Are enterprises really ready to move into the cloud?

By Sichao Wang

Many businesses are interested in finding out how they can benefit from the cloud computing hot wave. Cloud based services such as Saas, Paas and Iaas, are supposed to bring in customer the benefits including economies of scale, on-demand and cost savings. The pay-per-use model is really attractive, because it means companies can plan for the future without huge initial investment on the infrastructure.

But many enterprises are also concerned. A survey in 2010 by IDC shows that majority of the Fortune1000 companies will not adopt public cloud storage for storing their data, at least for the next couple of years; 75% of the surveyed businesses are concerned about the reliability, security, availability and the control over their own data in the clouds;

For example, business customers are concerned how their data is segregated if their data is stored on the same physical media shared by other businesses. Would data stealing malware craw from one tenant to another tenant, from one virtual machine to another virtual machine, from one virtual storage to another virtual storage? How is customer data privacy preserved in this environment? Some customers are also concerned how they can "move" their data out from the cloud back to their private data center, should they decide to keep the data really in premise. Similarly how could business customers move their data from one cloud service provider to another cloud service provider's hosting environment, should they become disappointed with their current provider?

Of all the concerns, one of the most important considerations is SLA. CSPs (or cloud service providers) need to implement a meaningful performance management system so that cloud service providers can prove that their cloud service delivery infrastructure has fulfilled the contractual service agreement, in terms of application response time, bandwidth allocations and security activity monitoring as well as recovery time over outages etc.. The Amazon and Sony outages in 2011 are examples that how vulnerable cloud service infrastructures are today, and how much business pains that can cause to customers. The outage came on the same day that Amazon’s cloud-based web services business went down, affecting lots of businesses relying on AWS and S3 including Reddit and Quora etc.. It also shows how immature the cloud-based services are, how risky to rely on a single cloud service provider.

Unfortunately, for many of these concerns, there are no standard procedures defined by industry associations or regulatory agencies, which are partially the reasons that serious businesses are slow in adopting cloud based services.

The implications of cloud computing on audits and compliance are also depressing. Laas service providers must produce evidence (or by third party compliance/audit vendor) that one customer can not access other customers resources (storage, web server and etc.) physically or electronically. Customers can only have the access to view and control over their data and system status. Audit and logging trails must be uniquely associated with a specific customer with unique ID; CSP must define policies allowing customers or third party venders hired by customers to perform compliance and audit, as well as forensic investigations.

Cloud computing brought in the complexities that often are overlooked because of the monetary benefits. The pressing needs for integration, monitoring and management of cloud services,
cloud applications with the traditional security infrastructures (firewall, IDS/IPS, UTM, and IAM etc.) are on the way.

Cloud computing even creates confusion on the service providers' relationships, and hence the liability and transfer of legal liabilities. For example, as depicted perfectly by the book "Security 2020" (authored by Doug Howard and Kevin Prince), a SaaS provider could host their applications on the infrastructure hosted by another IaaS providers, which may hire another managed service provider (MSP) on operations and maintenance. In case of outages, data breaches, who are responsible for what?

In summary it is apparently compelling that the cloud computing industry forums need to define the standards and procedures for security, privacy, data moving and service recovery, in order to boost the public confidence on the cloud. Without necessary regulatory and industry standards, the acceptance of cloud based services, would be still "cloudy".