Private Clouds

Krishnan Subramanian
Analyst & Researcher
Krishworld.com

A whitepaper sponsored by Trend Micro Inc.

Introduction

Cloud computing has completely transformed the way business organizations use IT both inside and outside of their organization. In spite of the economic benefits offered by public cloud services, organizations are reluctant to move their infrastructure outside their premises. However, they also want to apply the lessons learned from public clouds to better optimize the resource usage in their infrastructure. Private clouds offer an easy solution to help businesses take advantage of some of the benefits of cloud computing without compromising on security and control. In this whitepaper, we will discuss the business benefits of private clouds and the security requirements needed to mitigate any risks.

What is a Private Cloud?

Simply put, private clouds are cloud infrastructure based on dedicated hardware under the control of the organization offering services on-demand through a self-service portal. Private clouds provide elasticity that was previously unavailable in the traditional computing models, including rapid computer resource provisioning with services billed back to individual business units.

The infrastructure services are single-tenant and they can be managed by the organization or a third party either on premise or in third-party datacenters. Private clouds can be deployed either by using one of the packaged cloud platforms like Eucalyptus, OpenStack, etc. or by adding automation, management, and self provisioning capabilities to an already virtualized infrastructure. It does not matter how one deploys a private cloud as long as it results in resources being pooled together into one centralized unit; available on demand to the users to provision, manage, and monitor using a management interface; and a chargeback mechanism.

Unlike public cloud services, private clouds are capital intensive but offer more control and greater security. Trend Micro, a cloud security company, conducted a survey concerning cloud adoption and captured information on the top barriers to cloud implementation. A private cloud has advantages that can address many of the respondents' concerns.

Trend Micro Survey Results

A recent survey conducted by Trend Micro offers some insights into the expectations and concerns businesses have about cloud technologies. The survey was conducted in six different countries with 1200 respondents from companies with at least 500 employees. Some of the key results are:

- 50% of the survey respondents pointed to apprehension over security as a key reason for holding back on their adoption of cloud technologies.
- 40% of the respondents said that their IT security requirements were not being met by the current cloud providers.

© Krishnan Subramanian 2011

- 48% of the survey respondents were worried about performance and reliability of cloud services.

- Other barriers to cloud adoption included: 27% were concerned with lack of transparency about data center facilities, hardware, and disaster recovery by public cloud providers; 27% of respondents quoted compliance as an implementation barrier; and 25% were worried about vendor lock-in.

Even though the concerns of the survey respondents point out to some of the barriers to cloud adoption, these can be overcome in both the public and private clouds by using appropriate security. In this whitepaper, we will discuss the benefits specific to private cloud, its unique security considerations and the best practices to remove the implementation barriers.

Benefits

Even though private clouds lack some of the benefits of cloud economics and are restricted in scalability compared to public clouds, it offers other benefits suitable for business users.

Cost Savings

- Gives the key benefit of better resource usage by effective pooling and distribution of resources. This results in a drastic reduction of resource wastage, offering increased infrastructure cost savings.

- Furnishes a chargeback model that helps individual units better utilize their budgets, especially in today's economic climate where budgets are limited by deeper cost cuts.

- Removes the need for re-architecting the existing applications to meet the requirements of public cloud environments, thereby, saving any additional costs.

Business Agility

- Provides on-demand availability for all business units without the long wait associated with the traditional IT procurement process. This results in increased agility across all the business units, benefiting the organization in terms of cost, faster time to market, and higher productivity.

- Supplies better workload management in terms of faster deployment, easy management, higher reliability, and better scaling than the traditional IT infrastructure.

Security, Control and Customization

- Offers better security than in public clouds. This is especially critical in meeting some of the compliance needs. Having a private cloud infrastructure takes away concerns about lack of transparency on the service provider side.
- Delivers more control over the underlying hardware than in the multitenant environment of the public cloud, addressing the concerns expressed by survey respondents about the performance and reliability offered by public cloud service providers.
- Affords better customization of the infrastructure to meet the organization's functional needs.

Security Considerations

Even though private clouds offer more control and security than public clouds, a move from the traditional computing environments to a cloud environment requires a different set of security considerations. In this section, we will highlight some of these considerations and in the following section we will offer solutions that can be employed to take safe advantage of cloud technologies. Some of the age old security ideas tied to the physical infrastructure cannot apply in the cloud environment. Similarly, security should meet the needs of the on-demand nature of the cloud environment. Some of the security considerations in the private cloud are:

- **Elastic and changing perimeter:** In private clouds, the resources are pooled centrally and delivered on demand. The resource usage changes elastically based on the needs of the users. Businesses need to move away from the fixed perimeter idea of the traditional computing world to a more diminished and elastic perimeter. Moreover, most of the hypervisors today support VM migration which means virtual machines are not bound to specific hardware or even network. This, along with some of the other cloud features, like scaling out, will ensure that the perimeter is always changing.
- **Management and containment issues:** In private clouds where resources are pooled centrally and delivered across the organizations, managing security, assessing vulnerabilities, and fixing security flaws are different and more dynamic, partly due to its elastic nature and, also, due to the fact that multiple departments, users, and domains are involved with different sets of policies and stakes.
- **Ineffective device-specific controls:** Unlike in traditional IT, having device-specific controls, like restrictions based on MAC addresses, etc., will not work because we are dealing with virtual machines not bound to specific hardware.
- **Policies for dynamic environments:** Unlike in traditional IT, security policies need to be adaptive and intelligent and not be linked to trusted zones based on physical hardware.

- **Data leak risks:** The cloud environments break down departmental silos and offer increased accessibility, especially to non-employees outside of the organization if given access to the on-demand computer resources. Not properly locking data down becomes an issue leading to unwanted breaches. Protecting data from leaks becomes critical in a cloud environment.

Best Security Practices

The threat landscape looks the same in a cloud environment, but the cloud infrastructure creates new security requirements. Cloud technologies require reconsideration of traditional security practices to meet the needs of a more centralized and dynamic environment. There are some best practices that can help mitigate the risks in the private cloud. In this section, we will list some of the important ones:

- **VM-level security:** Perimeter-level protections like firewalls and device-specific controls like restrictions based on MAC addresses do not work. Instead, we need to build the defense at the Virtual Machine (VM) level so that it travels with the VM in the cloud infrastructure. Whether a firewall or a security policy, security technologies should be designed at the VM level and not based on physical hardware.

- **Multi-layered defense:** Using tools like firewall, IDS/IPS, log inspection, etc. geared towards virtual machines is important. More importantly, the traffic between the virtual machines should be continuously monitored by setting policies appropriately.

- **Patch management:** Having the right set of policies around patching is important. Patching in the cloud environment is much more difficult than in the physical environment because VMs can be moved around and switched on and off at will.

- **Data and encryption:** In order to protect the data in a more dynamic cloud environment, businesses should have data protection policies in place. Data should be encrypted both at rest as well as in motion. Well-designed encryption key management policies ensure data integrity and specify when and where data can be accessed to support compliance and internal governance.

- **Regulatory compliance:** Businesses should understand the impact of regulations and assess which policies and procedures change in a private cloud deployment. For example, activity reporting, logging, controls testing, etc. might be different in a private cloud environment compared to traditional environments. So, it is critical to understand the nature of this change and associated impact; develop processes to collect evidence, such as audit logs; and store them securely. Also, businesses will benefit from selecting an auditor who understands the changed dynamics and challenges of cloud services.

Recommendations for Private Cloud Implementation

Private Cloud Implementation

In the Trend Micro survey, 13% of respondents had a private cloud in production and another 43% were implementing or were in the midst of piloting a private cloud.

Private Cloud Use Cases

Private clouds are useful in highly regulated industries like financial sector, healthcare, scientific computing, etc. Similarly, businesses wanting to run legacy applications will find private clouds suitable for their needs. However, it should be noted that most of the workloads can be moved to public clouds by ensuring that proper security procedures are implemented. In fact, the availability and business continuity offered by public clouds are comparable to those offered by private clouds.

Conclusion

Private clouds offer organizations a way to better optimize their infrastructure by taking advantage of some cloud-like features while still enjoying the security and control needed for their businesses. Private clouds are especially useful for organizations with strict compliance requirements or a need to protect their high value IP, although encryption and virtual machine-level security may allow even sensitive data to be moved to a public cloud. However, any organization worried about moving their mission critical workload to public clouds can take advantage of private clouds. A move to the cloud model requires a different set of security considerations and any associated risks can be easily mitigated with best security practices.