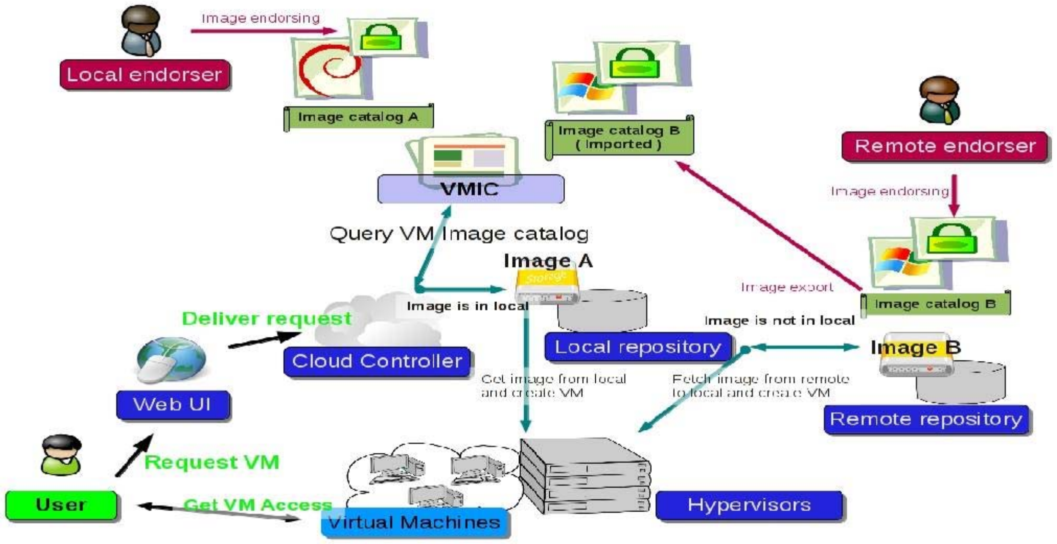


Figure 2-6 VMIC image endorsing and trusting of distribution [20].

2.2.2.1 HEPiX Virtualization Working Group

The High Energy Physics Unix Information Exchange (HEPiX) forum brings together worldwide Information Technology staffs, including system administrators, system engineers, and managers from the High Energy Physics and Nuclear Physics laboratories and institutes, to foster a learning and sharing experience between sites facing scientific computing and data challenges [21]. Its Participating sites around the world and its organization was formed in 1991. HEPiX is a twice yearly conference in spring and fall.

HEPiX Virtualization Working Group is one session of HEPiX, it was made in the spring 2009 HEPiX. HEPiX Virtualization Working Group is to investigate the implications use-cases and requirements of sites that where at the time expected to come from the relatively new technology of Virtual Machine technology. Main focus is to provide sites a way to control and mange Virtual Machine Image's provided by experiments, and run them in trusted environments with in the current computing environment provided under Grid computing. There are two objectives of HEPiX Virtualization Working Group; one is to produce a framework to securely run Virtual Machine Images across multiple sites supporting High Energy Physics, the other is that sites need to control over Virtual Machine Image selection [22]. VMIC was published on HEPiX conference in 2009 and cooperate with HEPiX Virtualization Working Group. The HEPiX Virtualization Working Group applications are VMIC, StratusLab[23], and Repoman [24].

2.2.2.2 Image Trust

All images published or subscribed must trust the security policy, VMIC security policy is based on EGI Security Policy Group (SPG). The details of image trust will be introduced below. EGI.eu is a not-for-profit foundation established under Dutch law to coordinate and manage the European Grid Infrastructure (EGI) federation on behalf of its participants: National Grid Initiatives (NGIs) and European International Research Organizations (EIROs) [25]. EGI.eu is to promote collaborative work within the community and to integrate the computing resources provided by the different members of the EGI federation. EGI Security Policy Group (SPG) is based on EGI Infrastructure to support all strategy and policy documents and papers that its daily activities in grid operations, software quality, security and user communities. SPG also supports HEPiX in security policy for the Endorsement and Operation of Virtual Machine Images [26].

SPG defines the following terms.

- Endorser: A role, held either by an individual or a team, who is responsible for confirming that a particular virtual machine image has been produced according to the requirements of this policy and states that the image can be trusted. An Endorser should be one of a limited number of authorized and trusted individuals appointed either by the Infrastructure Organization, a Virtualization Organization (VO) or a resource centre. The appointing body must assume responsibility for the actions of the Endorser and must ensure that he/she is aware of the requirements of this policy.

- Virtual Machine operator: A role, held either by an individual or a team, who is responsible for the security of the virtual machine during its operation phase, from the time it is instantiated, until it is terminated. Typically this addresses individuals with root access on the virtual machine.

- Third party: An external entity other than the resource centre where the virtual machine is operated [27].

2.2.3 Virtual Machine Image Security

Virtualization the companies' IT infrastructure lets owners reduce IT costs while increasing the efficiency, utilization, and flexibility of their existing assets. Around the world, companies of every size benefit from virtual machine virtualization. Virtual machines let people share the current resources of a single physical computer across multiple virtual machines for maximum efficiency. Those resources are shared across multiple virtual machines and applications. To get more and more benefits, the companies use large number virtual machines. The virtual machine as a forensic tool in security field, the Operation system can be booted into a virtual machine, the investigator can perform investigation works in a live system, directly and repeatedly, and the efficiency is improved [28]. Creating virtual machine images it to simplify the whole installation process, the related software involves operation system, applications, security patches. Due to the federation cloud concept, these images should be created, trusted, transferred and submitted between sites and sites. At the same time, people start to take account of virtual machine image security issue.

A cloud service provides three types of resources: a set of virtual machine images, a set of computer servers for virtual machine images environment, and a storage space to store the related data. While reducing cost is a primary motivation and objective for moving towards a company or a cloud provider, reducing responsibility for security or privacy should not be. Virtual machine images are unique and special entities in the cloud. The security and integrity of such images are the foundation for the overall security of the cloud because Virtual machine images need high integrity, because they determine the initial states of running virtual machines, including their security states. Second, many of the virtual machine images are designed to be shared by different and often unrelated users. On the other hand, sharing of virtual machine images poses privacy and safety issues.

An endorser should be one of a limited number of authorized and trusted individuals appointed either by sites, can create and publish image files with no limit. Therefore, the endorsement of a virtual machine image should be defined by the standard and trust third party or policy. Images are referenced by an image list which contains a secure hash (SHA512) signed using x509 technology. These image lists are published, and interested sites subscribe to the lists in a catalogue at the site. When an instantiation request for an image is received, the image validity is checked. If the image list is valid, the image is contextualized and then instantiated. Images that do not pass validation are not instantiated [29].

Sharing virtual machine images is a common action in some cloud computing environments. Such techniques mainly focus on two aspects of security: 1) security of running instances, and 2) integrity and privacy of customer data [30]. Image repositories, the real deposition of image files must be carefully managed and controlled to avoid security problem. Since an image can contain proprietary source code and sensitive data, the provider of an image will face risks [31]. In opposition to an attacker may attempt to supply a virtual machine image containing malware and risks to users of a cloud computing system [32]. Virtual machines and applications need to be secured in IaaS Clouds. Following policies and procedures, hardening of the operating system and applications should occur to procedure virtual machine images for deployment. Care must also be taken to make adjustments for the virtualized environments in which the images run. So managing virtual machine images carefully is also import to avoid accidently deploying images containing vulnerabilities [31].

3 Virtual Machine Image Catalogue System

Since production of image files rise steadily, sharing virtual machine images has become a simple case around the world. Users could easily construct a new virtual machine by using shared images; however, to find the suitable image file entails a lot of work. Therefore, it is an essential requirement to assist people getting their wanted image files from numerous resources. In this thesis, we propose the Virtual Machine Image Catalogue system (VMIC) to fulfill the requirement. CERN and HEPiX Virtualization Working Group published this conception of image catalogue system on HEPiX fall meeting in 2009, and realized a draft system and web interface to provide simple service. In 2011, CERN and ASGC started to cooperate with this virtual machine image catalogue project to improve original system and add new functions to reach high performance; in this chapter, we will introduce the system structure of VMIC and the functionalities.

3.1 System Introduction

The Virtual Machine Image Catalogue system (VMIC) is to implement a useful software tool to facilitate the management of internal images and the image distribution between different sites. The images are pre-cached in the compute nodes. Users expect to search all useful virtual machine image information on the catalogue, find the exact location to download those files.

The system is based on Scientific Linux CERN6 (SLC6) a Linux distribution build within the framework of Scientific Linux which rebuilt from the freely available Red Hat Enterprise Linux 6 (Server) product sources under terms and conditions of the Red Hat EULA [32]. This system is developed in Python language and uses OpenStack software to manage virtual machine, user accounts and passwords. OpenStack is open-source software for building private and public clouds, in other words, OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface [33]. Glance OpenStack in this system is to provide services for discovering, registering, and retrieving virtual machine images. And virtual machine images made available through Glance can be stored the object-storage systems such as OpenStack Swift. The system integrates with HEPiX Virtualization Working Group tools to create and subscribe image lists. Depends on the result of subscription, the approach will add images when images are subscribed or remove images when images are unsubscribed. Keystone is an OpenStack project that provides Identity, Token, Catalog and Policy services [37]. VMIC project uses OpenStack Keystone to manage user accounts and passwords. In Glance, there are several storage backend to use by default when storing images. Swift is one of them. VMIC will preserve a copy of each image in the VMIC Image archive. The image archive will use Swift. For Glance, when the image is registered it is created a new entry in the image service and a new image copy in the Glance store method. Figure 3-1 is shown the architecture and concepts of virtual machine image catalogue (VMIC) [34]. Image administrator use VMIC or HEPiX tool to image lists with updated images, before publishing those image lists, image administrator uses HEPiX tool to subscript the image list and gets checksum to append the image file. Image information and metadata will save in OpenStack Glance and OpenStack Swift via Glance Application Programming Interface (API). And Keystone will be used for the authentication with Glance server. So users can search images and list all available images with VMIC. And then they can get the image’s location to download it. More details of this architecture and concepts will be explained later.

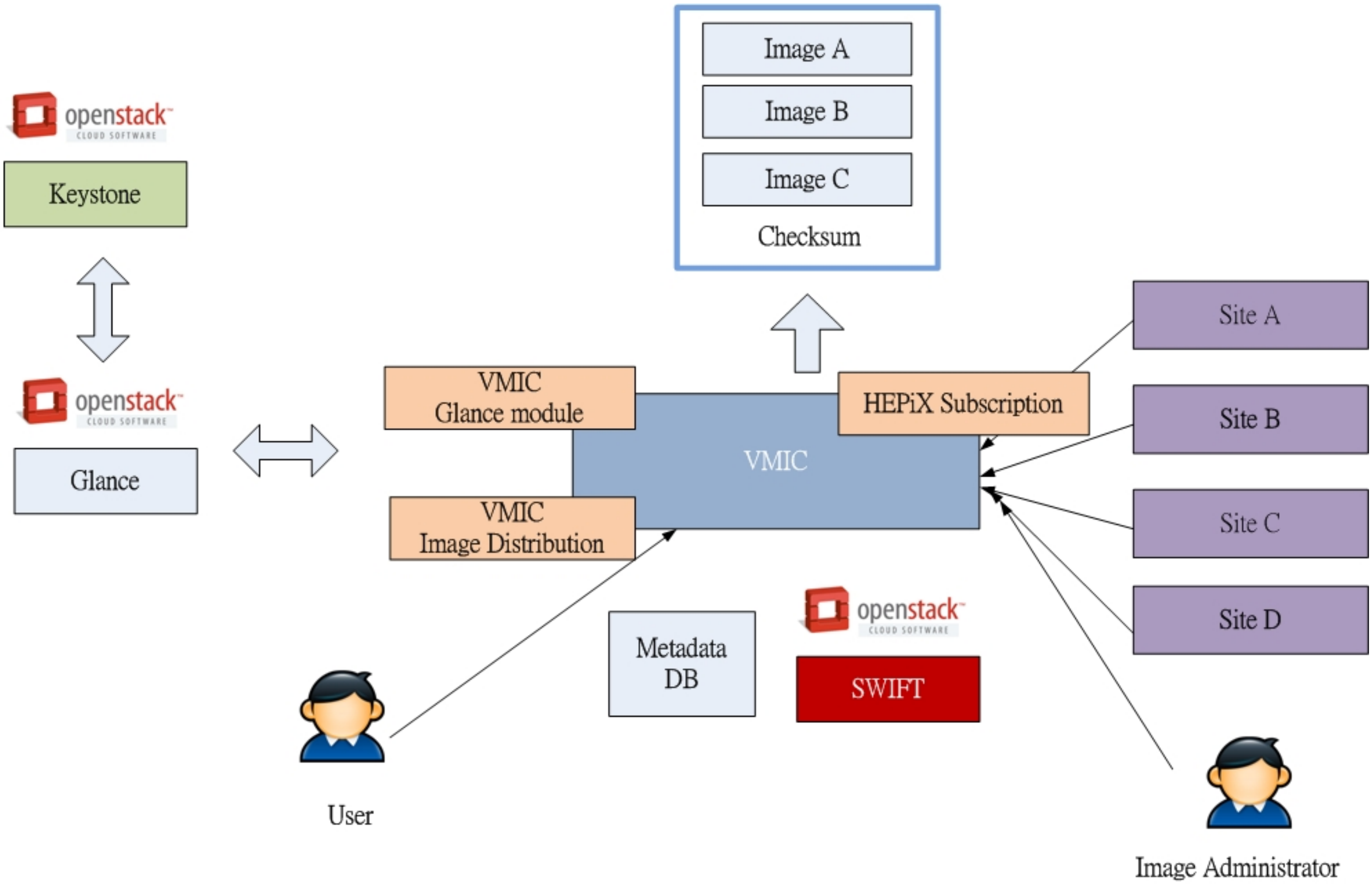


Figure 3-1 the architecture and concepts of VMIC.

3.2 Virtual Machine Image Catalogue Components

3.2.1 Command Line Interface

The VMIC CLI is a simple interface to manage images and image list information; users could easily execute the related commands by following the instructions. The VMIC CLI tool will be used to interact with OpenStack Glance image service using the Representational State Transfer (RESTAPI) provided. According to different data-interchange format, there are current three formats of metadata; eXtensible Markup

Language (XML), Javascript Object Notation (JSON) and Yet Another Markup Language (YAML). Hence image administrator is possible to create three kinds of image formats depends on his requirement. In short, the VMIC CLI is used for people to get trusted images easily from the available image list.

3.2.2 HEPiX Tool Subscription

Deutsches Elektronen-Synchrotron (DESY) [35] from Germany developed a set of tools that allows sites to distribute and subscribe images. With VMIC this system wants to change and improve all the flow that a user need to follow to expose images to others. The main focus is to reinvest the actual HEPiX image tools and integrate them with OpenStack Glance.

Add/subscribe an image should be easy and similar to what is implemented in the current version as Figure 3-1 mentioned. An image administrator will use the HEPiX tool to create a new image list with updated images in Figure 3-2. Then image administrator publishes this image list for other sites. This image list involves image information, image metadata and checksum in Figure 3-3.

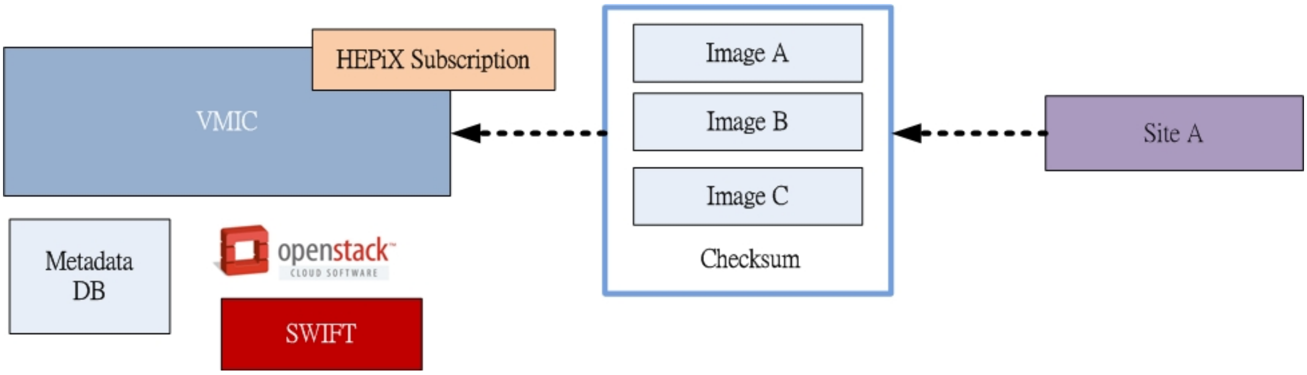


Figure 3-2 import images from other sites.

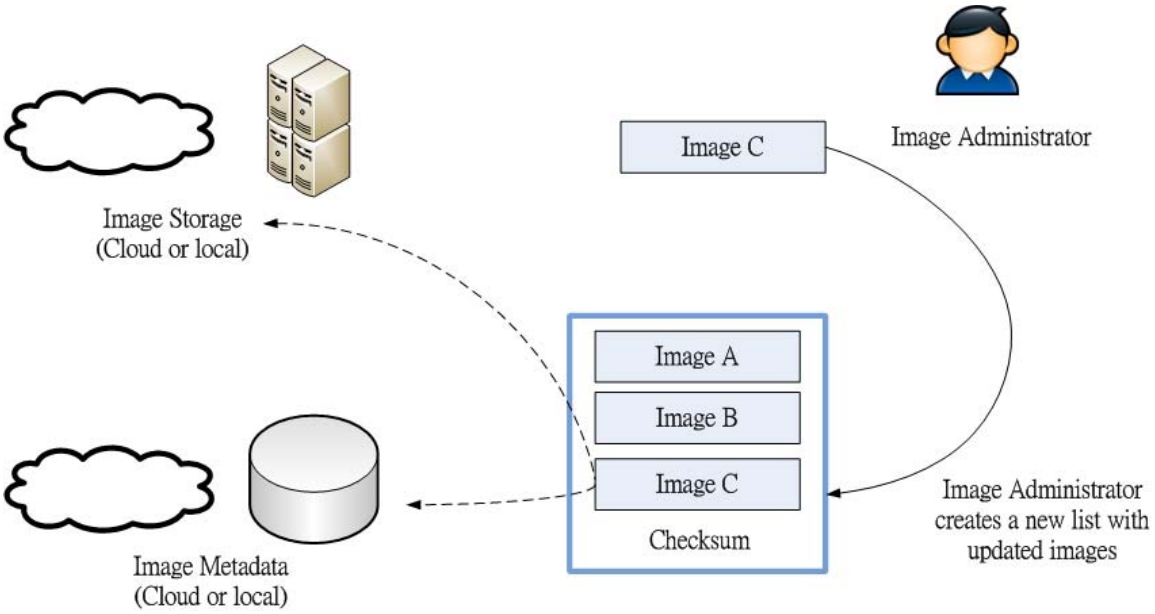


Figure 3-3 image list publication.

3.2.3 VMIC Image Distribution

At CERN, some applications such as vmbatch are used to fetch the instances faster if the images are pre-staged in the hypervisors. Several methods exist to transfer images between the image manager and the compute nodes; however, after several tests at CERN they concluded that the BitTorrent protocol is the best option. BitTorrent is a protocol that underpins the practice of peer-to-peer file sharing and is used for distributing large amounts of data over the Internet [36]. A BitTorrent node is as a seed, more seeds can get faster speed of download. When every VMIC (BitTorrent node) keep an image list, image metadata in the Database and image files in Glance server. RTorrent as a BitTorrent client can catch image files on high performance and faster speed. So VMIC image distribution is used this protocol for image distribution.

Figure 3-4 is the steps of image distribution:

a) The compute node queries VMIC for the image list.

b) The image integrity is verified.

c) Check which images are for the node.

d) Download the torrent files for the desired images.

e) Rtorrent downloads the images.

f) Image management software in the nodes deploys the new image.

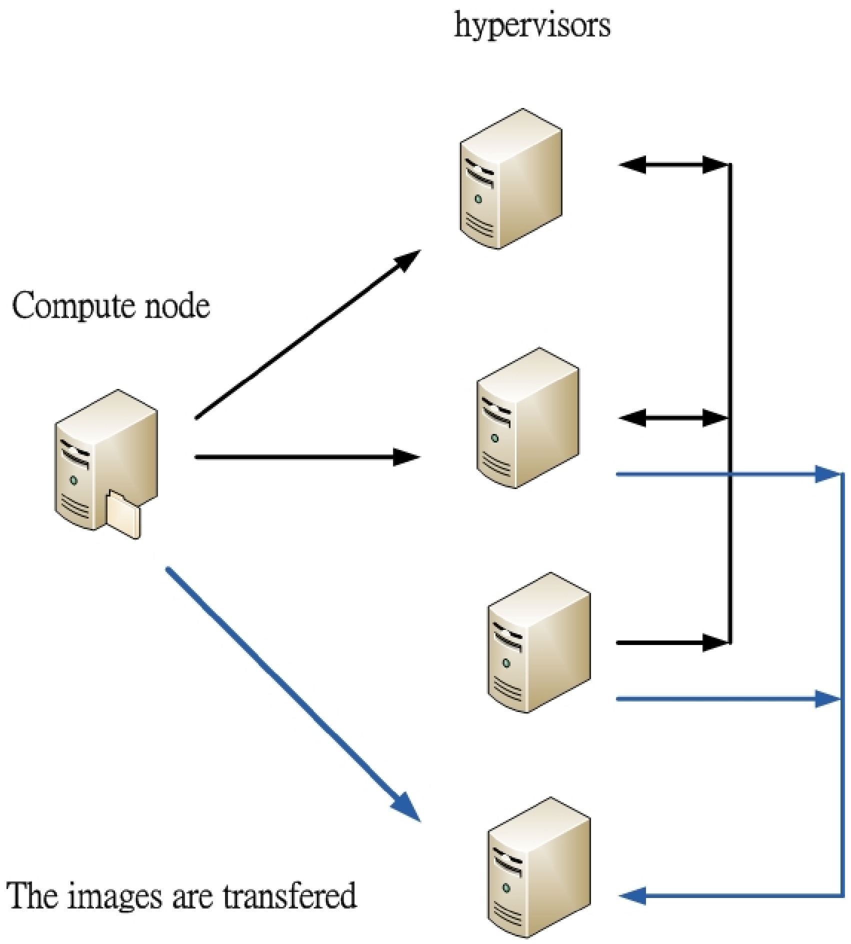


Figure 3-4 VMIC image distribution.

3.2.4 Glance Module and Authentication with Keystone

In Figure 3-5, when a user does some action of an image such as: added, removed or updated, the VMIC will preserve a copy of each image in the VMIC image archive by using Swift and in the Glance store method. In VMIC, Glance is integrated with Keystone which is used for the authentication. When editing the Keystone configuration files, it can set images permission and owner attribute according to different requirements.

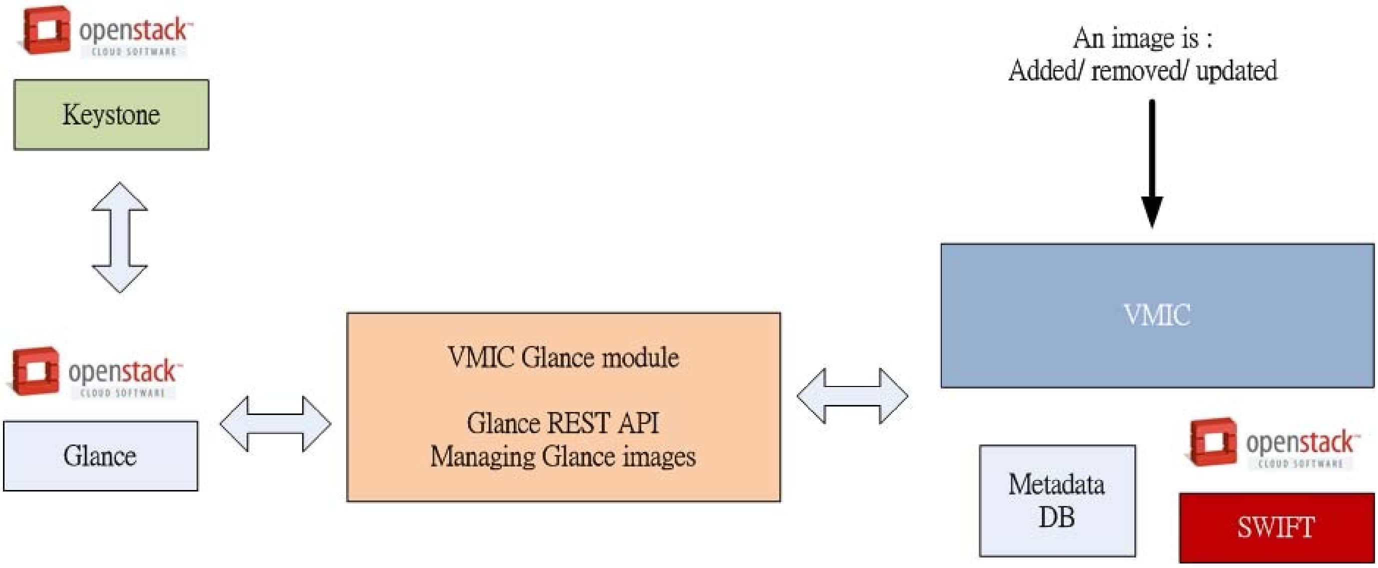


Figure 3-5 Glance Module and authentication with Keystone.

3.3 Security Considerations of VMIC

We have mentioned some virtual machine image security in 2.2.4, the VMIC is a catalogue system and to store virtual machine image metadata in Glance Swift. For cloud economical consideration, the VMIC will be used for different sites, different countries. More images transfers between each other, more attentions we have to pay on security events. Image metadata and image repository should be secured and stored in a safe place. Security patches of images should be updated regularly to avoid attacking. A reliable system is needed to help image administrator or users to check the safety of running and dormant virtual machine. We will propose some solutions in the next section.

4 VMIC Security Improvement

We have already mentioned about the whole system architecture of VMIC and pointed out its potential security problem. VMIC is a convenient tool for users to list trusted virtual machine image files; however, how to maintain information security will be a great challenge for the moment. We expect the following research is able to improve VMIC system current situation to protect users and image administrators.

4.1 Security Improvement

By now, many industries began to use plenty of virtual machines to replace the requirement of physical machines in cloud computing environment. Each physical machine can create multiple virtual machines to run specific programs. So that industries could reduce enormous procurement and gain much efficiency. Since virtual machines are easily to be created and reset, creating a new virtual machine seems to be the prior way when system crashes. However, this phenomenon makes users to ignore the security of virtual machines and reveal vulnerabilities for hackers to attack. When a virtual machine is infected by attackers, the attack may expand to other virtual machines via sharing memory, the connection of Internet or share resources. In Figure 4-1, the attack is caused by first virtual machine and expands to others.

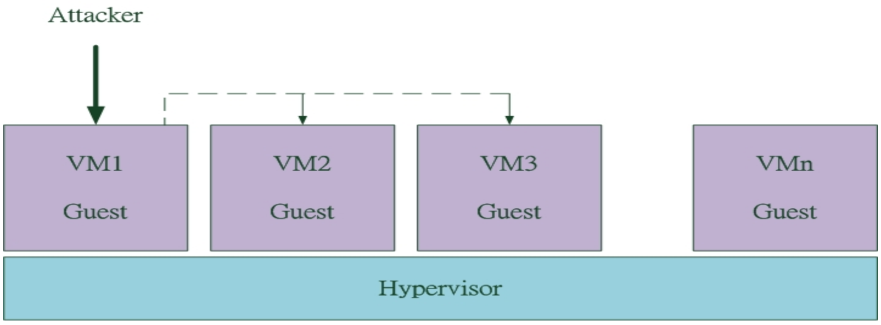


Figure 4-1 VM Communication Attack on VM2 and VM3 [38].

Besides, not only physical machines are vulnerable but also virtual machines are as well. For instance, there was some security incidents happened in Amazon EC2 when users use cloud resource. During the development of VMIC project, its original environment tends to internal not the public. But VMIC will apply to the distributed cloud computing in global organizations or international corporations everywhere in coming future, security mechanism should be considered. Security staffs must keep trace of all machines involve of virtual machines to ensure their status is monitored and maintained well. When they are attacked, security staffs must have the ability to minimize losses in time when hackers attack.

We have mentioned virtual machine security events in 3-3, virtual machine image metadata and image repository must be placed in a safe environment, and security patches from vendors should be updated regularly to avoid targeting attacks; moreover, some monitoring tools (Shavlik HfnetchkPro, eEye Retina, Microsoft SUS or Pakiti) could assist system administrators or security staffs to manage virtual machines when they are running.

Sometimes some unexpected problems appear after machines run for a period of time. At first these problems cannot detect, but afterwards they have vulnerabilities in computer applications that provide the attacker access to the system. A patch is a piece of software designed to fix problems includes security vulnerabilities, bugs and improve the usability or performance. The problem is caused by poorly designed patches. After a patch has been released by vendors, security staffs must notice and update the systems using this patch to keep off viruses, rootkits or worms. Briefly speaking, Security patches are the primary method of fixing security vulnerabilities in software [39]. In whole process, security staffs must ensure to own the patch is up-to-date before updating. If a new machine increases suddenly in original system, security staffs have to examine their system status involves security patches are the newest as well. It is essential for security staffs to continue analyzing and monitoring all machines are far from vulnerabilities; moreover, they must notice all patches release from vendors and update at the short time. Many security vulnerabilities were caused by security staffs ignore to update security patches and let attackers can access to the systems with a malicious code. For this reason, an efficient tool is needed to monitor the patch status and report patches of all machines, such as Pakiti, Nuwa. In next section, we will discuss patch management tools in detail, and point out how to use it to improve the current VMIC system.

4.2 Online Patch Management - Pakiti

A growth of large scale grid and cloud infrastructures are in operation around the world, which means that security staffs must be careful of the following security risk. Unpatched security vulnerabilities are often misused by wicked attackers to control machines or cause other harm to computers and other legal users. Security patch updates become one of the main causes of security incidents to affect computing infrastructures. Hence, having a proper and instant patch management is crucial to keep the system in safety and to resist common attacks targeting known weak spots. Pakiti [40] is a system that provides a monitoring and notification mechanism to check the patch status of machines.

Pakiti was originally designed by Steve Traylen in 2004 at the Rutherford Appleton Laboratory (RAL) UK. In the beginning, it provided a simple client and server to enable the team to detect the nodes where patches were missing. Romain Wartel (RAL/CERN) took over this basic tool and transformed into Pakiti, hosted on SourceForge. EGEE Operational Security Coordination Team (OSCT) adopted this tool to start to monitor the security patch status of its more than 200 sites. For the moment, Pakiti is used by plenty of research organizations and computing infrastructures around the world.

4.2.1 Pakiti Architecture

Pakiti is a client/server model, where clients and servers are exchanging information using HTTP(S) protocol. Once installed Pakiti service, Pakiti client will send the list of installed packages to the relevant Pakiti server(s) every night, then Pakiti server compares the versions against versions which Pakiti server obtains from packages repositories and Open Vulnerability and Assessment Language (OVAL) [42] definitions from MITRE [43] who applying systems engineering and advanced technology to critical national problems. OVAL is an XML language allowing specifying vulnerability, and OVAL identifies a complete set of conditions that describe at least the version of software components. OVAL is supported by RedHat, SuSe and Microsoft such as some large OS vendors. These vendors issue up-to-date version on each release of security patches. The main procedure of Pakiti can be defined as follows (see Figure 4-2).

(1) The hostname of Pakiti server is giving in the client configuration and verified during the SSL/TLS handshake in order to reduce the risk of leaking sensitive information. The cron jobs update scripts are run regularly, so all the information is sent from Pakit client to the Pakiti server using HTTP POST over HTTPS.

(2) When Pakiti server receives client's patches information, these data will save in Pakiti DB such as Mysql.

(3) After receiving information from clients, Pakiti server will make a list on the website.

(4) Up-to-date patches information is provided according to packages repositories or CVEs by cron jobs.

(5) By another way, Pakiti clients do not send information to server directly. They transfer patches information to Nagios this monitoring tool.

(6) When Nagios server catches these patches information, it will send them to Pakiti server.

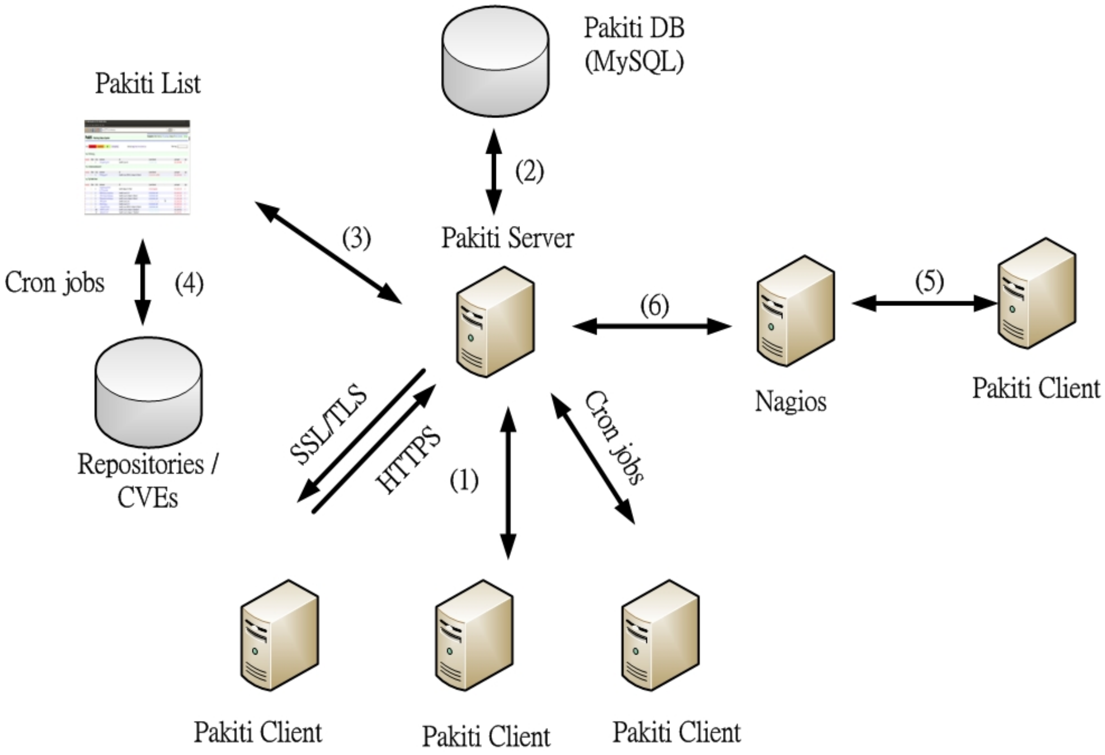


Figure 4-2 Pakiti environment.

Pakiti uses a Web page provides a list of the registered systems and the list of the pending patches for them. This helps security staffs to keep multiples machines up-to-date and prevent unpatched machines to be kept silently on the network. In addition, a security module in Pakiti is able to distinguish security fixes from normal bug fixes/product improvement for all Linux distributions which has packages repositories based on rpm (yum) or dpkg (apt) and has different location for normal and security updates. For Linux distributions based on the RedHat, Pakiti is able to check packages against the Common Vulnerabilities and Exposures (CVEs) [44]. In the next release Linux distros based on SuSE will be also checked. Debian based distros are also a candidate, but Debian currently does not provide approved data in CVE format [41].

CVE (Common Vulnerability and Exposure) is an international security organization, the most credible to expose security weaknesses and publish news. For the moment, CVE cooperates with many global organizations and product manufacturers. CVE is a unified vulnerability number of format and report message from firewall, antivirus software, intrusion detection systems, and system vulnerability scanning tools. Each published weakness has only CVE number (for example, CVE-2008-0234), to ensure this weakness is already identified and described. Each independent weakness number databases are unified with the standard numbers.

By now, Pakiti has been utilized by many organizations in the world especially EGI Computer Security and Incident Response Team (CSIRT) on daily basis. According to the result of the risk assessment, EGI CSIRT uses it to monitor all related sites. When EGI CSIRT finds these sites are running the vulnerable software, they contact site managers and ask to apply the updates immediately. If site managers ignore notifications without updating security patches in time, EGI CSIRT will follow the critical vulnerabilities handling procedure to suspend these sites to avoid unstoppable risks.

Every day the EGI Pakiti server receives more than 2300 reports from EGI production sites. Only Authorized EGI CSIRT members and site security staffs can check the result through a web interface (https://pakiti.egi.eu/). An alerting email will also be sent to EGI CSIRT if a critical vulnerability has been detected. Until 2012, Pakiti server has collected about 400,000 reports from 22,000 nodes of 335 production sites over 6 months period [45].

Moreover, Pakiti is enough to be integrated into an existing monitoring infrastructure. There are two ways from Pakiti server receive all information from clients. First is traditional way that the client sends the data directly to the server using HTTPS. Second is the client prints the data to its standard output, to let another monitoring tool such as Nagios [46] transfer the data to the server using another messaging mechanism.

4.3 Offline Patch Management

By now, there are many kinds of commercial or non-commercial software to manage patches on the market, however, most of them are focus on online system not offline system. Nuwa is researched in an offline manner.

4.3.1 Nuwa

American North Carolina State University and IBM have invented a new way to update system patches in cloud virtual machines even if those system programs are offline. The new patch management tool developed by them is called Nuwa [47]. It not only protects virtual machines from malicious attacks but also ensures these virtual machines always receive important security upgrades. Nuwa avoids the expensive virtual machines start and stop time, it ensures when a virtual machine image is ready to be started, it has the up-to-date patches installed. In addition, the researchers have determined that offline application of security patches is more than four times faster than online patch application. Current patch management systems are designed for computers that are online and they do not work for dormant computers. Nuwa is developed automatically analyzes the ‘script’ that dictates how a security patch is installed, and then automatically re-writes the script to make it compatible with an offline system.

Usually patch scripts are written in shell scripts. In fact, patching an offline virtual machine image, one thing needs to care about is the changes made to the file system in the virtual machine image. When presented with a patch, Nuwa first performs safety analysis on the patch scripts included in the original patch. If all scripts are safe, Nuwa utilizes simple emulation-based patch directly to perform offline patch. If some scripts are unsafe, Nuwa applies various rewriting techniques to these scripts, and performs safety analysis on the rewritten scripts. If these rewriting techniques can successfully convert the unsafe scripts to safe one, Nuwa will utilize simple emulation-based patch with the rewritten patch to finish offline patch. Emulation-based patch is to perform the file replacement actions from another host, referred to as the patch host. The patch host can mount and access an offline virtual machine images as a part of its own file system. Using the chroot [48] system call to change the root file system to the mount point, the patch host can emulate an environment required by the patch process on a running virtual machine and perform the file system actions originally developed for patching a running virtual machine. Therefore if some scripts are unsafe, Nuwa applies various rewriting techniques to successfully convert the unsafe scripts to safe ones. Figure 4-3 shows the rewriting techniques that Nuwa applies before executing each patch script. Rewriting a script can change the results of safety analysis, so Nuwa returns safety analysis after applying these techniques.

If safety analysis proves that all command lines in the script are safe, then the rewritten script is executed offline.   Otherwise, Nuwa resorts to online patch.

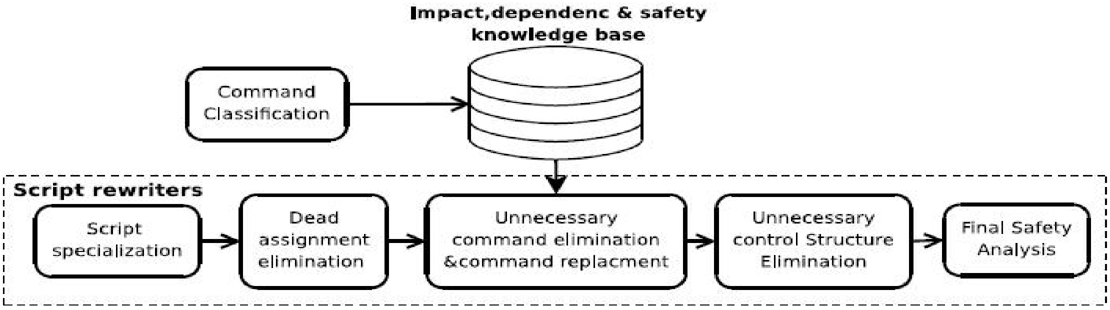

Impact,dependenc & safety knowledge base
Command Classification
Script rewriters
Script specialization
Dead assignment elimination
Unnecessary command elimination &command replacment
Unnecessary control Structure Elimination
Final Safety Analysis

Figure 4-3 Flow of script analysis and rewriting[47].

Nuwa utilizes and improves Mirage [30] techniques that developed by IBM, that is used for performing efficient offline introspection and manipulation of a large collection of virtual machine images, to allow cloud administrators to patch multiple virtual machines simultaneously.   A program already exists that allows cloud computing systems to operate more efficiently by saving one version of a computer file that is used by multiple virtual machines, rather than saving the same file repeatedly for each individual virtual machine. Nuwa takes advantage of this technology and, by patching one file, can ultimately protect all of the virtual machines that use that file.   Figure 4-4 shows the two phases of batch patch via Mirage.   Phase 1 performs the loop-invariant operation: Nuwa extracts the patch's files and imports them into Mirage.   The result is a list of content identifiers, one for each file.   In phase 2, Nuwa iterates over the images. For each image, Nuwa mounts the image with Vmount, rewrites and executes the pre-installation scripts, emulates the “unpack” step of the package manager (e.g., dpkg), using the Mirage file system attribute to set the contents of the patch’s files, rewrites and executes the post-installation scripts, and checks in the modified virtual machine image. If script rewriting ever fails to produce a safe script, then Nuwa resorts to online patch. North Carolina State University and IBM have successfully tested and evaluated Nuwa on the IBM Research Compute Cloud, a compute cloud that is used by IBM researchers worldwide.

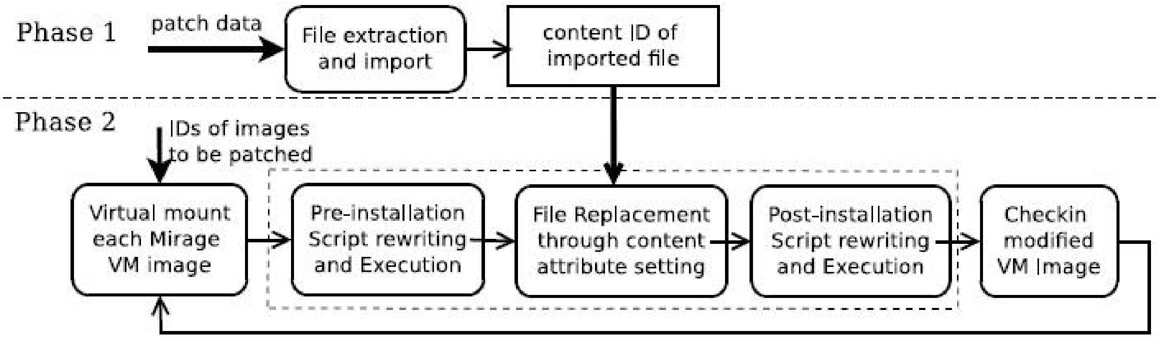

Phase 1
patch data
File extraction and import
content ID of imported file
Phase 2
IDs of images to be patched
Virtual mount each Mirage VM image
Pre-installation Script rewriting and Execution
File Replacement through content attribute setting
Post-installation Script rewriting and Execution
Checkin modified VM Image

Figure 4-4 Batch patch virtual machine images via Mirage[47].

As the result, Nuwa is a novel tool to enable efficient patch of offline virtual machine images. It uses safety analysis and script rewriting techniques to convert patches, or more specifically the installation scripts contained in patches, which were originally developed for online updating, into a form that can applied to virtual machine images offline. Its advantage will be useful to improve online or offline virtual machine image security patches.

4.4 Method: Patch Management in VMIC System

To be brief, Pakiti is an open source lightweight system that helps to monitor security patches status and informs authorized members to handle critical patches carefully. Nuwa is applied in checking security patches in dormant virtual machines. Those functionalities could make contribution on the existing VMIC system to improve its security mechanism.

According to previous VMIC introduction in 3-1, image administrators use VMIC or HEPiX tool to create image lists with updated images, before publishing those image lists, image administrator can use HEPiX tool to subscribe the image list and gets checksum to append the image file. Image information and metadata will be saved in OpenStack Glance and OpenStack Swift via Glance API. And Keystone will be used for the authentication of image administrators with Glance server. After that, users can search trusted images and list all available images with VMIC to download those images from current locations. The problem is that there is no security mechanism to help image administrators to check security patches of image files. Following this explanation, we expect to use patch management service to trace all virtual machines before image administrators subscribe the image list with HEPiX tool and publish with VMIC. In Figure 4-5 showed the ideal security patch management service in VMIC environment.

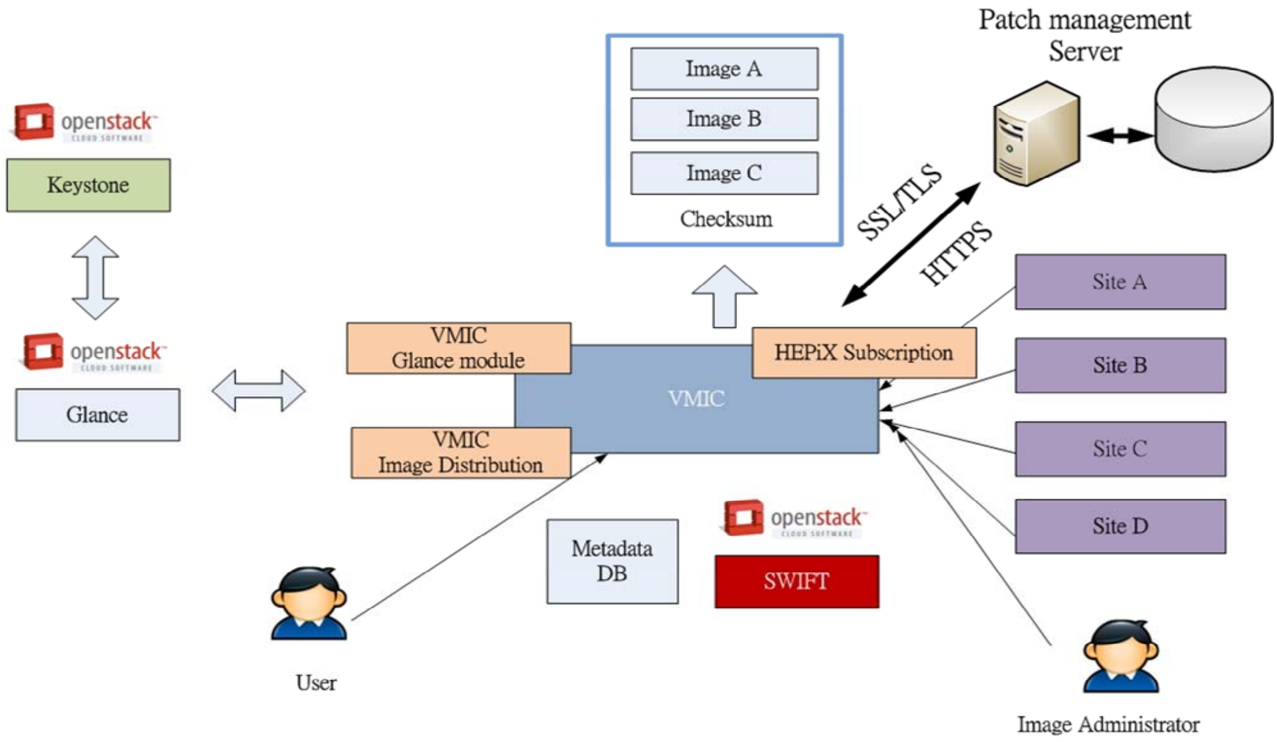


Figure 4-5 Patch management in VMIC system.

4.4.1 Pakiti in VMIC System

To evaluate the effect of the proposed approach, VMIC service and HEPiX virtualization working group tool are installed in one dedicated machine. Another standalone is for Pakiti server to monitor all virtual machine patches status. Pakiti client is installed in each virtual machine that will be subscribed by HEPiX virtualization working group tool and registered in VMIC.

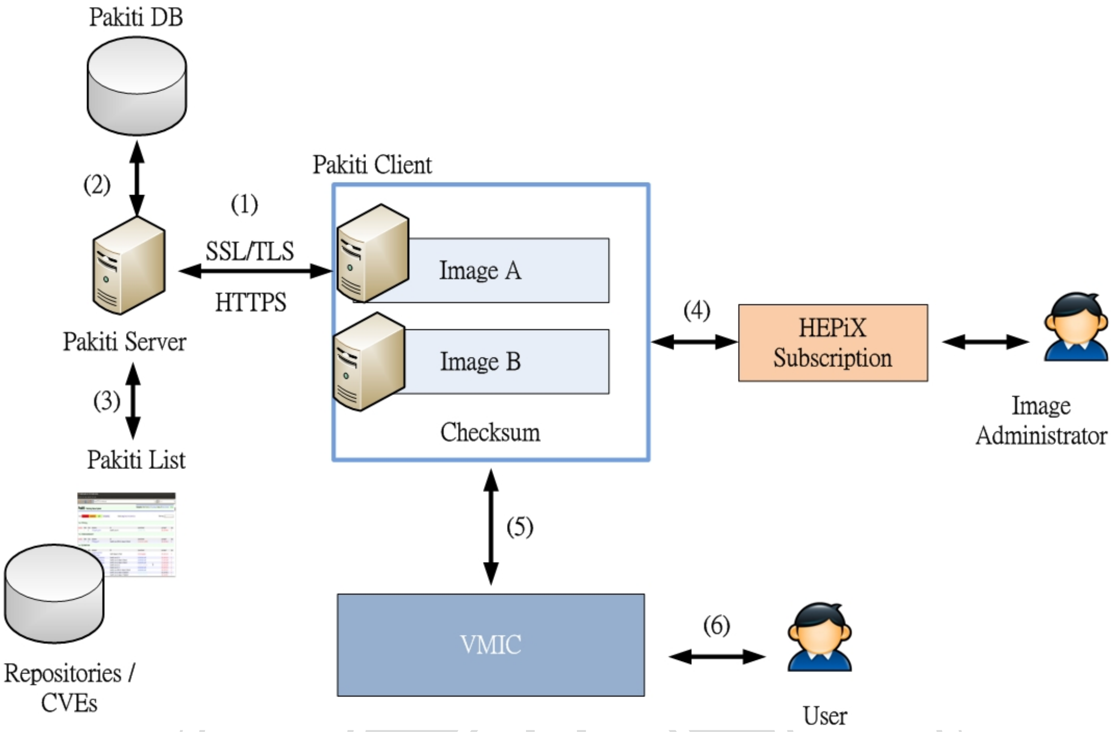


Figure 4-6 Pakiti Service in VMIC.

The procedure of this approach below in Figure 4-6:

(1) Each virtual machine installs Pakiti client on the host and it connects Pakiti server via SSL/TLS and HTTPS

(2) Pakiti server makes a patch status list every day from each Pakiti client, the current patch information is from CVEs and software's repositories

(3) Before Image administrators subscribe virtual machine images, each Pakiti client should transfer their patches information to Pakiti server to ensure security patches are up-to-date

(4) Image administrators use HEPiX virtualization working group tool to subscribe an image list

(5) Image information and metadata is stored with VMIC

(6) Users can choose and download safe virtual machine images from VMIC

4.4.2 Nuwa in VMIC System

In this approach, VMIC service and HEPiX virtualization working group tool are installed in one dedicated machine. Nuwa is installed in OpenStack File system to do safety analysis and script rewriting to check security patch status.

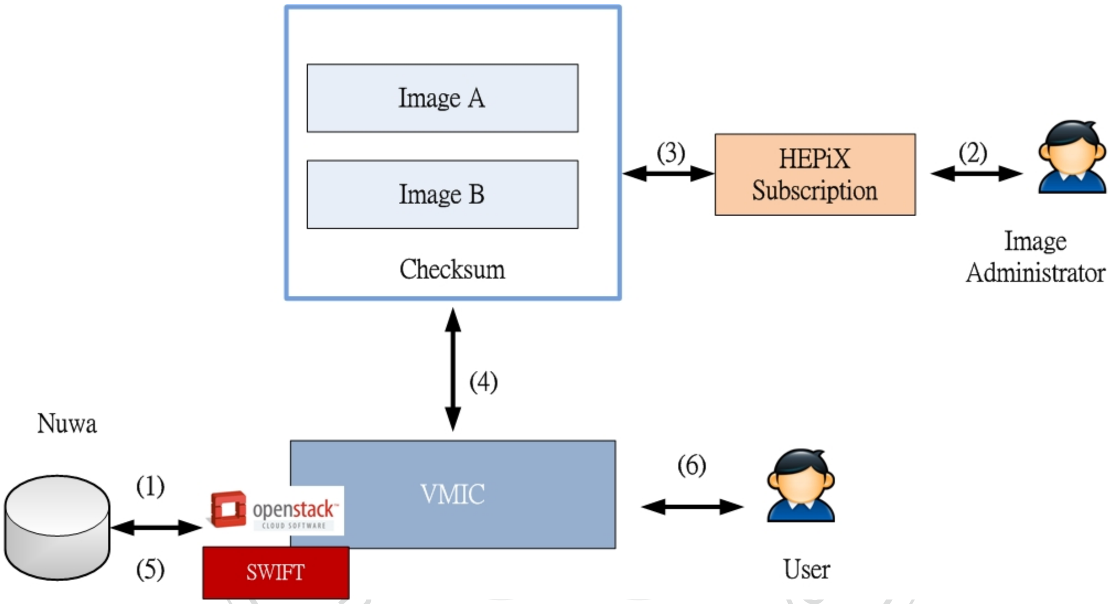


Figure 4-7 Nuwa Service in VMIC.

The procedure of this approach below in Figure 4-7:

(1) Nuwa is installed in OpenStack File system, for example: Swift

(2) Image administrators use HEPiX virtualization working group tool subscribe virtual machine images

(3) Image administrators use HEPiX tool to subscribe an image list

(4) Image information and metadata is registered and stored in File System of VMIC

(5) Nuwa will do safety analysis and script rewriting

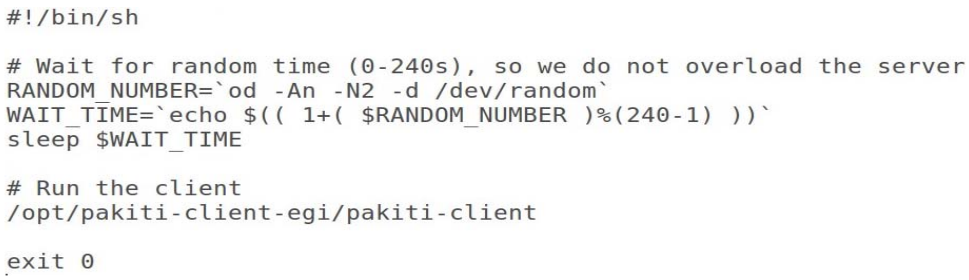
(6) Users can choose and download safe virtual machine images from VMIC

5 Implementation of VMIC Security Improvement

Patch management is assumed to improve current security environment in VMIC according to previous descriptions. Pakiti is an open source to download from its official website (http://pakiti.sourceforge.net/) freely. Nuwa is invented by American North Carolina State University and IBM, and is integrated with the Mirage image library, which stores identical files once and treats images as logical views on this collection of file. By now, Nuwa is applied in IBM Research Compute Cloud (RC2). Since Nuwa is a commercial tool that belongs to IBM, it is not an open source to retrieve resource or source code with ease. In this thesis, Nuwa will not be implemented without charge. In this implementation patch management will focus on Pakiti application. EGI CSIRT is utilized by Pakiti server and the client program is running at local clients. When client scripts run regularly, the total reports will be shown on EGI Pakiti server which is authenticated by HTTPS. The version 3.0 of EGI CSIRT Pakiti server is chosen to design for the environments with the 10.000+ hosts and should provides capabilities to be easily integrated into the existing monitoring infrastructures.

5.1 Pakiti Client

Pakiti Client runs a simple script as a cron job every day; the Pakiti client software can be downloaded from EGI CSIRT websites and the parameters are modified to fit for this implementation. When unpacking downloaded client software, there are two directories, etc and opt in current path. The primary Pakiti client script is in opt directory and the client cron script is in etc. The client cron script (Figure 5-1) is stored in /etc/cron.daily and Pakiti client will be lunched every day.

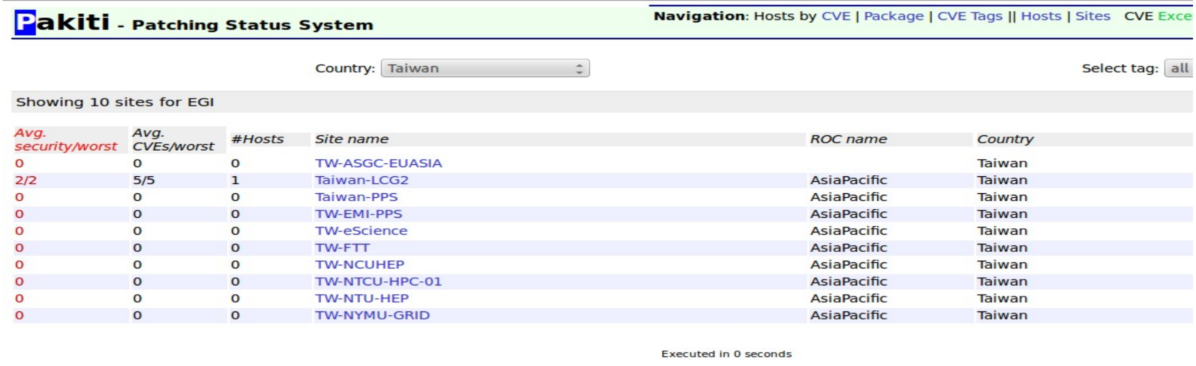


```
#!/bin/sh

# Wait for random time (0-240s), so we do not overload the server
RANDOM_NUMBER=`od -An -N2 -d /dev/random`
WAIT_TIME=`echo $(( 1+( $RANDOM_NUMBER )%(240-1) ))`
sleep $WAIT_TIME

# Run the client
/opt/pakiti-client-egi/pakiti-client

exit 0
```

Figure 5-1 The Pakiti client cron script.

5.2 Pakiti Server

Since the EGI CSIRT Pakiti server is authenticated by HTTPS, so personal certificates should be imported to the browser in advance and the Distinguished Name (DN) is registered to Access Control List (ACL) on EGI CSIRT Pakiti server. The user have to login by personal certificate such as "C=TW/ O=AS/ OU=GRID/ CN=Chen Yi Chien 124172" for access control of the Pakiti server. After accessing the main page, hosts can be searched by different classifications on the top toolbar. Hosts are searched by sites and the country as Taiwan is chosen with the pull-down menus. The web page lists all current site names that register country information as Taiwan (See Figure 5-2). If the security patches are out-of-date, the warning information in red will be displayed to remind security staffs. Only vulnerable hosts will be shown on this list not all hosts. It helps security staffs to point out problem immediately.



Pakiti - Patching Status System
Navigation: Hosts by CVE | Package | CVE Tags || Hosts | Sites CVE Exce

Country: Taiwan

Select tag: all

Showing 10 sites for EGI

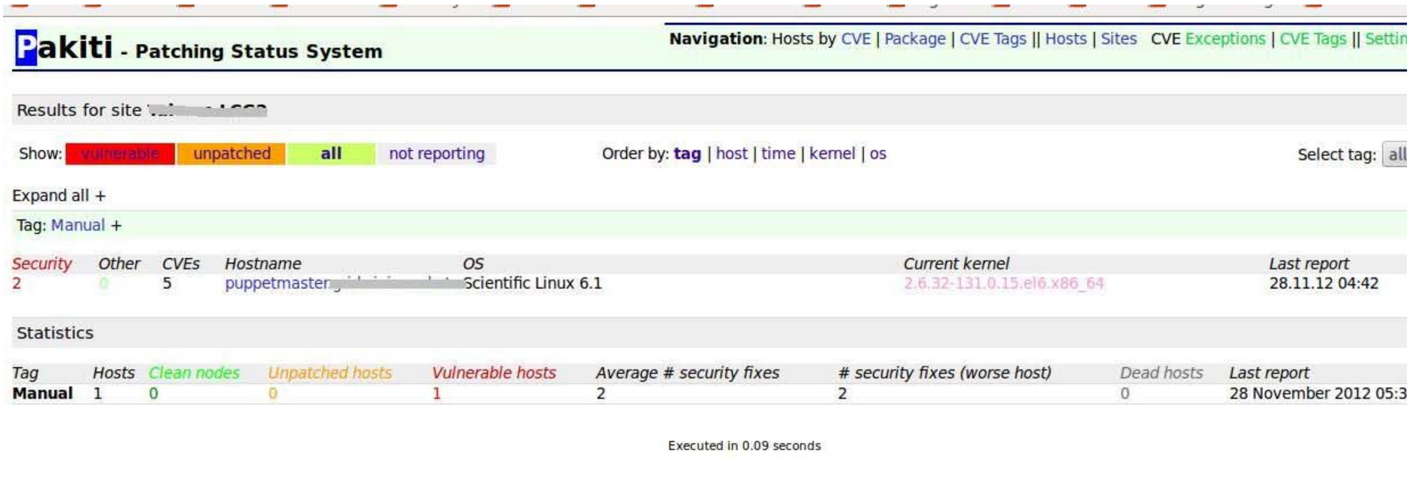
Avg. security/worst	Avg. CVEs/worst	#Hosts	Site name	ROC name	Country
0	0	0	TW-ASGC-EUASIA		Taiwan
2/2	5/5	1	Taiwan-LCG2	AsiaPacific	Taiwan
0	0	0	Taiwan-PPS	AsiaPacific	Taiwan
0	0	0	TW-EMI-PPS	AsiaPacific	Taiwan
0	0	0	TW-eScience	AsiaPacific	Taiwan
0	0	0	TW-FTT	AsiaPacific	Taiwan
0	0	0	TW-NCUHEP	AsiaPacific	Taiwan
0	0	0	TW-NTCU-HPC-01	AsiaPacific	Taiwan
0	0	0	TW-NTU-HEP	AsiaPacific	Taiwan
0	0	0	TW-NYMU-GRID	AsiaPacific	Taiwan

Executed in 0 seconds

Figure 5-2 Hosts list on Pakiti server and this list sorts hosts by country.

For more details of the vulnerable site, click on the site name. In Figure 5-3, puppetmaster is the hostname which has 2 security vulnerabilities and 5 related CVE events. Clicking the hostname to access security patch warning in Figure 5-4, there are all CVE numbers of this vulnerable hostname and all warning security packages need to be updated. In this case, there are five CVE numbers (2010-2761, 2010-4410, 2011-1487, 2011-2939 and 2011-3597) affected by puppetmaster host. These security patches are shown in the left since many Perl packages need to be updated. CVE-2010-2761 is clicked to get the package names and versions in Figure 5-5.

The Pakiti server is user-friendly to provide the URL for security staffs to connect the official CVE website to search solutions. For example, when CVE-2010-2761 in bold URL on the top is clicked; this main page will connect to Red Hat official website. In Figure 5-6, CVE-2010-2761 and CVE 2010-4410 indicate some related Perl packages on our host machine for update. This page provides bug information and useful RPM to download for updating.



Pakiti - Patching Status System

Navigation: Hosts by CVE | Package | CVE Tags || Hosts | Sites CVE Exceptions | CVE Tags || Settin

Results for site [redacted]

Show: vulnerable unpatched all not reporting

Order by: tag | host | time | kernel | os

Select tag: all

Expand all +

Tag: Manual +

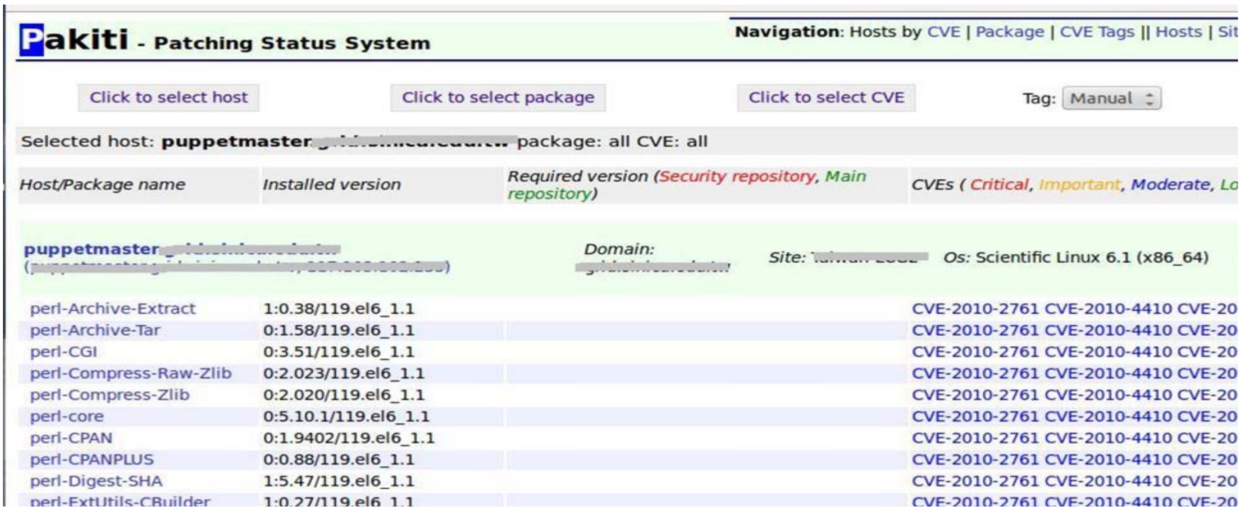
Security	Other	CVEs	Hostname	OS	Current kernel	Last report
2	0	5	puppetmaster[redacted]	Scientific Linux 6.1	2.6.32-131.0.15.el6.x86_64	28.11.12 04:42

Statistics

Tag	Hosts	Clean nodes	Unpatched hosts	Vulnerable hosts	Average # security fixes	# security fixes (worse host)	Dead hosts	Last report
Manual	1	0	0	1	2	2	0	28 November 2012 05:3

Executed in 0.09 seconds

Figure 5-3 security events and CVEs statistics.



Pakiti - Patching Status System

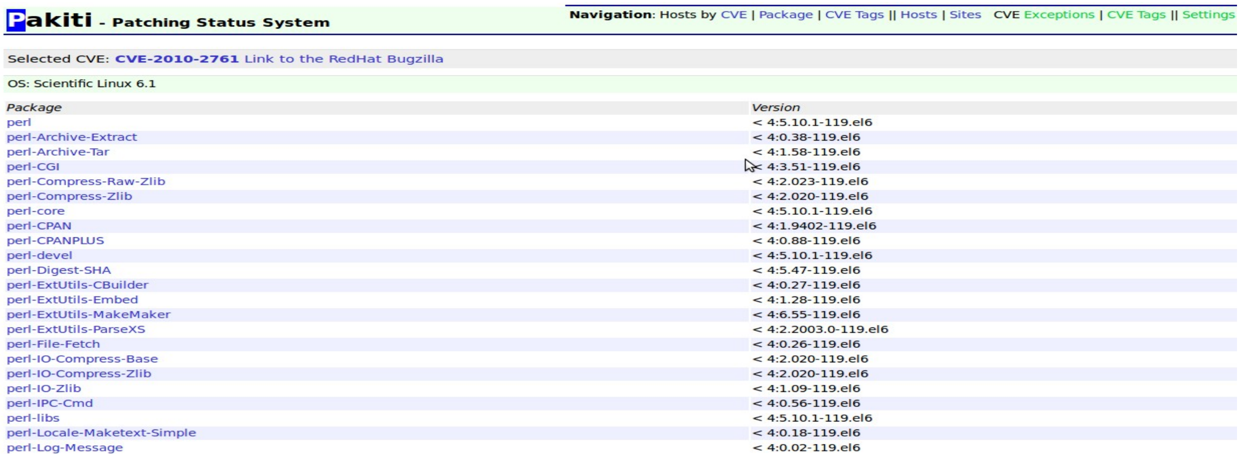
Navigation: Hosts by CVE | Package | CVE Tags || Hosts | Sit

Click to select host   Click to select package   Click to select CVE   Tag: Manual

Selected host: **puppetmaster**[redacted] package: all CVE: all

Host/Package name	*Installed version*	*Required version (Security repository, Main repository)*	*CVEs (Critical, Important, Moderate, Lo*
puppetmaster[redacted] ([redacted])	*Domain:* [redacted]	*Site:* [redacted]	*Os:* Scientific Linux 6.1 (x86_64)
perl-Archive-Extract	1:0.38/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-Archive-Tar	0:1.58/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-CGI	0:3.51/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-Compress-Raw-Zlib	0:2.023/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-Compress-Zlib	0:2.020/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-core	0:5.10.1/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-CPAN	0:1.9402/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-CPANPLUS	0:0.88/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-Digest-SHA	1:5.47/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20
perl-ExtUtils-CBuilder	1:0.27/119.el6_1.1		CVE-2010-2761 CVE-2010-4410 CVE-20

Figure 5-4 all vulnerable CVEs on puppetmaster host.



Pakiti - Patching Status System

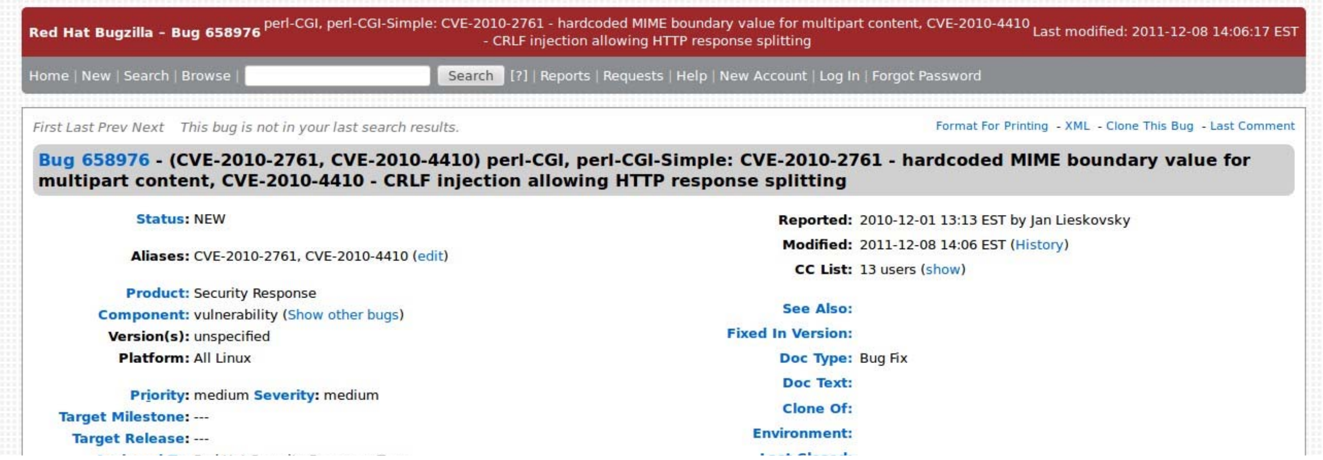
Navigation: Hosts by CVE | Package | CVE Tags || Hosts | Sites   CVE Exceptions | CVE Tags || Settings

Selected CVE: **CVE-2010-2761** Link to the RedHat Bugzilla

OS: Scientific Linux 6.1

Package	*Version*
perl	< 4:5.10.1-119.el6
perl-Archive-Extract	< 4:0.38-119.el6
perl-Archive-Tar	< 4:1.58-119.el6
perl-CGI	< 4:3.51-119.el6
perl-Compress-Raw-Zlib	< 4:2.023-119.el6
perl-Compress-Zlib	< 4:2.020-119.el6
perl-core	< 4:5.10.1-119.el6
perl-CPAN	< 4:1.9402-119.el6
perl-CPANPLUS	< 4:0.88-119.el6
perl-devel	< 4:5.10.1-119.el6
perl-Digest-SHA	< 4:5.47-119.el6
perl-ExtUtils-CBuilder	< 4:0.27-119.el6
perl-ExtUtils-Embed	< 4:1.28-119.el6
perl-ExtUtils-MakeMaker	< 4:6.55-119.el6
perl-ExtUtils-ParseXS	< 4:2.2003.0-119.el6
perl-File-Fetch	< 4:0.26-119.el6
perl-IO-Compress-Base	< 4:2.020-119.el6
perl-IO-Compress-Zlib	< 4:2.020-119.el6
perl-IO-Zlib	< 4:1.09-119.el6
perl-IPC-Cmd	< 4:0.56-119.el6
perl-libs	< 4:5.10.1-119.el6
perl-Locale-Maketext-Simple	< 4:0.18-119.el6
perl-Log-Message	< 4:0.02-119.el6

Figure 5-5 package names and version of CVE-2010-2761.



Red Hat Bugzilla – Bug 658976 perl-CGI, perl-CGI-Simple: CVE-2010-2761 - hardcoded MIME boundary value for multipart content, CVE-2010-4410 - CRLF injection allowing HTTP response splitting   Last modified: 2011-12-08 14:06:17 EST

Home | New | Search | Browse | Search [?] | Reports | Requests | Help | New Account | Log In | Forgot Password

First Last Prev Next   This bug is not in your last search results.   Format For Printing - XML - Clone This Bug - Last Comment

Bug 658976 - (CVE-2010-2761, CVE-2010-4410) perl-CGI, perl-CGI-Simple: CVE-2010-2761 - hardcoded MIME boundary value for multipart content, CVE-2010-4410 - CRLF injection allowing HTTP response splitting

Status: NEW

Aliases: CVE-2010-2761, CVE-2010-4410 (edit)

Product: Security Response
Component: vulnerability (Show other bugs)
Version(s): unspecified
Platform: All Linux

Priority: medium **Severity:** medium
Target Milestone: ---
Target Release: ---

Reported: 2010-12-01 13:13 EST by Jan Lieskovsky
Modified: 2011-12-08 14:06 EST (History)
CC List: 13 users (show)

See Also:
Fixed In Version:
Doc Type: Bug Fix
Doc Text:
Clone Of:
Environment:

Figure 5-6 CVE-2010-2761 and 2010-4410 on Red Hat.

In above case, Pakiti client software is installed on a local host (puppetmaster) and EGI CSIRT Pakiti server monitors vulnerable sites. For this experiment, no security patch is updated in advance, so security patches on puppetmaster should be out-of-date. When Pakiti server collects client information and publishes on its website, puppetmaster is displayed on the list and the server provides some details of CVEs for finding solutions to fix these security patches problem.

In conclusion, Pakiti provides a solution to keep security patches up-to-date; as a result, Pakiti clients should be installed in physical machines or virtual machines when those machines register in VMIC system. This improvement facilitates machines to receive the latest patches in VMIC. So before users download virtual machine images from VMIC, Pakiti server has been monitored security patches and reported to security staffs in advance, to guarantee virtual machines images in VMIC are safe.

6 Future Work

The purpose of this research expresses Pakiti improves security in VMIC because of security patches monitoring. However, not all physical or virtual machines have been in a running state, security staffs should be pay much attention to those dormant machines

In order to ensure all virtual machines images to defend all attacks, Pakiti should be applied to monitor the states of dormant machines such as Nuwa. Nuwa is different than Pakiti server to check security patches during registering to VMIC. When images and image lists are subscribed by HEPiX tool and registered to VMIC, all image files are stored in VMIC file system. After that, Nuwa will do the safety analysis and script rewriting in VMIC file system (OpenStack Swift), Nuwa is valuable to trace those offline virtual machine images and update their security patches in time. As the result, Nuwa not only examines online virtual machines but also offline virtual machines in current VMIC environment. On the other hand, a friendly web interface for VMIC is needed, not only users but also image administrators can search or manage virtual machines via this web interface.

There are some enhancements for VMIC in progress. OpenStack has its specific dashboard (Horizon) [49] to connect all OpenStack components via API. VMIC could integrate with OpenStack dashboard in web services based system, and provides identity management services to protect user accounts and passwords are required for authentication and authorization [50] [51] [52]. Or it is better to provide one-time password authentication which utilizes dynamic password facilitates to enhance the security of password [53]. When VMIC web interface provides an entrance with user accounts and passwords, secure password recovery is valuable and essential for VMIC to protect user's sensitive information or avoid malicious attackers [54] [55] [56].

In the future, security staffs must strengthen its security in offline patch management, identity management and password recovery schemes in VMIC.

7 Conclusion

This paper has investigated the security improvement of current VMIC system to strengthen its patch management and monitoring to avoid malicious attacks. Pakiti collected patch reports from its clients and published via web pages. As a result, security staffs could control all virtual machines' patch status timely and updated them. According to the result, Pakiti was able to monitor plenty of machines effectively but did not increase servers' overloading. In addition, Pakiti is an open source for customization to apply in customers' current environments. However, VMIC has already improved partial security functions; it still has some security subjects needed further researches, for instance, offline patch management, identity management and password recovery schemes. The future researches will be focused on these security improvements.

8 Reference

[1] Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing.

[2] M. Armbrust, A. Fox, R. Griffith, and et al. 2009. Above the Clouds: A Berkeley View of Cloud Computing. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[3] I. Foster, Y. Zhao, I. Raicu, S. Lu. 2008. Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environment Workshop.*

[4] P. Mell, T. Grance. 2011. Effectively and Security Using the Cloud Computing Paradigm. The National Institute of Standards and Technology.

[5] Cloud computing security.http://en.wikipedia.org/wiki/Cloud_computing_security.

[6] Virtualization . http://en.wikipedia.org/wiki/Virtualization.

[7] 陳瀅(2010)。*雲端策略*。 台北：天下。

[8] Gerald J. Popek. 1974. Formal Requirements for Virtualizable Third Generation Architectures. *Magazine Communications of the ACM Volume 17 Issue 7, Pages 412-421.*

[9] Virtual Machine. http://en.wikipedia.org/wiki/Virtual_machine.

[10] KVM. http://www.linux-kvm.org/page/Main_Page.

[11] Kernel based Virtual Machine. http://en.wikipedia.org/wiki/Kernel-based_Virtual_Machine.

[12] Oracle VM VirtualBox. https://www.virtualbox.org/.

[13] Oracle VM VirtualBox. http://en.wikipedia.org/wiki/VirtualBox.

[14] VMWare. http://www.vmware.com/.

[15] VMWare. http://en.wikipedia.org/wiki/VMware.

[16] Xen. http://en.wikipedia.org/wiki/Xen.

[17] XEN. http://www.xen.org/.

[18] R. Wartel, T. Cass, B. Moreira, E. Roche, M. Guijarro, S. Goasguen, U. Schwickerath. 2009. Image Distribution Mechanisms in Large Scale Cloud Providers. *2nd IEEE International Conference on Cloud Computing Technology and Science.*

[19] Academia Sinica Grid Center (ASGC). http://www.twgrid.org/en/.

[20] Distributed Cloud of ASGC. 2012. *The International Symposium on Grid Computing.*

[21] The High Energy Physics Unix Information Exchange. https://www.hepix.org/.

[22] The HEPiX Virtualisation Working Group. http://w3.hepix.org/virtualization/.

[23] StratusLab. http://stratuslab.eu/doku.php/start.

[24] M. Vlieta , A. Agarwala , M. Andersona , P. Armstronga , A. Charbonneaub , K. Franshama b , I. Gablea , D. Harrisa , R. Impeyb , C. Leavett-Browna , M. Patersona , W.

Podaimab , R.J. Sobiea. 2011. Repoman: A Simple RESTful X.509 Virtual MAchine Image Repository. *International Symposium on Grid and Clouds and Open Grid Forum 31.*

[25] EGI European Grid Infrastructure. http://www.egi.eu/.

[26] EGI Strategy and Policy. http://www.egi.eu/about/policy/index.html.

[27] Security Policy For The Endorsement and Operation of Virtual Machine Images. https://documents.egi.eu/document/771.

[28] L. Zhang, D. Zhang et al., 2010. Live Digital Forensics in a Virtual Machine. *International Conference on Computer Application and System Modeling.*

[29] HEPiX Virtualsation Working Group report.

[30] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning. 2009. Managing Security of Virtual Machine Images in a Cloud Environment. *CCSW.*

[31] Wayne A. Jansen, NIST. 2011. Cloud Hooks: Security and Privacy Issues in Cloud Computing. *The 44th Hawaii International Conference on System Sciences.*

[32] Scientific Linux CERN6. http://linux.web.cern.ch/linux/scientific6/.

[33] OpenStack. http://www.openstack.org/.

[34] U. Schwickerath, B. Moreira, J. Chien, V. Sharma. 2011. CloudMan and VMIC projects overview. *HEPiX Fall.*

[35] DESY. http://www.desy.de/index_eng.html.

[36] BitTorrent. http://en.wikipedia.org/wiki/BitTorrent.

[37] Keystone. http://docs.openstack.org/developer/keystone/.

[38] D. Hyde. 2009. A Survey on the Security of Virtual Machines.

[39] Patch (computing). http://en.wikipedia.org/wiki/Patch_(computing).

[40] M. Prochazka, D. Kouril, R. Wartel, C. Kanellopoulos, C. Triantafyllidis. 2011. A Race for Security: Identifying Vulnerabilities on 50 000 Hosts Faster than Attackers, in Proceedings of Science (PoS). *International Symposium on Grid and Clouds.*

[41] Pakiti. http://pakiti.sourceforge.net/.

[42] The MITRE Corporation, "Open Vulnerability and Assessment Language". http://oval.mitre.org/language/.

[43] MITRE. http://www.mitre.org/.

[44] Common Vulnerabilities and Exposures , CVE. http://cve.mitre.org/.

[45] M. Ma, M. Prochazka, D. Kouril et al. 2012. EGI Security Monitoring, in Proceedings of Science (PoS). *International Symposium on Grid and Clouds.*

[46] Nagios. http://www.nagios.org/.

[47] W. Zhou, P. Ning, X. Zhang et al. 2010. Always Up-to-date-Scalable Offline Patch of VM Images in a Compute Cloud. *ACSAC.*

[48] Chroot. http://en.wikipedia.org/wiki/Chroot.

[49] Horizon. http://docs.openstack.org/developer/horizon/.

[50] B.Ross, C. Jackson et al. 2005. Stronger Password Authentication Using browser extensions.

[51] A. Choudhury, P. Kumar et al. 2011. A Strong User Authentication Framework for Cloud Computing. *IEEE Asia-Pacific Services Computing Conference.*

[52] R. Warschofsky, M. Menzel, C. Meinel. 2011. Automated Security Service Orchestration for the Identity Management in Web Service based Systems. *IEEE Asia-Pacific Services Computing Conference.*

[53] S. Luo, J. Hu and Z. Chen. 2009. An Identity-Based One-Time Password Scheme with Anonymous Authentication. *International Conference on Networks Security, Wireless Communications and Trusted Computing.*

[54] L. Jin, H. Takabi, J. Joshi . 2010. Security and Privacy Risks of Using E-mail Address as an Identity pp.906-913. *IEEE International Conference on Social Computing*.

[55] Reeder, R.W. 2011. When the Password Doesn't Work Secondary Authentication for Websites Volume: 9, Issue: 2, Page43- 49. *The IEEE Computer and Reliability Societies.*

[56] S. Schechter, S.Egelman, R. Reeder. 2009. It's Not What You Know, But Who You Know - A social approach to last-resort authentication, *CHI.*