PRIVATE CLOUD COMPUTING CHALLENGES AND ARCHITECTURE FOR IMPLEMENTING EFFECTIVE SECURITY

M.N.B.Gayathri

M.P.R.Sekhar

M.Adithya

Abstract

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over. Public clouds are available from Google.com, Amazon.com, Microsoft, Oracle/Sun, and many other vendors. Private cloud technologies, where the cloud software is loaded on local or in-house server hardware, are available from VMware, Eucalyptus, Citrix, Microsoft, and there are thousands of vendors offering private cloud with all sorts. With all of the hyperbole has come a large swell of early-adopters and developers. This paper aims to provide an architectural blueprint for implementing effective security within a private cloud environment.

Keywords: private cloud computing, private cloud environment, private cloud security

Introduction

Implementing a private cloud environment requires IT departments to re-evaluate many aspects of how they interact with their organization. Private cloud computing provides the ability to allocate costs in a fair and metered manner to the service user in proportion to the user's demand for those services. Private cloud implementations also affect the way in which IT departments need to view security. The chief change is that security can no longer be viewed as a discrete silo that contains traditional capabilities such as authentication, authorization, auditing, and so on. The security model shows that to approach any part of the cloud environment, the consumer or provider must pass through the security wrapper. Additionally, all communication between layers in the cloud model (for example, between infrastructure and platform layers) must also pass through security controls. Security also applies to intra-layer communications, The opportunity with the move to private or hybrid cloud architectures is that it gives you the chance to re-examine the provisioning of security within your datacenter. We can take a holistic view of the central importance of security and ensure that you achieve this goal within your private cloud design. The following section defines the new security threats from the cloud and identifies the private cloud security domains within the Cloud Security Alliance (CSA) model and suggests a security model

Cloud Security Alliance Domains:

The Cloud Security Alliance (CSA) is an independent grouping consisting of over 120 corporate members. CSA is becoming the focal point for security standards globally, aligning multiple, disparate government policies on cloud security and putting forward standards for ratification by international standards bodies."

CSA has recently released Version 3 of their Security Guidance for Critical Areas of Focus in Cloud Computing document. The CSA document defines fourteen security domains for both private and public cloud. In contrast, this document covers the areas that these domains reference by using the Microsoft private cloud security model.

Before diving deeper into the security architectural issues and challenges, we have to consider the following points:

1. Defining the Private Cloud Security Problem Domain: Security is a universal component of cloud service provisioning Key Security Differences in Private Cloud Environments are

- Security Responsibility

- Security Attack Targets
- Shared Tenant Model
- Virtualization

Security Responsibility:

. Generally, the responsibility was aligned with ownership of the physical component, 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. Following figure shows the split of security responsibility for the three main cloud provision models.

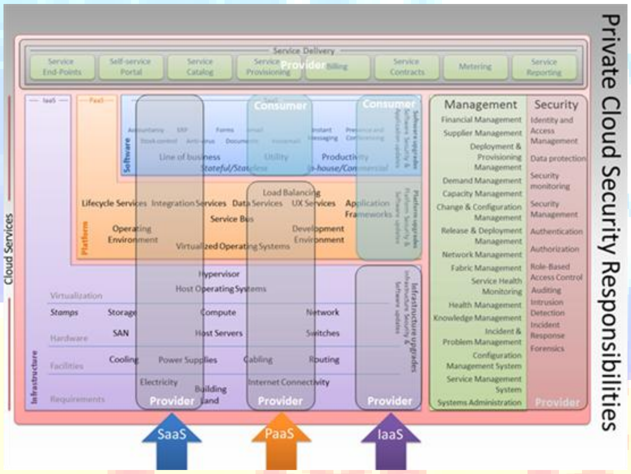


Figure: Division of security responsibility for private cloud service models

Security Attack Targets

Taking the private cloud reference model as the basis for analysis, we can identify threats to the private cloud infrastructure and place these threats into appropriate places within the model. This approach provides a basis for threat modeling and risk analysis.

Hence, we can classify attacks according to the layer or stack that the attack targets. Following figure highlights the primary areas in the private cloud where these individual attack types can target. Note that this diagram is not showing responsibilities but listing the different types of attacks that might take place against the management stack, the infrastructure layer and so on.

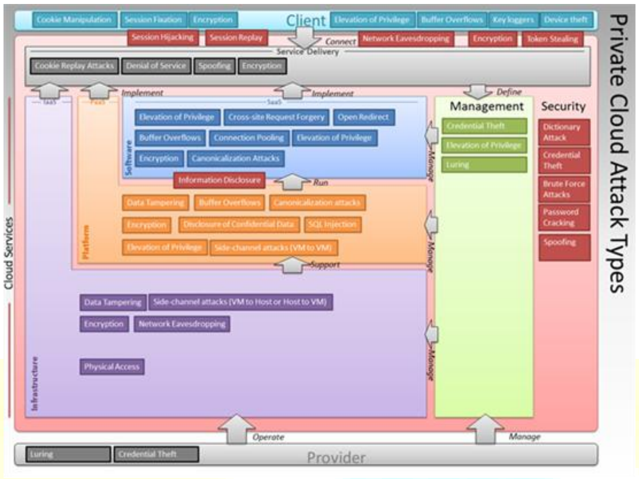


Figure: Security Threats to Private Cloud Architectures

Shared Tenant Model:

A key differentiator with public cloud environments is that the service is provided on a shared tenant basis and multiple tenants use the same services. In private cloud terminology, a tenant is a client, typically a business unit within the organization, who is using the private cloud to run their applications and services.

The perception of a private cloud is that it is only hosting one organization, and in consequence, security partitioning is not required. In consequence, 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.

Virtualization:

Virtualization radically changes the way an organization secures and manages their data center. As 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.

A key factor for implementing effective security in virtualized environments will be 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

2. **Cloud Security Challenges**: To highlight the changes in security between traditional IT systems and cloud-based environments, this paper takes four of the five the NIST cloud computing definitions and analyses This paper considers each of these challenges in turn before moving on to identify how to respond to these challenges.

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. Resource pooling needs to be considered at all three service layers of the private cloud model. But this resource pooling also requires significant consideration of the security aspects from such a configuration.

With a private cloud implementation, a similar requirement for strict data partitioning as in public cloud is not immediately obvious. If, however, you do need to protect data and applications from access by authenticated users who are not authorized to view that information or use those applications, then you do need to implement some form of partitioning within your private cloud environment. Similarly, administrative rights need to be carefully controlled, as you may want to give certain groups or business units the right to carry out limited administrative actions on their resources.

With each pooled resource, you must ensure that each tenant's data or applications are kept partitioned from those belonging to other tenants. Any data that is exclusively owned by a consumer should not leak to other sessions nor be accessible by other users or tenants, whether maliciously or not. Partitioning and Role Based Access Control (RBAC) also applies to your administrators, who should not have automatic access to tenant data. In the case where an administrator does require access to tenant data, then that access must be carefully audited.

The following areas are those that need to be considered when planning for resource pooling:

- Virtualization
- Multi-Tenancy
- Infrastructure security

- Platform security
- Software security
- Data protection
- Service Level Agreements (SLAs)

On-Demand Self-Service:

The essence of cloud provisioning is that of 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. No longer is it necessary to go through a cumbersome process to request a new server, development platform, or software – you can simply go to a self-service portal and select what type of computing resource you want from a standardized service catalog. The portal then provisions the environment, allocates resources from the shared pools, mounts the environment, configures security, and then connects the consumer to the requested service.

When the requesting user indicates that the resources are no longer required, you must be able to deprovision those resources, remove access, and destroy any residual data that might be present. All resources must then be returned to the cloud in the same base state as all assets in the respective resource pools. The destruction of residual data is particularly important. Cases have come to light of public cloud providers finding that tenant data from one session was not being adequately purged, which enabled subsequent tenants to access this data.

The following areas are those that need to be considered when planning for on-demand self-service:

- Monitoring
- Security Management, including templates and standardization
- Infrastructure security
- Management security
- Incident response and forensics
- Legal issues, such as compliance, data protection, and SLAs

Rapid Elasticity

Rapid elasticity enables organizations and business units to scale their operations up and down quickly to meet demand Rapid elasticity enables organizations to cope with a variety of variations in demand such as irregular spikes (such as might occur after an exceptional news event) or regular patterns, like running month-end financial reports.

There is a resource limit even in the most well-founded private cloud implementation. In consequence, repeated requests to provisioning resources or an inability to deprovision resources properly could lead to resource exhaustion.

The following areas are those that need to be considered when planning for rapid elasticity:

- Monitoring
- SLAs
- Attacker profiles (authenticated attackers)
- Infrastructure security

Broad Network Access

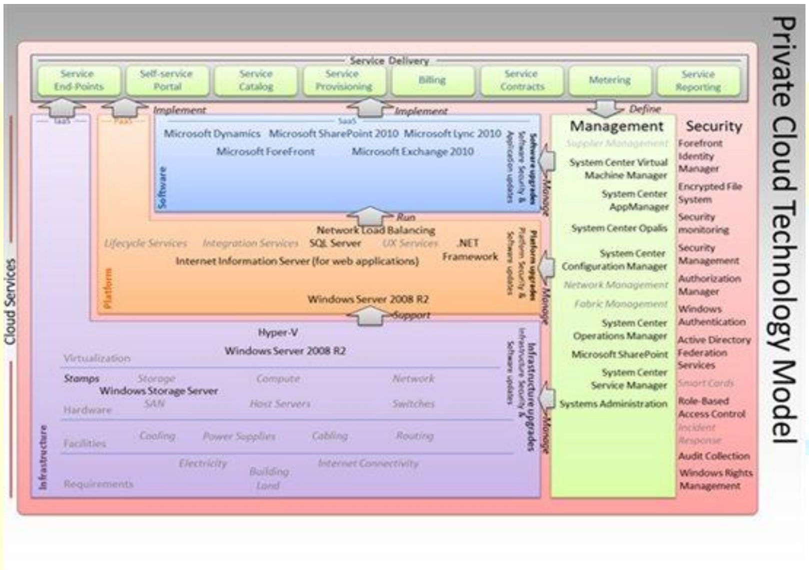
In private cloud environments, there is no absolute requirement to connect your data center to the Internet, although not having this connectivity might adversely affect the potential benefits from the private cloud implementation.

However the broad network access cloud characteristic requires IT departments to consider the entirety of the client to service network journey. It is also requires consideration of the effect of this requirement for universal access on management of the environment. Coping with broad network access requires consideration of the following factors:

- Perimeter network role and location
- Identity and Access Management (IdAM)
- Authentication
- Authorization
- Role-based access control (RBAC)
- Federation
- Auditing
- Public network connectivity
- Service delivery security
- Endpoint protection
- Connectivity to software, platform, and infrastructure layers
- Client security

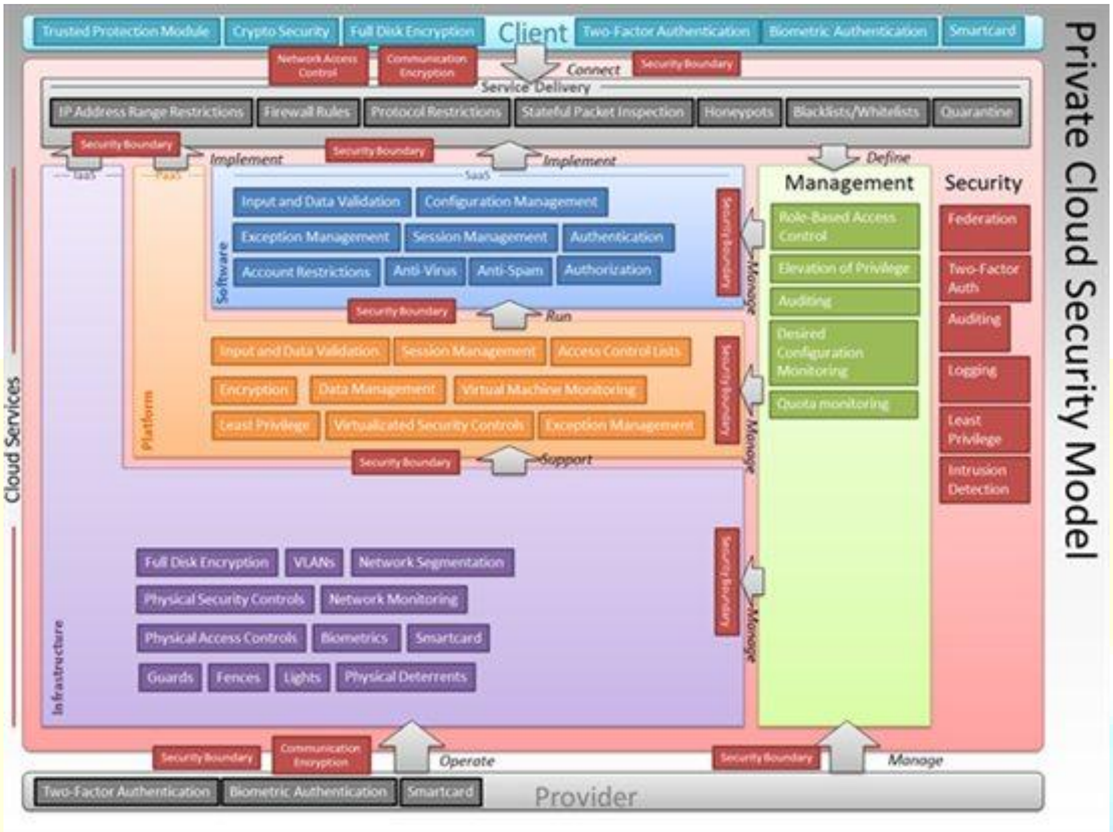
3. **Private Cloud Reference Model Security Perspective:**

When envisioning your route to the private cloud, a reference model can help you visualize your complete environment. There is currently no universally accepted reference model for private cloud and several organizations that work in this area have published their own model. Microsoft is no exception and has devoted significant investment into creating a private cloud reference model that Enterprise Architects can use to create their design. Figure below shows what a technology view might look like with a private cloud implementation based on Microsoft technologies.



4. Private Cloud Security Model :

The private cloud security model uses the same design as the private cloud reference model but replaces the capabilities with mechanisms for implementing security. Figure below shows how these mechanisms tie in to the different layers of the private cloud reference model.



Conclusion

Having a way to tell whether the mechanisms and capabilities in the private cloud are patched properly would also be a useful part of the framework. People's behavior can be tracked and monitored; for instance whether people allow the automated patching software to run, or updating anti-virus software whether people understand how to harden their virtual machines in the cloud.

Annotated Bibliography

1. Basta, A., & Halton, W. (2007). *Computer Security and Penetration Testing* (1st ed.). Delmar Cengage Learning.

2. Berre, A. J., Roman, D., Landre, E., Heuvel, W. V. D., SkÃ¥r, L. A., UdnÃ¦s, M., Lennon, R., et al. (2009). Towards best practices in designing for the cloud. In *Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications* (pp. 697-698). Orlando, Florida, USA: ACM. Retrieved from http://portal.acm.org.library.capella.edu/citation.cfm?id=1639950.1639970 &coll=portal&dl=ACM&CFID=80867670&CFTOKEN=24312614

3. http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman

4. Cloud Security Alliance Guidance Version 2.1. (2009). . Cloud Security Alliance. Retrieved from www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

Hayes, B. (2008). Cloud computing. *Commun. ACM*, *51*(7), 9-11. Retrieved from http://portal.acm.org.library.capella.edu/ft_gateway.cfm?id=1364786&type=html&coll=portal&dl=ACM&CFID=80867670&CFTOKEN=24312614

5. Milne, J(2010, February 9). Private cloud projects dwarf public initiatives. Retrieved fromhttp://www.cbronline.com/news/private_cloud_projects_dwarf_public_initiatives_281009