Five Key Considerations for Selecting Cloud Recovery Services

Looking for a cloud-based solution for backup and recovery? Here are some important things to keep in mind when interviewing providers.

By Massimo Mauro, Solution Architect, Cloud Compute and Managed Hosting Services, Allstream

SUNGARD® AVAILABILITY SERVICES™

allstream™

cisco Powered

FIVE KEY CONSIDERATIONS:

- Business Impact Analysis
- Continual Updates to Business Continuity Plan
- Tailoring the Cloud Recovery Service
- Service Level Agreements
- How does a cloud provider guarantee RPO and RTO times?

Technology has added tremendous efficiency to how we work, communicate, learn, shop, and a myriad of other things. But when the electricity goes out or the network goes down, we're immediately aware of how dependent we are on network services and applications. For businesses, the speed with which networks come back online and the amount of data that is lost when network connections are inaccessible can mean the difference between losing or retaining customers. It can also cost businesses significant amounts of money in lost business, penalties issued by industry regulators, and incalculable amounts from tarnished reputations.

As more businesses recognize just how vulnerable their networks, applications, and data are, backup and disaster recovery initiatives have risen to the top of IT agendas. Cloud service providers that deliver backup and recovery as-a-service in the cloud have seen a corresponding increase in business. Why? Because many customers recognize that it's much more expensive to provide business continuity themselves. Businesses that contact providers such as Allstream have a general idea of how they want to use backup and recovery services. Here are some items that should be part of an evaluation of a cloud-based backup and recovery service.

Business Impact Analysis

It's natural to focus on your most treasured assets first when looking at a backup and recovery service. For retailers, that is often the Web site and ordering system. For manufacturers, it might include various process and logistics systems. For financial services, transaction systems used by customers and employees would probably be the first area of focus.

But cloud providers that specialize in backup and recovery will suggest performing a more comprehensive business impact analysis that looks at other areas beyond mission-critical systems and applications because there are often other infrastructure and assets that interact with mission-critical ones and will impact the performance of backup and recovery solutions. Examples include an order processing system that might be part of a larger ordering application or an independent system that has yet to be identified.. Other assets that relate to a reliable and dependable backup and recovery solution might include the availability of electricity in the event of a disaster. I've spoken to companies that acknowledge that they have a backup generator for redundant power. But when asked if they have tested it, they admit that they haven't and have no periodic testing scheduled. And they don't know how long the run time will be.

© 2014 Cisco and/or its affiliates. All rights reserved.

These are examples of factors covered in a comprehensive business impact analysis report, how they impact backup and recovery services, and why it is so important to complete this in-depth analysis. The analysis would include such things as the Data Centre Tier Classification System: I, II, III, IV, as introduced by the Uptime Institute. Tier IV representing the highest level of availability.

Continual Updates to Business Continuity Plan

Once you have your business continuity plan in place, it shouldn't be set in stone. If you're like most businesses in the 21st Century, your environment is changing all the time. So the business continuity plan must be continually updated to align with the business design and requirements. Testing is also critical to make sure that backup and recovery processes work flawlessly. With testing, we've found that key factors arise that are missing from your run-book and failover processes. These might include configuration changes on a server, the decommissioning of or changes to an application, or the change from one service provider to another.

Failure to keep your business continuity plan up-to-date can mean the difference between success and failure of backup and recovery services.

Tailoring the Cloud Recovery Service

In the past, there wasn't a lot of flexibility and customization in backup and recovery services. Today, we base our services on two different metrics: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is defined as the duration of time and a service level within which a business process must be restored after a disaster. RPO is the maximum allowable period in which data might be lost due to a major incident. The RPO is not a direct measure of how much data might be lost.

For some businesses, RTO must be as short as possible. Companies that depend on orders or exposure on the network (e.g., financial institutions, retailers, media companies, entertainment companies) will want a very short RTO. Other businesses may be able to trade a lower cost for an hour RTO or even longer.

Likewise, reduced RPOs are more costly to ensure minimal to no data loss. Most companies can assign different RPOs to different tiers of applications. They often reserve shorter RPOs for mission-critical applications that might also be subject to industry data and application compliance regulations. They'll use longer RPOs for operational or back office applications that can sustain some data loss without catastrophic impacts on the business.

The costs for a cloud-based backup and recovery service can be calculated once RTO and RPO numbers are assigned for network resources and applications. An experienced provider will guide you through this process with questions that will produce the right service level agreements (SLAs).

Service Level Agreements

One thing to keep in mind about SLAs: Most cloud providers don't offer them on recovery services. There may be language that sounds like a SLA but if you don't see a guarantee based on specific RPOs and RTOs, then the guarantee is vague and open to interpretation.

© 2014 Cisco and/or its affiliates. All rights reserved.

How does a cloud provider guarantee RPO and RTO times?

Experienced, professional cloud providers continually audit and test their data centers and their own processes to ensure they can back their SLAs with demonstrated service levels. Many things go into ensuring a reliable, world-class backup and recovery service in the cloud, including:

- **Operational excellence** based on a variety of industry certifications (including ITIL v3 & ITSM standards; ISO-20000-1 certification, which audits how a cloud provider delivers IT services — formerly ISO 9000-2001 a manufacturing standard—SSAE 16 Type II audits conducted annually to look at physical controls, security, and project management; FISMA-NIST; and facilities built to support regulatory requirements such as PCI-DSS and HIPAA).
- **24/7 support** that combines industry best practices, robust help desk tools, and extensive technical and engineering expertise.
- **Service desk** with dedicated support staff that can handle communication on technical issues, change request processing, internal and external problem notifications; and use a Service Now Portal Ticket System for resolution and escalation processes.
- **Portal** for use by customers that provides access to essential information, such as infrastructure performance, problem and change activity, account information and more.

Where do I start?

For those of you who are embarking on a cloud service for the first time, where should you start?

First, have you formulated an overall cloud strategy? Have you had a bad experience with cloud services or a cloud-based application? Are you already locked into a vendor agreement? These are important questions to answer before you look for a cloud vendor.

Another variable to consider: Do you want backup for both physical and virtual infrastructure? Many cloud providers can't backup both effectively. The more experienced, professional ones can.

Look for a true turnkey service. Some providers give you access to their data center resources and you must hire a developer to use the APIs to create a backup solution that connects to the cloud provider's storage. The cost may be low but once you factor in your own operational costs, this partly do-it-yourself approach using a provider's cloud can be extremely time-consuming and therefore expensive as well as problematic.

Larger cloud providers will have many data centers and will be able to offer geographic redundancy thousands of miles away from the primary data center. This offers peace of mind but it is important to verify if regulatory compliance requirements that your business must adhere to specify data backup restricted to the same country.

© 2014 Cisco and/or its affiliates. All rights reserved.

Massimo Mauro is a Solution Architect with more than 15 years of data centre and hosting experience, including many years as a consultant. He has worked on various technology platforms and heterogeneous environments, serving enterprise to mid-sized companies. Currently he specializes in hosting and cloud infrastructure and recovery and business continuity services for Allstream.

Allstream is the only Canadian-owned national communications provider that works exclusively with business customers. They provide voice, data and Internet services guaranteed to make a difference in how your business operates, helping you manage costs, improve collaboration and ultimately increase productivity. All Allstream services run on our secure national network, built and managed using advanced IP and fiber technologies.

Backup and recovery in the cloud from Allstream is based on the world-class Recover2Cloud® solution from Sungard Availability Services. Recover2Cloud is among the few recovery service for applications on an enterprise-class cloud infrastructure with guaranteed SLAs. Customers have reported up to 70% savings over DIY solutions and the use of a cloud environment for recovery can save an additional 30-50% compared to recovering on physical systems. What differentiates Recover2Cloud for competitive solutions? Recovery for both physical and virtual environments. Strict adherence to SLAs. Data centers based on the industry-leading Cisco Unified Computing System converged infrastructure, EMC vStorage arrays, VMware virtualization technologies, and VCE Vblock Systems. And Sungard has the capacity and expertise to recover a wide variety of IT environments, including legacy mid-range and non x86 systems. Sungard was recently cited as a Cisco partner in the creation of the world's largest global Intercloud – a network of clouds.

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)