

# Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud

Ramaswamy Chandramouli

*Computer Security Division, Information Technology Laboratory*

*National Institute of Standards & Technology*

*Gaithersburg MD 20899, USA*

[mouli@nist.gov](mailto:mouli@nist.gov)

**Abstract:** Infrastructure as a Service (IaaS) is one of the three main cloud service types where the cloud consumer consumes a great variety of resources such as computing (Virtual Machines or VMs), virtual network, storage and utility programs (DBMS). Any large-scale offering of this service is feasible only through a virtualized infrastructure at the service provider. At the minimum, this infrastructure is made up of resources such as Virtualized hosts together with associated virtual network and hardware/software for data storage. An IaaS's consumer's total set of interactions with these resources constitute the set of use cases for IaaS cloud service. These use cases have associated security requirements and these requirements are met by protection options enabled by available security solutions/technologies. The purpose of this paper is to analyze these protection options from the viewpoint of: (a) Security functionality they can provide and (b) the architecture that governs their deployment, so that IaaS consumers can decide on the most appropriate security configuration for their VM instances depending upon the profile of the applications running in them.

**Keywords-***Virtualization; Cloud Infrastructure; Virtual Machine; Virtual Network; Infrastructure as a Service*

## I. INTRODUCTION

Infrastructure as a Service (IaaS) is one of the three main cloud service types where the cloud consumer consumes a great variety of resources such as computing (Virtual Machines or VMs), virtual network, storage and utility programs (DBMS). Any large-scale offering of this service is feasible only through a virtualized infrastructure at the IaaS cloud service provider. At the minimum, this infrastructure is made up of resources such as Virtualized hosts together with associated virtual network and hardware/software for data storage. The IaaS consumer's different interactions with these resources constitute the typical set of use cases for the IaaS cloud service. In order that these interactions are secure, certain security requirements should go with each use case.

With increasing demand for IaaS cloud service and competitive nature of the market place, cloud providers and

third parties are offering many security solutions. Depending upon the functionality and architecture of these security solutions, they can either be deployed by IaaS cloud consumer (e.g., VM-based Anti-Virus software) or only by IaaS cloud provider (e.g., Hypervisor-based firewall). Also given the varied feature set and the deployment architecture of these security solutions (let us call them as protection options in the rest of this paper), we need an objective way of correlating their security functionality (features) with the security requirements of use cases and determine as to how effectively they (protection options or security solutions) address those security requirements. In other words, we need a methodology for performing analysis of the available protection options in the context of the security requirements stemming from a typical set of IaaS cloud service use cases. This is the objective of this paper.

The first step of the methodology therefore, is to identify the typical set of use cases encountered by IaaS cloud consumer. Those that we consider in this paper are: (a) Checking out VM Images, (b) Configuring VM instance OS (Guest OS), (c) Configuring Virus/Malware protection for VM instance, (d) Configuring VM instance access protection, (e) Configuring VM instance lifecycle operation protection, (f) Configuring VM instance isolation and (g) Comprehensive Data protection in IaaS cloud service. For each use case, we consider the security requirements and then analyze the features/capabilities of the available protection options (provided either by IaaS cloud provider as an integral part of the service or COTS solutions deployable by IaaS cloud consumer) to meet those requirements. The rest of the paper is organized as follows: Each of the Sections II through VIII provide a brief description of the use case, the security requirements for each use case and an analysis of protection options that are enabled by available security solutions/technologies. The Conclusions & Benefits section summarizes the protection options and findings resulting from analysis for each use and also outlines the benefits of our approach.

## II. CHECKING OUT VM IMAGES

VM images launched on a virtualized host become running VM instances. Each VM image is a self-contained package that contains all constituents needed for running a complete computing stack such as: (a) OS binaries together with other files in the OS distribution as well as patches and, (b) files containing description of all virtual resources that make up a VM – starting from processor cores, memory size, virtual disks or data stores etc. Thus we see that VM images are a set of files which are stored as data and this data forms the foundation for the security profile of production VM instances launched from them. Any VM instance with unsafe security profile can result in jeopardizing the integrity of applications hosted on that VM instance and in some cases may endanger the integrity of other VM instances on the virtualized host. Hence, at the minimum, VM images have the following security requirements:

- Integrity Protection (VM Images can be created/modified only by authorized administrators and its contents should carry this seal of integrity)
- Authorized use (limiting the administrators who are allowed to check out images from the Image repository and launch VM instances. This is to prevent a phenomenon known as “VM Sprawl” which may result in proliferation of unauthorized VM instances.

The protection options that can cover the above requirements are [1]:

- The integrity of the VM images can be protected using checksums or digital signatures.
- There should be a specific name space definition associated with names that are given for VM images – as giving arbitrary names may result in uncontrolled VM images sprawl.
- The VM configuration information in VM images should conform to the “Enterprise VM Gold Standard” in terms of OS Distribution Version/Patch # as well as the amount of virtual resources allocated.
- The file containing metadata information about VM images should be logically separate from VM Images themselves and access to both of them subject to access control.

The above protection options can be realized through COTS crypto modules and Configuration Management Tools. The integrity protection option has to be implemented by the stakeholder who created the VM image repository (IaaS cloud provider or IaaS cloud consumer)

while authorized use of VM images for launching has to be implemented by IaaS cloud consumer.

## III. CONFIGURING VM INSTANCE OS (GUEST OS)

Securing the OS installed in the leased VM instance (Guest OS) is the first security task of the IaaS cloud consumer. The minimal set of security requirements for this task is:

- The OS modules configured should result in a hardened installation – one that contains the minimal modules from the OS distribution [1] that will provide the functionality for the purpose for which the VM instance is going to be deployed.
- It should contain the latest version of the OS distribution as well as the latest patches.

The protection options available to IaaS cloud consumers for meeting the above requirements are straightforward: (a) Verify whether any of the pre-defined VM images offered by the IaaS cloud provider meets the above security requirements or build their own VM image meeting the above requirements and (b) deploy only those compliant VM images as their VM instances in the cloud provider infrastructure. Being an automated verification process, these options require no further analysis.

## IV. CONFIGURING VIRUS/MALWARE PROTECTION FOR VM INSTANCE

Before loading them with applications, VM instances need to be secured with an anti-malware/ anti-virus engine as application execution involves lots of file activity. The security functions expected of these engines are [2]: Monitor file events (e.g., downloads and modifications), periodically scan files resident on the VM, detect viruses and malware using the set of signature files and perform the necessary remediation and/or generate alerts. Remediation may take the form of either deleting or quarantining the malicious files. These requirements can be met using one of the following protection options [2]:

- Run an Anti-virus engine on each VM instance
- Run an anti-virus engine as a virtual security appliance (VSA) in a specially hardened security VM that uses the hypervisor introspection API to scan and monitor file-level events in all VM instances in that virtualized host

Obviously the second option holds more advantages than the first because:

- It consumes less resources overall compared to a in-VM solution

- Easier maintenance due to a single copy of anti-virus engine and signature files running in a VSA on a hardened VM
- Uniform application of policies across a set of VM instances since policies are specified centrally at one location
- Ability to add sophisticated logging (generating logs conforming to a standard syslog format) and auditing capabilities since the anti-virus engine is not running in a production VM instance and hence not likely to hog the resources and affect application performance.

However, running an anti-virus engine as an appliance can only be done by IaaS cloud provider as it uses the introspection API of the hypervisor to which individual IaaS cloud consumers cannot be provided access. At the same time, an IaaS cloud consumer cannot hand over the task of providing anti-virus, anti-malware protection through a VSA to the IaaS cloud provider as the latter will gain visibility into all files belonging to the former, thus potentially compromising the confidentiality of enterprise assets.

## V. CONFIGURING VM INSTANCE ACCESS PROTECTION

The first security requirement for any server after loading and configuring application is access protection and the VM instance (virtual server) is no exception to this. VM instance access protection requirements can be met through following protection options:

- Establishing a secure session using a secure access protocol such as SSHv2 or TLS/SSL.
- Access to VM instances using multi factor authentication with one of the authentication factors being “what you have” type consisting of a public key certificate [3]
- Enabling privileged access (e.g., using SSH) to VM instances only from IaaS cloud consumer’s corporate network (e.g., specifying the sub network from which SSH access (using port 22) is possible)

The criteria to look for in the above protection options are: (a) Strength of cryptographic keys supported in SSH & TLS solutions and (b) the entropy of authentication secrets.

## VI. CONFIGURING VM INSTANCE LIFECYCLE OPERATION PROTECTION

One of the core class of functions that administrative users of IaaS cloud consumer perform is Lifecycle operations on their VM instances – Start (Launch),

Suspend and Stop (Terminate). These operations are performed using API calls to the hypervisor management interface. The security requirements for these operations are:

- Ability to restrict the set of administrators who can make these API calls
- Sending the API calls with integrity and in some certain instances in a confidential way

The protection options for meeting these requirements and an analysis of implementation issues are given below:

Restricting the set of API calls a particular IaaS cloud consumer user can invoke can be enforced using conventional access control mechanisms. Very often the Identity & Access Management system provides the ability to create groups or roles to which a set of allowable API calls can be assigned. By assigning an individual IaaS cloud (administrative) consumer to one or more of these groups or roles, that individual’s access rights can be restricted only to the set of permissions assigned to those groups or roles. Further API calls are protected by channeling them through a dedicated management network that is isolated from the network that carries the traffic for applications running on VM instances.

To ensure that lifecycle operations on VM instances have originated from the authorized IaaS cloud (administrative) consumer user and have not been tampered with, while being submitted across the network, commercial IaaS cloud services require that API calls to perform those operations are digitally signed and the interfaces are on a dedicated management network [3]. To obtain this capability, an IaaS cloud (administrative) consumer user has to generate a private cryptographic key and have the corresponding public key vouched for through a Certificate issued by a trusted Certificate Authority (CA). In addition if the IaaS cloud (administrative) consumer user wants to send the API calls with confidentiality protection, he/she has to establish a SSL session with management interface provided by the IaaS cloud provider.

## VII. CONFIGURING VM INSTANCE ISOLATION

The business value for IaaS consumers to lease VM instances from an IaaS cloud provider comes from the ability to architect a multi-tier enterprise application by leasing multiple VM instances. To protect these applications running on different VM instances, IaaS consumers need to have mechanisms for isolating VM instances based on the type of application/application-tier hosted on them. This isolation requirement can be met by

the following protection options. A detailed analysis of these protection options follow:

- Isolation through Firewall Configurations
- Isolation using VLAN ID/Portgroup

#### *A. Isolation through Firewall Configurations*

Firewalling functions perform monitoring and place restrictions on both inbound and outbound traffic to and from specific VM instances. The argument for placing restrictions on outbound traffic is that if a VM instance belonging to a consumer is compromised, it could be used as a launching pad to attack other VM instances belonging to the same IaaS cloud consumer because of pre-established connections of a multi-tier application.

There are two firewalling architectural options:

- Firewall based at the Virtual Network layer
- Firewall housed on VM instance

Firewalls implemented at the Virtual Network layer restrict inbound and outbound traffic to and from targeted VM instances and have the following architecture & features:

- They generally consists of two components [4]: (a) A Hypervisor kernel module that forwards all or selected (based on a set of rules) packets coming into a virtual network card (vNIC) of every VM in a virtualized host to a firewall that is run as a VSA and (b) A firewall that is run as VSA on a specially-hardened VM instance that receives packets received from the hypervisor kernel module and enforces traffic restrictions (allow or restrict). These restrictions are enforced based upon traffic filtering rules centrally defined on a virtual infrastructure management server and pushed into this VSA running on each virtualized host.
- They make use of VMI (Virtual Machine Introspection) capability of the hypervisor to gain invisibility into the network traffic flowing in and out of VM instances and reside between the physical network interface of the virtualized host and the vNICs of VM instances
- Traffic restriction policies can be enforced at the following level of granularity: (a) Based on TCP 5-tuple (Source IP, Destination IP, Source Port, Destination Port, Protocol type (e.g., TCP/UDP), (b) Application Ports & (c) Administrator-defined Security Groups (Cluster (a group of virtualized hosts), Resource pool (group of VMs) and Port Group/VLAN

(that can be defined at the level of virtual switches within a virtualized host))

Since in a given virtualized host, VM instances belonging to multiple tenants (consumers) run in a typical IaaS cloud service, the virtual network configuration has to be under the control of IaaS cloud provider and hence a virtual network-based firewall can only be installed and run by the IaaS cloud provider. However the cloud provider can provide the capability for selective administration of this firewall to cloud consumers to specify firewall traffic rules pertaining to their own VM instances in that cloud service.

A typical scenario for IaaS cloud consumer to use a virtual network-based firewall provided by the IaaS cloud provider is the following:

- IaaS consumer runs three VM instances one each for three application types – Web Server, Application Server and Database Server. Each of these types can be designated as a Security Group.
- Restrictions on external access to VM instances belonging to each of the security group can be specified [3]. For example, access to VM instances in the Web Server Security Group can be allowed only on ports 80/443 either with no restrictions on the IP source address or restricting it to the corporate IP network of the IaaS cloud consumer. Similarly access to VM instances belonging to Application Server Security group or Database Security Group can be restricted to only designated administrators on the corporate IP network and that too only to ports needed for establishing secure sessions (e.g., SSH on Port 22).
- Restrictions on VM instances from other VM instances run by the same cloud consumer can be specified based on the architecture of the multi-tier application. For example access to VM instances in the Application Server Security Group can be restricted to VM instances from the Web Server Security Group [3]. Similarly access to VM instances in the Database Security Group can be restricted to VM instances in the Application Server Security Group.

In order to obtain enhanced security assurance for applications running on VM instances, the IaaS cloud consumer should also augment the capabilities provided by virtual network-based firewalls with host-based firewalls running on their VM instances, though it may take away some valuable CPU cycles that could otherwise be dedicated to production applications.

### B. Isolation using VLAN ID/Portgroup

Another set of network level isolation (protection) options that IaaS consumers can look for in an IaaS cloud provider infrastructure consists of the following:

- VLANID-based Isolation
- Portgroup Isolation

It may be difficult in many large scale IaaS cloud provider environments to provide isolation for multi-tenant VMs based on VLANIDs due to the following:

- VLANIDs are complex to configure and the number of IDs are limited (e.g., 4000)
- The security profiles of IaaS cloud consumer VMs are bound to change continuously requiring frequent re-configuration of VLANs.
- In providing isolation using VLANs, the enforcement point is a physical firewall or the physical switch. This requires routing all traffic originating from or coming into a VM to the physical NIC of the virtualized host and on to the trunk port of a physical switch, thus increasing the latency of communication packets with consequent increase in application response times.

Because of the above difficulties in providing isolation through VLAN IDs, IaaS cloud providers could be providing isolation between multi-tenant VMs through a feature called Portgroup Isolation [4]. In the Portgroup isolation, the required isolation between multi-tenant VMs could be provided by assigning the VMs of each tenant to a different portgroup. A portgroup is a software-defined port on the software defined virtual switch on a virtualized host. Isolation between two VMs belonging to two different tenants is obtained by assigning their corresponding VM instances to different portgroups and by installing a gateway software that routes inter-VM traffic based on Portgroup IDs.

## VIII. COMPREHENSIVE DATA PROTECTION IN IAAS CLOUD SERVICE

The complete set of data in a typical IaaS cloud service consists of the following: (a) Data generated/used by applications running in the VM instances and (b) Data defining the entire running VM instance. Examples of former type of data are: (a) Data originating from cloud consumer's client software (e.g., Data Input to an application running in a VM instance) and (b) Data originating from a VM instance (e.g., an application in a VM instance that generates data). Let us now look at the security requirements and the available protection options that IaaS consumers have for these two types of data.

### A. Data Protection for Data Generated/Used by VM Instances

The storage artifact available to IaaS cloud consumer for associating storage with their VM instances is the concept of "Virtual Disks". However the mapping of these logical storage units (i.e., virtual disks) to physical storage artifacts is entirely under the control of IaaS cloud provider. For example, the virtual disks may map to: (a) local physical disks of the virtualized host (b) remotely located NFS file volumes or (c) remote block storage devices accessed through iSCSI or SAN protocols. Irrespective of the storage technology deployed by IaaS cloud provider, protection of data is entirely the responsibility of the IaaS cloud consumer and may span the following requirements:

- Data in Transit protection – This applies to: (a) data in transit between IaaS consumer's client software and VM instance and (b) data travelling between two VM instances of the same IaaS consumer. The protection options for both these classes of in-transit data can be provided through the capability to set up secure sessions (to or between VM instances) using protocols such as SSHv2 or TLS/SS (described under VM instance access protection) as these protocols enable data to be both encrypted and digitally signed.
- Data at Rest protection – This applies to: (a) unstructured data stored under a file system defined over a virtual disk volume and (b) structured data stored by DBMS engine running in VM instances. Regardless of the type of data, it can be protected from unauthorized access/modification through the following: (a) Access Control – Using access control mechanisms available in file systems or DBMS engines, IaaS consumer administrators can define permissions at the appropriate level of granularity for their cloud users, and (b) Encryption. Generally most cloud offerings leave it to the IaaS cloud consumer to encrypt their data. The practical limitation that IaaS consumers encounter while deploying an encryption mechanism to encrypt data going into the virtual disks associated with their VM instances is that the encryption engine and the associated key management engine have to be run in the IaaS cloud provider's infrastructure [5] – most likely in a dedicated VM instance for performance reasons.
- Data Durability/Recoverability protection – This applies to protecting data due to corruption and loss/theft of the media holding the data. The most

common technique applied is a mechanism for periodical backup and recovery capability for restore/recovery of data in case of data corruption incidences. This kind of protection again may apply to two types of data. They are: (a) Data generated/used by applications running on VM instances (for which transit/access/storage protection have been discussed in the previous sections) and (b) Data defining the entire VM instance itself. For data of the first type, the IaaS cloud consumers should have to employ on their own, either a data backup/recovery solution or rely on a Cloud Storage service that may be offered by the same IaaS cloud provider or some other cloud provider. This is due to the fact that such a backup/recovery service is usually not offered as an integral part of IaaS cloud service. Regarding durability/recoverability protection for “data that defines the entire VM instance”, there are several options and hence we devote a separate section to discuss this.

#### *B.Data Protection for Files that define the VM instance*

Since VM images are a set of data files (refer section II), VM instances that are launched from those images are made up of the same set of files augmented with files that capture the state of the VM instance such as virtual memory swap files and log files. The following backup & recovery solutions are available for backing up files that define the VM instance:

- Image-level backup with Snapshot capability [6]: In this backup mode, the entire contents of the virtual disk defined in the VM instance is backed up as an Image. This backup is done without going through the guest OS of the VM instance. In this type of backup, in order to obtain a transaction-level consistency of data in the various disk blocks, the following procedure is adopted: First the VM instance is subject to quiescing using a special driver that runs inside the guest OS. This action momentarily pauses the running processes on the VM instance and forces the guest OS and applications to write any pending data to disk. Once that is complete, a virtualization-specific process called

Snapshot is performed using a tool at the hypervisor layer. The effect of this snapshot process is that any subsequent writes by the running VM instance will be written to a temporary virtual disk file, thus freezing the contents of the original disk file. After the image-level backup of the original (virtual) disk file is completed, the contents of the temporary virtual disk file is merged block by block with the original disk file to bring the contents of the VM instance up to date and the snapshot is also deleted. The advantage of image-level backup is that it not only makes the backup a simple process but also the restore as well since the image-level backup can simply be copied to any other storage device attached to any other virtualized host and the VM restarted in the new virtualized host.

- File-level backup: This backup is done at the level of individual files that constitute a running VM instance and is done through VM instance OS (Guest OS). The downside of this type of backup is that it may take away some valuable CPU cycles allocated to a VM instance which might otherwise be used by applications running on them.

## IX. CONCLUSIONS & BENEFITS

In this paper, we identified the typical set of use cases for IaaS cloud consumer, the associated security requirements for its safe operation and analyzed the protection options available to meet those requirements based on security solutions/ technologies offered by IaaS cloud providers and third parties. The security requirements, protection options and the focus of analysis of those protection options in terms of feature set/deployment architecture are summarized in table 1. The primary benefits of the analysis of the protection options are: (a) Provides a realistic picture of security protection options the IaaS cloud consumer can deploy, (b) Provides a realistic assessment of IaaS cloud provider’s security capabilities and those that can be demanded and (c) Enables IaaS cloud consumer to choose the most appropriate security configuration for their VM instances depending upon the profile of the applications running in them.

Table 1. Summary of Protection Options Analysis for IaaS Use Cases

Section – Use Case	Security Requirements	Protection Options	Feature Set/ Deployment Architecture Analysis
Checking out VM Images	(a) Integrity of VM Image files (b) Preventing Unauthorized VM launches	(a) Digitally signed VM Images (b) Name Space Control, Gold Standard Configuration, Separation of Data & Metadata & Access control	(a) Strength of Cryptographic Signing Keys, Secure session with Image Repositories (b) Robust Configuration Mgmt Utilities
Configuring VM Instance OS (Guest OS)	(a) Hardened OS Distribution (b) Latest Patches	Verify that IaaS provider's pre-defined images meet the IaaS consumer's Gold Standard	N/A
Configuring Virus / Malware Protection	(a) Monitor File Events, Scan Files (b) File Remediation	Run Anti-Virus Engine on each VM instance (or) Run one copy as a Security Virtual Appliance	Security Virtual Appliance enables uniform application of policies & Consumes less resources
Configuring VM instance Access Protection	(a) Secure Session (b) Multifactor Authentication	(a) SSHv2 or TLS/SSL (b) PKI-based Authentication or One-time Password Token	Strength of Encryption / Signing Keys & Entropy of Authentication secrets
Configuring VM instance lifecycle operation	(a) Limit API calls to authorized admins (b) Sending API calls with integrity & Confidentiality	(a) Identity & Access Management System (b) Digitally signed API calls & Dedicated Management network	(a) Creation of Admin Groups/Roles (b) Public Cryptographic Keys on Virtualized Host
Configuring VM Instance Isolation	Restricting the type of inbound & outbound traffic between VMs	(a) In-VM or Virtual Network based Firewall (b) Isolation using VLAN ID/ Portgroup	(a) Virtual Network based Firewalls use Hypervisor's Introspection API (b) Portgroup Isolation solutions function as Application Gateway
Comprehensive Data Protection in IaaS cloud service	Confidentiality & Integrity protection for in-transit & stored data (generated by & constituting VM instance)	(a) Secure Session Protocols (in-transit data) (b) Access Control + Encryption (stored data)	(a) Strength of cryptographic session keys (b) Strong Authentication + Strong Encryption Keys

## REFERENCES

- [1] T.Brooks, C.Caicedo and J.Park, Security Challenges and Countermeasures for Trusted Virtualized Computing Environments, World Congress on Internet Security, 2012, p 117-122.
- [2] J.D. Sherry, Continuous Monitoring in a Virtual Environment, Nov 2013, [http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt\\_continuous-monitoring-virtual-environment.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_continuous-monitoring-virtual-environment.pdf)
- [3] Amazon Web Services: Overview of Security Processes, March 2013, <http://aws.amazon.com/security/>
- [4] The Technology Foundations of VMware vShield, Oct 2013, <http://www.vmware.com/files/pdf/techpaper/vShield-Tech-Foundations-WP.pdf>
- [5] R. Chandramouli, M.Iorga, S.Chokhani, Cryptographic Key Management Issues and Challenges in Cloud Services, NIST IR 7956, Sept 2013, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf>
- [6] E. Siebert, The Expert Guide to VMWare Data Protection and Disaster Recovery, July 2012, <http://www.veeam.com/wp-vmware-data-protection-disaster-recovery-expert-guide.html>