Cloud Computing – Bright or Stormy?

Solutions to successfully meet the requirements of business continuity.

Kroll Ontrack.

An Altegrity Company

Introduction

Ask the average computer user to describe cloud computing and chances are you will get a blank look or a chat about the weather. Marketing has succeeded with informing Internet users of the existence of cloud computing, yet few users can explain what the cloud represents or what it means to them. Virtually all Internet users have been introduced to cloud technologies without being aware of it. Have you used a photo–hosting Website? You've used cloud storage. Are you using an interactive social media site or office applications from a Web browser? You're using cloud software.

The cloud computing industry has entered the formative years and is now able to provide solutions for organizations looking to keep new technology investments and costs low. Virtualization technology, or software that emulates computer hardware, provides the foundation for all of cloud computing's service offerings.

Cloud computing offers three services: Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Cloud infrastructure as a service (IaaS) is the most established of the cloud service offerings because it allows organizations to use only what they need for computer system requirements; for example, IaaS allows customers to have access to offsite, virtualized computers without having to pay the associated hardware costs or facility expenses.

SaaS is the most accessible of cloud service offerings because it provides full application functionality through a Web–based interface. The number of applications that have been developed for Web browsers is amazing. For example, there are complete office productivity applications that are available through only a Web browser and an Internet connection.

PaaS is targeted at rapid application development and leverages the two previously mentioned cloud services. Think of PaaS as the intermediary between SaaS and IaaS; this cloud service may be closer to adoption than was previously thought[1] because it will enable more SaaS functionality.

Gartner Research reports that the adoption of cloud infrastructure as a service (IaaS) is beginning to gain traction in the marketplace. Gartner predicts $3.7 billion USD worldwide for the cloud market in 2011 and $10.5 billion in 2014; an astonishing increase in market adoption over the next three years.[2]

Consumer acceptance of cloud services via mobile phone applications demonstrates that the technology is delivering an economic model that more companies are investing in. According to comScore, Inc., a digital business analytics company in the U.S., 69.5 million people own smartphones in the U.S. and as of late 2010 almost half of those users accessed their bank, credit or brokerage accounts through their mobile devices.[3]

> SLAs and contractual obligations may not provide cloud users complete protection in the event of a business disruption. Equally risky is not having a data recovery clause included in a cloud provider contract.

The Cloud – Designed to Weather a Storm

Jason Baker, chief technology officer at Visi, Inc., a data center hosting and IaaS service provider, reports that cloud technology is "designed to handle failure" through its inherent redundancy and distribution design. Baker explains that

---

[1] http://www.businesswire.com/news/home/20110314006630/en/Gartner-2011-Year-Platform-Service

[2] http://www.businesswire.com/news/home/20110407005575/en/Gartner-Maps-Rapidly-Evolving-Market-Cloud-Infrastructure

[3] http://www.comscore.com/Press_Events/Press_Releases/2011/4/comScore_Reports_February_2011_U.S._Mobile_Subscriber_Market_Share;
http://www.creativedepartment.com/news/mobile/use-mobile-banking-apps-rose-sharply-fourth-quarter-183600

"traditional application deployment…was on the Web server, the application server and database server. Cloud computing removes all of that and allows organizations to focus on either the Web-facing or application layers." The physical layer—the hardware—is provided by virtualization technology.

As the demand for the cloud increases, cloud services and applications will become commoditized. Yet the staying power of the provider and their reputation is what will stick with cloud customers. "Trust is essentially what will carry cloud service providers through the next few years," says Harold Moss, chief technology officer of IBM's cloud security strategy, "the service space will grow and then it will thin out. Only those providers that are offering complete solutions now will be the ones standing in the future." Moss relates how service providers may dilute their solutions by outsourcing their own services to another service provider in an effort to stay price competitive. This turns into a "compounded service level agreement," Moss says, and the overall provider's service is devalued because it too has used the cloud to deliver computing resources. Each of those SLAs becomes reliant on another provider.

> As the demand for the cloud increases, cloud services and applications will become commoditized. Yet the staying power of the provider and their reputation is what will stick with cloud customers.

When it Rains in the Cloud

Adherence to compliance, security and accountability governance policies are expected of cloud providers. Unfortunately, certificates and audit assessments do not reveal how a cloud service provider will respond to a business disruption.[4]

Stormy weather in the cloud can be disastrous for end-users, as exemplified by the events an IT service provider in Canada experienced. The service provider had a NetApp® 40TB Filer appliance that contained virtual LUNs, or iSCSI files at the NetApp volume level. Inside of those iSCSI files were VMware® ESX volumes. The ESX volumes contained the virtual disk files for servers of both the IT service company and some customer's IaaS virtual machines. The tempest facing this company was not external but internal.

A disgruntled employee issued the "Delete Volumes" command at the storage unit level. This particular storage unit employed NetApp's block snapshot technology and this alone would have saved the data if the rogue employee had stopped there. Unfortunately, this employee knew how the Filer's snapshot function worked. The Filer's system clock was set back one hour right before deleting the NetApp volumes so that the snapshot replication copied the empty volume metadata. After the damage was done, the employee reset the Filer's system clock before exiting the company's data center. The NetApp Filer continued to take volume snapshots, as scheduled, filling the entire snapshot list with empty blocks. When other administrators discovered the disaster, there was no valid recovery point to go back to.

This disaster moved into full category storm status because not only were some of their customer's IaaS systems gone, but the service provider didn't even have its own operational data. Worse still, there were no relevant backups of any original data.

This particular service company had promised a 99.99 percent uptime for its data center and large Tier-1 Internet connections. During the whole business disruption, uptime and lightning-fast connectivity were maintained, thus meeting their stated SLAs. As customers of this cloud service soon discovered, system uptime and connectivity are not the same as data availability.

---

[4] For purposes of this article a business disruption is anything that prevents day-to-day work from being done, including power disruption, downed phone lines, and so forth. Data loss occurs when data is corrupted or inaccessible. Hence, data loss is a subset of business disruption.

The Canadian IT company was forced to engage a data recovery service provider to recover its own data and its client's IaaS virtual systems as well. During this business disruption, the company worked hard to take care of its customers. However, some customers were informed that if they had not purchased additional replication or did not have a backup of their data, they would need to purchase their own recovery through the same data recovery service company. This was a shocking realization for customers who assumed their SLAs included data availability.

This example illustrates that SLAs and contractual obligations may not provide cloud users complete protection in the event of a business disruption. Equally risky is not having a data recovery clause included in a cloud provider contract. Overconfidence that storage equipment will be self–healing or 100 percent redundant is naive and cost–prohibitive. Synchronous data replication is expensive and does not prevent the results of human error or malicious data destruction.

Have an Umbrella for the Cloud

Storms broke in the early part of 2011 causing outages for some of the biggest names in cloud service.[5] These storm cloud events were unrelated to each other; however the disruptions resulted in downed or disabled websites, affecting Internet users. Subscribers of these services were met with the message, "This service is temporarily unavailable." Because cloud services are relatively new, a customer may not realize the limitations of an SLA contract until a business disruption occurs. For example, what compensation or credit does the SLA provide due to an outage, or how will the cloud provider's recovery procedure restore the missing services? Cloud customers may realize too late that they require more resiliencies from their cloud contracts.[6]

Cloud providers without in–house or third–party recovery specialists available to assist in resolving the business disruption are not providing an expected level of trust to their clients. During an outage, all IT hands are on deck, working feverishly to restore services, replace equipment, restore backups, and perform root cause analyses and other investigative tasks associated with management's need to understand what triggered the event. Cloud providers that attempt to keep everything in–house quickly discover that an already burdened IT staff nears the breaking point during an outage.

A cloud outage can result from network failure, hardware replacement, a network attack from the outside, or a software bug, to cite common causes. Additionally, despite advances in data storage technology, data loss occurs in the cloud and can contribute to an outage. Data recovery service companies get data back from storage devices that have failed, have been mismanaged through human error, or have even been victimized by outright sabotage. However, data recovery service providers are not directly tied to the storage–to–consumer supply chain. Recovery services are used by storage consumers only after they have lost access to their data. No one really believes that a storage failure or data loss will happen to them. Yet, when it does, a cloud provider (or client) that did not fully backup their data immediately before the disaster can work with a data recovery service company to get that original data back.

> System uptime and connectivity are not the same as data availability.

---

[5] http://www.computerworld.com/s/article/9216064/Amazon_gets_black_eye_from_cloud_outage, http://www.pcmag.com/article2/0,2817,2384214,00.asp, http://www.computerworld.com/s/article/9211798/Update_Google_Gmail_outage_leaves_thousands_of_users_without_e_mail_, http://news.cnet.com/8301-31001_3-20046091-261.html

[6] For purposes of this article a business disruption is anything that prevents day-to-day work from being done, including power disruption, downed phone lines, and so forth. Data loss occurs when data is corrupted or inaccessible. Hence, data loss is a subset of business disruption.

The virtualization technology of cloud storage adds yet another complex layer to the data recovery process. Due to the dual file system layout of both the host server and the virtual computer system, data fragmentation is doubled. As previously stated, virtualization technology enables cloud services and provides incredible flexibility for scaled growth. The storage layer can become a weak link because virtualization is so heavily relied on. The best umbrella to have when adopting cloud technology is to require your cloud service provider to partner with a reputable, full-service data recovery company. This will minimize downtime caused by data storage failures.

This goes beyond having offsite storage or asynchronous/synchronous replication, or tape backups, in the SLA (which all cloud providers should provide, at a minimum). A cloud provider that has partnered with a reputable data recovery service provider is demonstrating that data availability is more important than system uptime or accessibility. A cloud provider that has partnered with an enterprise–level data recovery company is building a client's trust in its service offering by having a complete business continuity plan to protect the subscriber's data.

Data recovery is only one aspect of the cloud computing discussion. Data destruction is equally important.

Understanding what happens to your data when the cloud contract ends is part of researching cloud providers. Large data centers will have OEM service contracts to maintain the storage equipment and have failed drives destroyed or degaussed before leaving the secure environment. It is easy to assume that deleted data will be quickly overwritten by the endless write operations of subsequent storage. However, complete data destruction requires that specific client files go through an erasure process. This is where sensitive files are overwritten with pseudorandom data and then deleted from the volume.

Nothing but Blue Skies in the Cloud

Having a clear forecast for your cloud strategies requires seeing all of the obstacles. Some of those obstacles will be from the service provider and others will be from the project strategy and budget. Knowing where the service provider's provisions end and where your data protection arrangements start is vital keeping your infrastructures or applications available for your customers.

Kroll Ontrack recommends these considerations to keep your company's skies blue.

The Technical Tornado – Considerations	Why This Matters
• Do the backup systems and protocols meet your own in–house back-up standards? • Does your cloud provider have a record of technical reliability to cope with your needs?	Suspect hardware, fragmented files and inappropriate RAID levels, for example, can compromise data availability.
• Is your data stored on reliable storage systems? • Are the different types of data and applications managed appropriately? • Does your cloud vendor have a data recovery provider identified in its business continuity/disaster recovery plan? • In instances of data loss, it is imperative that a rapid response procedure is adhered to. • How does the vendor prove they comply with data retention laws? • What are the service level agreements with regard to data recovery, liability for loss, remediation and business outcomes?	Waiting to find out how the cloud provider handles these questions may be too late for you to react to downtime. Do not assume that additional SLA equates to data loss. If the cloud provider does not have a data recovery partner, find one that does.

The Prevailing Wind of Security – Considerations	Why This Matters
• How secure is your data? What measures does the provider take to reduce the risk of a data breach? For example, is the data encrypted? • Do you know who within your company and the cloud service provider can access your data? • What are their security clearances?	Your company employs industry practices around data security, including employees. Understanding how your cloud partner manages their staff and data will help in choosing a service that closely matches the policies you already have.
• Data ownership – Do you still own your data once it goes into the cloud? • Do you own it once it leaves your possession? • Is end-of-life data erased and degaussed from all hardware, who certifies that it has been deleted, and has it been erased to your country's specific erase standards?	Recent debate over one popular social media site's security suggests that the question is worth a second look.

Navigating the Legal Fog – Considerations	Why This Matters
• Does the cloud vendor retain data in line with your company's corporate document retention policy? • Will the cloud provider offer assurances that it will comply with data protection regulations? • In case of litigation or an investigation, will you or your external e-discovery provider be able to access and either extract or preserve all electronically stored information?	In the case of e-crime, or a data breach, forensic investigators will secure all of the storage and that may include your data. If data is shared between cloud services, this may complicate the investigation and leave you and your customers without any access to storage or applications.
• Where exactly is your data stored? • Is it virtualized with data from other companies? • Where is the data center geographically? • Will the data be stored in jurisdictions that subject it to subpoena by third parties? • If you terminate a cloud relationship can you get your data back? What format will it be in? • How can you be sure all copies of your data are destroyed when the contract ends?	Multi-tenancy can pose issues for data recovery and the production of data in litigation or investigations, while geographical considerations are also important as data retrieval delays for recovery or collection can be exceptionally costly. You are responsible to your clients for protecting and maintaining their data—not the cloud provider. Understanding and overcoming the obstacles will prevent legal disasters.

Kroll Ontrack.

For more information, call or visit us online.

800.872.2599 in the U.S. and Canada

+1.952.937.5161

www.krollontrack.com