How to Utilize
the Cloud Securely and Improve Security in an Enterprise IT Environment

Introduction

Cloud computing has been a hot topic in the IT industry for the past few years, and the perspective of cloud services for enterprises has transformed from exploration and testing to utilization and expansion. According to IDC, US$17 billion was spent on cloud-related technologies, hardware and software only two years ago and this number is forecasted to grow to US$45 billion by 2013. Currently, IDC identifies that cloud IT services are worth US$10.7 billion globally, a figure that is estimated to grow to around US$27 billion by 2013. In addition, Gartner foresees that virtualization is projected to grow by leaps and bounds in the coming years, with worldwide cloud services revenue projected to reach US$148.8 billion by 2014. None would argue the attractiveness that cloud technology brings: on-demand, scalability and pay-as-you-go which could reduce both time to market and cost of ownership. However, the issue of security remains the biggest hurdle for enterprises to fully deploy their services to the cloud. As the market and technologies mature, these hurdles are quickly being overcome, and cloud computing can actually help to improve IT security if used wisely and effectively.

NTT Com Asia Enterprise Cloud Features - Issue 1

Author:
Taylor Man
Executive Vice President, New Business Division
NTT Com Asia Limited

NTT Communications

Virtual Desktop

Desktop management has been a major challenge for almost every player in the IT space. The combination of globalization and business continuity has caused a significant increase in the members belonging to the "mobile work force" and remote offices which add to the challenge faced by desktop management. Since members of the mobile workforce require access to critical information from outside their offices while using their notebook computers, mobile devices and mobile Internet, remote offices with limited IT staff and infrastructure are faced with an enormous security threat. Common security issues include the following:

- Data leakage via lost or stolen mobile / computing devices
- Illegal information transfer via USB or other removable storage devices
- Delay or failure to install security patches and anti-virus signatures
- Direct leak from local PCs and servers within the remote office

While one of the simplest ways to manage information security is to concentrate information in a single location, members of the mobile workforce and remote offices actually help to spread information.

Virtual desktop that is based on existing virtual desktop infrastructure technology has provided a solution to help enterprises contain information security hazards by centralizing information in the provider's data center. All mobile users are actually accessing this data/information without having to download it to an end device – whether it is a mobile device or desktop computer at a remote office. The information that is transferred to and from the end device is simply the image of the virtual desktop, the key strokes and instructions to the virtual desktop. All computation work is being done over the cloud server farm in the provider's data centre. These characteristics eliminate the risk of information leaks on lost mobile devices and prevent unauthorized copying of information. All desktops are in a centralized environment and have total connectivity to all virtual desktops, and with the deployment of security patches, anti-virus signatures are ensured while other security features are consistently updated.

Management, including security, is conducted centrally in the Virtual Desktop Infrastructure environment and will reduce efforts on support and services for end devices in remote locations – greatly reducing the Total Cost of Ownership for desktop management. The virtual desktop retains the strength of cloud service while, at the same time, it decreases the time spent for desktop management to a minimum. A virtual desktop can be created within minutes without going through any sophisticated procedures for both the hardware and software.

Secure Cloud Utilization in a Server Environment

Many companies hesitate to use the cloud in an enterprise environment at the early stages of cloud development because they envision a public cloud based on 100% shared infrastructure and Internet connectivity. Many public cloud providers do not disclose detailed information on their infrastructure or even their location. This makes enterprises skeptical when choosing to deploy any meaningful services to the cloud.

Cloud services have evolved to address different type of usage. Service providers that focus on the enterprise market are now primarily concerned about security. These providers are more focused on the private cloud and hybrid cloud, which provide Infrastructure as a Service with a composite on the traditional equipment and cloud platform. Some of these clouds are only connected to private networks, whether they are MPLS IP-VPN or leased line, which highly improves security as a whole.

Cloud computers are based on shared infrastructure. Economies of scale will help cloud users reduce the Total Cost of Ownership, but some of the private and hybrid clouds have adjusted their degrees of sharing to correspond to the security concerns of enterprises. For instance, certain infrastructures such as management, monitoring and backup are shared, which in general would not cause too much of a security risk. In terms of customer data, different degrees of sharing can be accommodated to different degrees of security requirements. Customers can request that the data stored on the common storage network be segmented. For example, a storage network generally contains the following elements:

- Storage network – containing network equipment such as fiber switches
- Controller – the controlling mechanism for flow of data
- Disk chaises – enclosure that holds the physical hard disks
- Disk – physical hard disks
- LUN – logical volume to be used by the computer equipment

Traditional cloud service providers will provide storage to cloud servers and virtual machines in a big LUN or, at most, dedicated LUN which may mix different customer data in different logic or physical layers. Some providers can offer segregation of the SAN unit in differ layers, which means providers can give customers a dedicated LUN or disk or even chaises according to the level of security that the customer has. On the network layer, logical or physical separation can also be provided according to customer demand. In terms of operation, most of these cloud providers are equipped with certified industry security standards such as ISO 27001 or SAS 70 and transparent policies to ensure that all customer operations are done appropriately.

Since cloud computing is about the economy of scale, providers are getting the scale by aggregating hundreds or thousands of servers in their server farms. Capacity can also be shuffled between different private clouds on a sudden surge of usage. The usage predication of the enterprise is much more logical compared with the Internet community, and Service Level Agreement (SLA) can also be given by the provider with pre-defined requirements. The SLA and turnaround time offered by cloud providers will always be better than the traditional self-built solution.

When and How to Use the Cloud

How much and what to put on the cloud will always be up for debate. Most companies will begin their experience with the cloud during internal development and staging, which is not a bad idea. On top of that, a mix of private clouds that hosts desktop and servers can help to reduce cost on seasonal hiring, shift the working environment and short-term remote office and deployment time. Regional and global cloud providers that allow users to choose location and shift their cloud infrastructure within different geographic locations can help IT managers to manage multiple locations. For a company that has already deployed virtualization services, using a cloud service provider's CPU to handle CPU surges as a result of marketing campaigns, seasonal events or even periodic services such as payroll is an option. Applications also exist that can be designed to require the execution process to be handed over to the vendor's cloud platform while relevant data would stay within the company LAN – addressing many security concerns. Using a cloud service to deploy a disaster recovery plan would also be ideal since the backup infrastructure will not be used frequently, but needs to be fully ready when needed.

There are improvements added to cloud services which let enterprise users benefit from the cloud while not forfeiting security concerns. Some of the new developments to the cloud would even help IT managers and CIOs to manage security issues of their teams / companies more effectively. Now is the time to seriously consider adopting cloud in your enterprise IT environment and jumping on the cloud bandwagon if you are not already on it.