Understanding Private Cloud Security

By Yuri Diogenes – ISSA member, Fort Worth, USA Chapter and Dr. Tom Shinder

This article covers the main elements that should be addressed from the security perspective while architecting and designing a private cloud infrastructure.

Abstract

There are a lot of reasons why cloud computing is getting so much media and industry attention, but one of the main reasons why companies are adopting cloud computing is the financial advantage. While public cloud seems to be the preferred choice for small and medium businesses, there is another cloud infrastructure model that is growing in large enterprises – the private cloud. The private cloud can have a substantial impact on the way information technology (IT) operates; it redesigns the data center by providing agility to the business, enables better resource utilization, and fuels higher availability. However, as with the public cloud, in a private cloud security concerns are still a major challenge. Although many cloud architects argue that private cloud does not present security concerns since it is owned and operated by the company itself, the reality is that there are many security elements that must be addressed before adopting, architecting, and designing a private cloud. This article will cover the main elements that should be addressed from the security perspective while architecting and designing a private cloud infrastructure.

Why care about security in a private cloud infrastructure?

Even if you take private cloud out of the equation, data center security and operations must be well planned and executed in order to enhance the overall security strategy. According to a report issued by Varonis,[1] internal threats are still the major concern for corporations in 2012, and with private cloud adoption the vast majority of the users will be authorized, authenticated, and have access of some type to the infrastructure. With private cloud adoption this risk is likely to increase because if an internal intruder successfully exploits a vulnerability in the private cloud infrastructure, he can potentially affect all other tenants as shown in Figure 1.

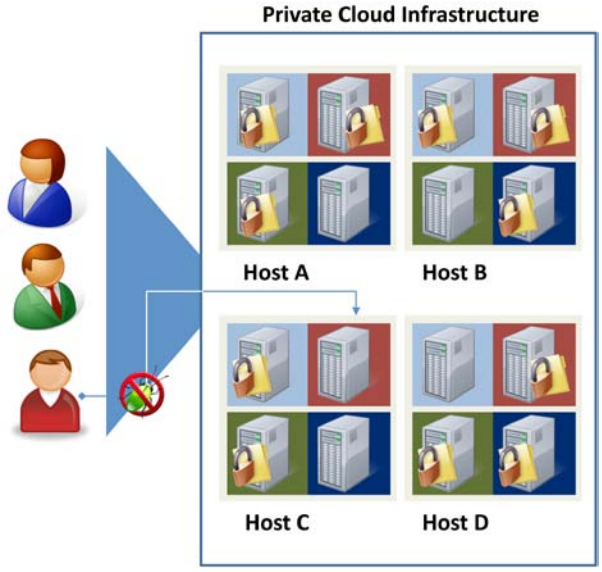

Figure 1 – Without security controls in place a compromised tenant can affect others.

In the private cloud, the importance of a well-architected and executed security design has not changed; the only difference is adjusting to this new model. In a traditional data center environment, the demarcation of security responsibilities between the data center operator and the service user was relatively well defined. Generally, the responsibility was aligned with ownership of the particular physical compo-

1 Varonis Top Predictions for Data Governance in 2012 http://www.varonis.com/go/resources/whitepapers/Varonis-Top-Predictions-for-Data-Governance-in-2012.pdf.

nent, whether that was a server, a networking device, or the overall network infrastructure; if the IT department owned and administered the server, then that department also managed and updated security on that asset. With cloud models, security responsibility has altered in that departments may be responsible for a portion of the security on the service that they pay for, depending on the service provisioning model in use.

A key differentiator in public cloud environments is that service is provided on a shared tenant basis and multiple tenants use portions of the same pooled infrastructure and services. In the private cloud the tenants will be the departments of the company as shown in Figure 2. The public cloud implementation then applies authentication, authorization, and access controls to create logical partitions between the tenants so that individual tenants are isolated from each other and cannot see other tenants' data.

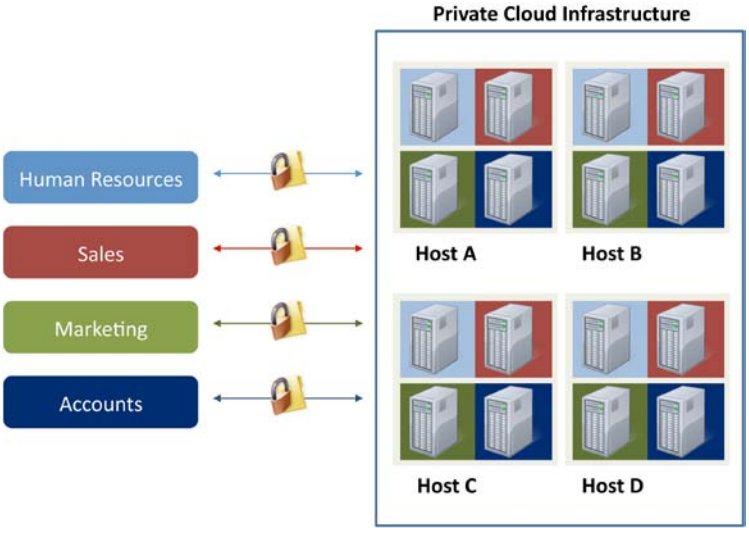

Figure 2 – Shared tenant model in private cloud infrastructure.

Similar to the multi-tenant scenario in the public cloud, in the private cloud each department or business unit within the company must be isolated from others even when their services are located on the same host operating system and server. There is nothing new on this requirement; even today large enterprises do have some sort of isolation to enhance security, privacy, and performance between departments. Generally organizations do have good reasons to implement such isolation, such as between different business units or between the accounts department and the rest of the organization. Consequently, a private cloud model may also be a shared tenant model with similar requirements for effective security partitioning between different business units as with public cloud implementations.

Virtualized environments

Although there is a natural tendency to correlate cloud with virtualization, the reality is that virtualization is not an "absolutely" essential component of private cloud architectures. Companies that are moving to a private cloud infrastructure can use blade server arrays or other compute configurations to provide cloud-based services. However, the advantages of improved server utilization and greater operational flexibility that virtualization platforms provide have led to very high uptake of this technology in cloud environments.

Virtualization introduces a very different threat landscape from a security perspective. This happens because virtualization changes the way an organization secures and manages its data center. Since workloads are mobile and can move from host to host based on optimization algorithms that require no human involvement, security policies linked to physical location are no longer effective, so security policies must be independent of network or hardware topologies.

Additionally, in order to provide effective security in virtualized environments, it is necessary to have virtualization of the security controls themselves. As these virtualized controls become available, they should as a minimum meet the following criteria:

- Fully integrate with the private cloud fabric
- Provide separate configuration interfaces
- Provide programmable, on-demand services in an elastic manner
- Consist of policies that govern logical attributes, rather than policies that are tied to physical instances
- Enable the creation of trust zones that can separate multiple tenants in a dynamic environment

Security in a virtualized infrastructure must be adaptive and natively implemented into a fabric where resources are allocated dynamically. Any security functionality that is tied to a server, an IP address, a MAC address, port, or other physical instance will no longer be as effective as in purely physical environments due essentially to the decoupling of services and the physical hardware seen in a virtualized environment.

Private cloud security challenges

NIST (National Institute of Standards and Technology) publication 800-145,[2] *The NIST Definition of Cloud Computing*, defines the five essentials characteristics of cloud computing:

- Resource pooling
- On-demand self –service
- Rapid elasticity
- Broad network access
- Measured service

These essential characteristics also apply to both public and private cloud models and for four of them there is at least one core security concern that must be addressed during the

2 NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

designing and planning phase of your private cloud infrastructure.

Resource pooling

Resource pooling is the mechanism by which cloud environments can increase utilization levels, reduce costs, and make use of cheaper resources such as commoditized servers and inexpensive hard disks. The user's (tenant's) primary security concern regarding this essential characteristic is related to how secure his data is, who else can access it, and if the data is safe even if something untoward occurs.

In order to address this security concern, the cloud architect will need to design the private cloud security infrastructure to:

- Prevent leakage between tenants by isolating them
- Use AAA (authentication, authorization, and access control) and RBAC (role-based access control)
- Use least privilege approach while delegating permissions

On-demand self-service

The essence of cloud provisioning is self-service. When combined with rapid elasticity, self-service enables cloud implementations to provide dynamic and timely responses to requests for more or fewer resources. However, simplicity and convenience of on-demand self-service can also be its weakness. Because cloud environments are often virtualized, any errors in assigning security permissions during the provisioning process could, for example, result in other tenants being able to access the newly provisioned environment.

It is very important to understand that many organizations do have IT operations in place (such as ITIL v3) that already require different levels of service agreement between divisions and IT. When you move to the private cloud, those service agreements should be reviewed so they are consistent with what can be provided by the new private cloud platform. It is quite possible that you will enhance the Service Level Agreement (SLA) for many operations due to the flexibility and agility that private cloud offers.

The cloud architect's major security concern as it relates to on-demand self-service is how to control who has access to private cloud services and how to monitor and audit these services. The open questions shown in Figure 3 must be answered and explicitly covered in the SLA.

Figure 3 – Details about on-demand self-service that must be on the SLA.

In order to address these security concerns it is important to:

- Monitor errors in security provisioning
- Have a cleanup process deprovision resources, remove access, and destroy any residual data that might be present
- Return to the cloud in the same base state as all assets in the respective resource pools

Rapid elasticity

Rapid elasticity enables organizations and business units to scale their operations up and down quickly to meet demand. Because the compute, storage, and network resources are pooled and can therefore be shared between tenants, users can request as little or as much of each resource as needed within their budgetary constraints. The management system can then rapidly allocate these additional resources either through manual requests or by automated, demand-led provisioning.

The security concern that a user (tenant) has regarding rapid elasticity is that a rogue application, client, or denial of service (DoS) attack might destabilize the data center by requesting an overly large amount of resources. The challenge here is to reconcile the perception of infinite resources while keeping control of the resources to avoid such problems.

In order to address this security concern it is important to:

- Monitor and manage resource utilization
- Use automation to avoid human error
- Enforce policy-based quotas to restrict overuse of the resources

Broad network access

Although some cloud architects will argue that broad network access only applies to public cloud, the reality is that this is not true. Even without cloud computing considerations, large enterprises already require broad network access, which is why for the past ten years VPN technologies have evolved to be more easily implemented and transparent to use. In a private cloud infrastructure remote users will still need to have remote access to those resources located in the private cloud.

Consumers of your private cloud services may be authenticating to an application provided by a public cloud provider using federated identity to authenticate from your internal directory service. Your internally-hosted private cloud implementations may also be using web services from a third public cloud provider. In consequence, failing to consider the broad network access picture is, therefore, inherently limiting.

The cloud architect security concern regarding this mechanism is how to ensure that an appropriate level of security applies regardless of client location and regardless of form factor. This requirement applies to both cloud management and application security.

In order to address this security concern it is important to:

- Access device state
- Implement application level access control
- Implement security controls to avoid data leakage located on user's own device

Summary

Cloud computing is having a major impact on our industry and how we think about security. While private cloud is often considered to have security concerns similar to those addressed in a traditional data center, there are a few issues that are unique to private cloud security, and others that represent similar data enter security issues, but with an increased emphasis when applied to the private cloud. Of all the security issues that you need to address in the private cloud, one of the most important is that of isolating tenants in a multi-tenant environment. Isolating tenant services from one another needs to be enforced at all levels of the private cloud infrastructure, including compute, storage and networking. You can use the five essential characteristics of cloud computing as a pivot for addressing the security issues that cloud computing introduces over those seen in the traditional data center. You can then use on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services as buckets in which to place your security design issues specific for private cloud.

Additional resources

For more information about private cloud security:

—A Solution for Private Cloud Security: Service Blueprint, http://social.technet.microsoft.com/wiki/contents/articles/6643.blueprint-for-a-solution-for-private-cloud-security.aspx.

—A Solution for Private Cloud Security: Service Design, http://social.technet.microsoft.com/wiki/contents/articles/6644.design-guide-for-a-solution-for-private-cloud-security.aspx.

—A Solution for Private Cloud Security: Service Operations, http://social.technet.microsoft.com/wiki/contents/articles/6645.operations-guide-for-a-solution-for-private-cloud-security.aspx.

We encourage you to review all three of these documents prior to and during the design and planning phases of your private cloud infrastructure. You can also download slide deck that we delivered at ShareCloud Dallas 2012 that covers this subject, available at http://gallery.technet.microsoft.com/A-Solution-for-Private-0739e4a1.

About the Authors

Yuri Diogenes, CISSP, CIEH, CICSA, CompTIA Cloud Essentials Certified, CompTIA Security+, MCSE+Security, currently works as Senior Technical Writer in the Server and Cloud Division Information Experience at Microsoft. Yuri is the co-author of the Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion from Microsoft Press, co-author of the Forefront book series also from Microsoft Press and currently it is writing a Windows 8 Security book for Syngress in partnership with Tom Shinder. Yuri is a candidate for a Master of Science Degree in Cybersecurity Intelligence & Forensics from UTICA College. Yuri can be contacted at http://blogs.technet.com/yuridiogenes or you can also follow him on Twitter (@yuridiogenes).

Dr. Tom Shinder is a 15-year veteran of the IT industry. Prior to entering IT, Tom was a practicing neurologist with special interests in epilepsy and multiple sclerosis. He then began his career in IT as a consultant, and worked with many large companies, including Fina Oil, Microsoft, IBM, HP, Dell and many others. He then started his writing career toward the end of the 1990s and has published over 30 books on Windows, Windows Networking, Windows Security and ISA Server/TMG. For over a decade, ISA Server and TMG were Tom's passions, and he ran the popular web site www.isaserver.org, in addition to writing 8 books on ISA/TMG. Tom joined Microsoft in December of 2009 as a member of the UAG DirectAccess team and started the popular "Edge Man" blog that covered UAG DirectAccess. Tom is currently a Principal Knowledge Engineer in the Server and Cloud Division Information Experience Group Solution's Group and his primary focus now is private cloud – with special interests in private cloud networking and security. You can follow him on Twitter (@tshinder).