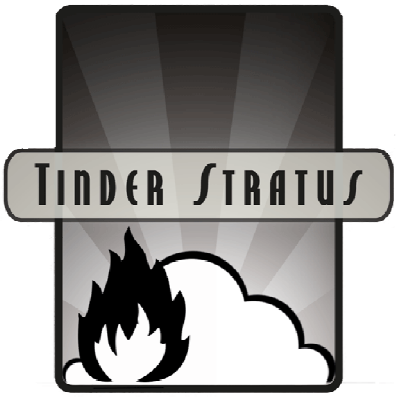

Cloud Adoption Benefits for Small And Medium Sized Organizations

Published January 2, 2012
By Andrea Bilobrk, CCSK

Contents

Introduction	**2**
Virtualized versus Cloud	**3**
Does Cloud Adoption Make Sense?	**3**
Security Concerns in Cloud Adoption	**4**
Benefits of Utilizing a Single Provider	**5**
Recommendations for Cloud Adoption	**7**
Summary	**9**

Introduction

For small and medium-sized organizations, the decision to move to cloud infrastructure (or virtualized infrastructure) involves many factors that would normally not apply to large organizations whom leverage in-house IT and security departments. Cloud or virtualized environments allow small and mid-sized organizations to leverage computing resources through a service provider without the requirement for up-front capital expenditures. A global survey of SMBs by Microsoft[1] saw an anticipated 74% adoption rate over the next 3 years for cloud services, both free and paid, with the key areas of adoption centered on off-site provisioning of accounting/HR resources, project management, collaboration, and data storage/backup functionality.

By utilizing cloud computing services, organizations are able to manage their IT requirements while lowering their infrastructure costs, and converting capital expenditures to operational ones. In addition, through outsourcing their infrastructure, small and mid-sized organizations have the ability to adopt the best practices of the larger providers without having to invest in the resources required. This is especially helpful in environments where there is limited IT or security expertise.

The key resistance for organizations of all sizes in the transition to cloud services is the risk of privacy and security, with 21% of respondents citing this as their key barrier to adoption. This is a perfectly understandable issue, as the main reason cloud computing can be so cost effective is that it is based heavily on multi-tenant infrastructure. This means that one organization may be storing sensitive data next to another organization, sharing the same Hypervisor and hardware. While there are logical separations between tenants, there is still a fear of cross-contamination of VMs through poor security practices held by the service provider. In reality, the audit controls that are in place in most large service

[1] http://www.microsoft.com/Presspass/presskits/commsector/docs/SMBStudy_032011.pdf

providers help to reduce the threat of VM compromise, but due diligence is always recommended when utilizing cloud services.

Virtualized versus Cloud

Let's take a step back and clearly identify the difference between cloud and virtualization. They are actually one and the same. When you leverage cloud services, you are moving your assets to a virtualized environment. The service provider might offer a private infrastructure where you have a dedicated physical server running your virtualized applications and hosting your data. In most cases this is not cost effective for the SMB, so public cloud will make up the largest group of service provider offerings geared towards this market. Public clouds allow service providers to utilize larger server stacks to host multiple clients, or multi-tenant. Each tenant is allotted a certain amount of infrastructure (in the case of IaaS) and can use as little or as much of that allocation as they like. The resources that are in excess of this client are often split up in the same manner and offered to other clients. In this way, each company might have their assets sharing the same physical server with another organization.

Everything on the server stack runs within a virtualized environment, such as VMware or Microsoft Azure. Clients have access to these resources and can build and run application environments off of it. There are other models such as Platform as a Service (PaaS) which provides the computing environment pre-configured to allow customers to build applications directly without the infrastructure configuration, and Software as a Service (SaaS) such as in the case of SalesForce.com whereby an application is hosted in a public cloud and clients login via a web portal. Depending on the needs of clients, cloud providers may offer one or all of these types of services.

Does Cloud Adoption Make Sense?

While the same basic principles that apply to large enterprise organizations apply to small and mid-sized ones, there are some key differences that help identify if adopting cloud services makes sense. Firstly, while all organizations are focused on growing in size and also increasing profits, the mid-market is predominantly interested in augmenting their employee base while increasing profits (42% and 41% respectively). A service that allows for the outsourcing of a CRM tool might be cost effective over an employee base of 2000+ employees, yet on a smaller scale, the monthly operations costs might be prohibitive for a company of 150 employees. This often will depend on the pricing models used by the service provider. In some cases it is a flat fee for infrastructure, such as in an Infrastructure as a Service (IaaS) model, or it might be through a per-user licensing as in the case of Software as a Service (SaaS). Overall, the CSC Cloud Usage Index highlights that 82% of cloud adopting businesses saw a cost saving, and 64% were able to extend their green footprint through reduced waste and lower energy consumption[2].

But there are advantages that SMBs can leverage over their enterprise competition. In many cases, smaller organizations are quicker to adopt new technologies. For instance, the adoption of mobile and tablet technologies, and in some cases even an open IT policy to allow for employee-owned laptops. This means an

[2] http://assets1.csc.com/newsroom/downloads/CSC_Cloud_Usage_Index_Report.pdf

increased importance in ensuring that these devices follow a strict security policy to prevent data leakage and the introduction of malicious data into the organization's IT ecosystem. Through cloud services, the back-end systems such as email, CRM, data storage, can all be moved offsite and connected through hosted security such as SSL VPN tied with a software based authentication solution. This would convert the original capital requirements for edge security (firewall, VPN, authentication, etc) into an OPEX (operations expense allocated) based solution where the back-end solution is managed by the service provider. The local IT administrator would be responsible for minimal configuration, but not time-intensive tasks such as patching, updating, monitoring security logs or provisioning tokens. The IT cost savings could be reallocated towards other capital expenditures.

But where do you begin? The first step is to look at your infrastructure. Identify where things are located and how they are being utilized. Are there wasted resources such as a dedicated server that runs a single application that takes 15% of its overall resource pool? Are there databases with sensitive information that would cripple the organization should there be a security breach? Once all these resources and assets are mapped, then you begin to get a clearer idea of which areas of your business are suitable for cloud adoption.

Security Concerns in Cloud Adoption

There is an exhaustive collection of whitepapers available that cover this topic extensively from an enterprise perspective, yet do not cover some of the benefits that are unique to small and medium sized organizations. In fact, one of the largest security benefits of cloud adoption is more valuable to these organizations than to larger enterprises that outsource small parts of their IT environments.

Big Organization Security Practices for SMB Pricing

In order for cloud providers to pass security audits, in particular those who offer PCI certified cloud environments or whom benchmark against ISO/IEC 27001, these providers must prove that they meet the criteria for the planning, implementation, management and continuous improvement of their security operations. In multi-tenant cloud environments, where there are varying requirements of each customer, cloud providers must be able to provide an environment to customers that meet the required policies, procedures, audits and controls specific to that tenant's compliance and governance needs. In the case of SMB tenants, a cloud provider might be required to provide certified environments which meet the criteria for compliance standards including (but not limited to):

- Payment Card Industry Data Security Standard (PCI DSS)
- SAS 70
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO/IEC 27000 standards
- Sarbanes-Oxley Act (SOX)

- Patriot Act

Since the cloud provider is required to ensure these standards are met, and prove to customers that the services they are subscribing to allow them to operate under the same compliance requirements, there is an immediate benefit to the customer. Customers no longer have to independently ensure they have all the controls in place to comply with these standards; they simply have to prove to the auditor that these requirements are in place through the service provider. In the case of PCI DSS, this means a significant cost savings since the customer no longer has to purchase many of the extensive security solutions encompassed in the PCI regulatory guidelines. These can include intrusion prevention and detection tools, log management and firewall requirements. However, an important note here is that depending on the service subscription (IaaS, PaaS, or SaaS), the security controls may lie outside the agreement of the service provider. Generally speaking, in IaaS situations, there is more security requirements that fall to the customer, as opposed to PaaS, where the provider is required to cover more security controls, and finally SaaS, where it is standard practice that the service provider controls the security processes and governance requirements.

It is recommended that smaller organizations which do not have sophisticated IT security practices leverage providers that include security provisioning in their SLAs. By doing so, these smaller organizations can provide their customers with proof that there are the required security controls in place, while not having the requirement to individually purchase and provision these services. This means that from a customer perspective, these organizations would have the same controls as many larger organizations (with dedicated IT security staff) without having the expenses associated. The SLA should clearly identify which controls are in place, and provide information on audit and litigation procedures.

Benefits of Utilizing a Single Provider

Many telecommunications providers are augmenting their current services with the introduction of cloud-based services. In the Canadian market, there is an increasing availability of IaaS and hosted security and data backup services from the major telecom corporations. It makes sense for these organizations to offer these types of service as they leverage existing infrastructure such as data centres and can be bundled with network services. SMBs should consider looking at these providers as there will be a strong need for optimized network capabilities, including WAN optimization, in order to best leverage the benefits of cloud services. In addition, because the cloud and network services are hosted by the same company, there is a single point of failure in most cases. If services are spread around several providers, then there is room for compatibility issues or in the case of service interruption, a longer time to remediate as both parties need to be involved.

Larger enterprise organizations can also leverage the advice of using a single provider for network and cloud services. Although many of these companies will introduce cloud and virtual environments into their infrastructure through on-site or hybrid/public clouds, there is still a need to optimize the network to ensure the infrastructure does not suffer from inadequately sized network capabilities. In this case, enterprises can look to their network providers to offer services such as off-site data storage/recovery, WAN optimization or increased network throughput, and to security solutions which are tailored to cloud and virtualized environments. Several telecommunication providers and managed security service providers can offer audits to help create a roadmap for enterprises to migrate to virtualized infrastructures which highlights policy, governance and security requirements. This is beneficial to organizations which lack in-house virtualization or security expertise as it

pertains to a hybrid or private cloud infrastructure as there is a capability to outsource professional services to complete the project.

The third benefit for organizations that utilize a telecommunications provider as their cloud service provider is the ability to augment the cloud offerings with additional virtualized products such as virtualized PBX for voice service, or video conferencing. These services are native to telecommunications and since the back-end hosting infrastructure is optimized to offer these services, there is less risk of non-supported technology being added to the network to provide these capabilities. In many cases, the SLA provided by the telecommunication provider covers a standard level of service that protects the customer from downtime issues or service degradation that could be caused if new services were built in-house and added to the network. Additionally, the costs associated with acquiring and maintaining these services become significantly more when done in-house versus taking advantage of hosted solutions that benefit from economies of scale pricing and eliminate the need for maintenance on behalf of the customer. When you eliminate the cost of maintenance and acquisition, in many cases, services that reside in a hosted model and offered through a service provider will ultimately result in lower total cost of ownership and operational expense. It will also eliminate the need for capital expenditures associated with acquiring these solutions for private use. The organization benefits from having the latest optimized technology, without the expensive acquisition cost normally associated with an infrastructure upgrade. These costs are even more predominant for SMBs that are building out next generation infrastructures and require significant expansion to their current architecture.

With the growing introduction and adoption of cloud services, there will be a significant change to the way the traditional internal IT structure is managed and the infrastructure used. The first step of the migration will see most organizations introduce virtualization technologies to make better use of existing resources or to reduce future costs through leveraging the cost benefits associated with running a virtualized vs. un-virtualized infrastructure. For small and mid-sized organizations, the adoption of hosted cloud services can result in significant benefits that would not be achieved through standard IT environments. Specifically, SMBs which utilize service providers to offer IaaS, SaaS and network services see several key advantages including:

- Decreased need to hire IT professionals with expertise in creating and maintaining on-premise virtual environments
- Dynamic infrastructure that can be increased and decreased to coincide with unique business requirements (increased traffic during certain times of the year including end of year, reduced use during summer months, etc)
- Reduction, and in some cases elimination, of capital expenses required with purchasing new IT infrastructure to create in-house private clouds.
- SLAs that ensure minimal service levels are met at all times and provide business continuity.
- A strengthening of security compliance through leveraging the existing security controls and governance policies in place on the host site without the cost associated with upgrading these security requirements.

- Next generation services including voice and network optimization without the cost and knowledge associated with implementing on the customer site.
- Extensive professional services to help ensure a smooth migration to virtualized or cloud architecture.
- 24x7x365 support for infrastructure and services
- In the case of SMBs which utilize services from network providers, a single point of contact for all services

There is strong motivation for small and mid-sized organizations to leverage these cloud services. However, before signing with a cloud provider, it is recommended that you thoroughly examine the SLA to ensure that you are protected as a customer from clauses that transfer security and operations obligations to the end-user. In addition, research the provider to ensure that their availability of service is as stated, and that the mentioned security policies and governance processes are in place.

There are many online resources that explore different cloud offerings and providers, as well as identify in-depth the key areas of awareness for the adoption of cloud and virtualized infrastructure. It is advised that before taking on any virtualization or cloud projects, the organization identifies the end-state goals as clearly as possible in order to ensure that all objectives are met upon project completion.

Recommendations for Cloud Adoption

This last section will identify and make recommendations on key areas of importance as it pertains to cloud service adoption. These areas include service level agreements (SLAs), litigation and portability/interoperability.

Service Level Agreement Recommendations

The service level agreement (SLA) between the customer and the service provider is the single most important document when it comes to ensuring that the proper controls are in place as it relates to the customer's assets. In a cloud environment, the customer or end user trusts a third party with the possession of corporate assets that may cause significant damage if accidentally destroyed or compromised. In order to reduce the risk of negligence or unforeseeable events, it is recommended that the SLA be carefully reviewed to ensure that the customer is protected.

The SLA should include verbiage that covers at a minimum:

- Security controls (how are they securing their environment from a physical and technical standpoint? Do they have managed or monitored security in place? What is their customer notification procedure in

the case of a security event? Is there security controls on the individual servers, especially where multi-tenancy is practiced?

- What are the provider's policies for audits? Can security tests be performed by the customer, or do they need to be arranged with the provider?
- How does the provider perform regular maintenance on the infrastructure? Are there periods where the customer's assets will be unavailable?
- Are there regular backups performed to protect the customer in the event of a system failure?

These topics should at least be discussed with the provider before signing any agreement in order to protect the end user in the case of any dispute or technical outage. Until cloud adoption becomes more commonplace, we can expect to see examples of poorly written SLAs in which the provider is not held responsible for events that should normally be included in these agreements.

Litigation

While litigation doesn't seem like a particularly important topic when it comes to hosting off-site data and applications, due to the unique nature of cloud environments, it becomes quite important should any situation that requires legal involvement arise.

So why is litigation so important in cloud environments? If there is a situation whereby legal entities (government, customer or business protection agencies, etc) require access to your resources, the terms contained in the SLA will make the difference as to who has the right to grant access. In most cases, the provider has a legal obligation to provide the information to the legal body, and in the case where the cloud provider resides in another country, there may be several legal bodies involved.

Traditionally, the organization itself had full decision over whether to release, or what to release to the government or legal agency. When using a cloud service, the cloud provider may make these calls instead, and if no notice is given to the customer, this might affect the outcome of a legal decision.
It is therefore recommended, that if you use an out-of-country provider, or are planning to host business sensitive information, that your legal team review the SLA to ensure that the litigation stipulations are correctly applied to protect the organization.

Portability/Interoperability

Since cloud adoption is still in the early stages, it is critical that the concept of portability and interoperability be considered when making a decision on a cloud provider. Currently there are three major cloud platforms; VMware, Microsoft Azure and Amazon EC2. Depending on the platform that the organization chooses to standardize on, this may limit the available options should the organization have a requirement to change providers in the future. It is essential that any organizations that are planning on using outside cloud providers choose a platform that is widely adopted, and avoid creating platform specific applications that might later require rebuilding due to an obsolete back-end environment. Many providers are starting to standardize on one

platform or another, and before signing an agreement with a cloud provider, it is recommended that the possibility of changing providers be considered when selecting which platform to adopt.

Summary

While cloud computing has significant benefits to both enterprise and small-medium sized organizations, there are clear advantages for smaller organizations to adopt cloud computing models. In particular, the cost savings between cloud adoption and building in-house next-generation architecture allows these organizations to reallocate funding towards more business-critical projects. In addition, by leveraging cloud providers to outsource IT security requirements, and layering on compatible network services, small and mid-sized organizations can enjoy the same advanced services as enterprises utilize without the significant capital expenditures and staff requirements.

However, cloud services do not come without risks. It is highly recommended that before signing with a cloud provider, that organizations research the provider to ensure that they have a clean track record, have platforms that allow organizations to easily move their assets to another provider, and have clear SLAs that identify security and governance at a minimum.

As cloud services continue to evolve, there will be more standardization and regulation in these areas, but until that time comes, it is crucial that organizations who want to leverage the many benefits of cloud services be aware of the key areas of risk.

For more information on cloud, please visit the following links:

http://www.tinderstratus.com

https://cloudsecurityalliance.org/

http://www.vmware.com

http://www.microsoft.com/readynow

http://aws.amazon.com/ec2/

Andrea Bilobrk is cloud and virtualization security specialist in the Toronto area. You can visit her blog at www.tinderstratus.com.