TECHNOLOGY ASSESSMENT

The Opportunity for and Challenges with Continuity in the Cloud

Laura DuBois          Eric Sheppard

IDC OPINION

Firms are investing on various forms of backup to the cloud with the expectation these services provide for continuous data access (and perhaps even application access). Despite this perception, backup to the cloud does not provide for business or application continuity because most services only provide data protection and do not provide compute, application, or networking services. Recovery in the cloud is an excellent step up from backup to the cloud, but still requires a recovery process although it can be accomplished in minutes. The highest level of availability is continuity in the cloud. This IDC study highlights several scenarios available to attempt to achieve continuity in the cloud and the challenges firms face with trying to gain higher levels of business, application, and data continuity. In addition:

- Achieving continuity in the cloud requires the application of different technology and introduces an expanded set of service provider requirements.
- A nascent yet emerging set of solutions are coming to market to provide early forms of continuity in the cloud.
- Several technical and operational challenges surface in trying to achieve continuity in the cloud.
IN THIS STUDY
This study looks at the opportunity for continuity in the cloud and identifies key players that are early movers in this market.

SITUATION OVERVIEW
Business continuity and disaster recovery are terms often used interchangeably. However, they are quite different in terms of service-level objectives (SLOs) and the underlying infrastructure technologies used to achieve those SLOs. At the crux of the distinction between the two is the difference between a failover process and a restoration process. A failover process is the capability to automatically switch over application processing to redundant or standby compute resources in the event of a failure or termination of an active application. Failover may occur automatically or can be initiated manually once a "disaster has been declared," which is called switchover. When business operations resume to normal, a failback is initiated, which will synchronize the two systems.

Conversely, a restoration process (also referred to as data recovery) requires that a backup or copy of data (and perhaps the system itself) has been made. A restoration process requires access to a new server and storage capacity. The new server must have the right backup software to enable the copying of data to it as well as the applications to actually make use of the data. While failover operations are measured in seconds, a recovery or restoration process can take hours or days depending on the environment and configuration. Business continuity, as the name implies, means continuous business operations. Given the state of infrastructure technology today, those processes in the restore category do not provide this level of business processing and operational uptime.

In summary, there are distinctly different technologies that perform continuity versus recovery operations, and they have varying infrastructure requirements. Moreover, not all applications and systems require business continuity as measured in a return-to-business operations and processing in seconds. Best practice is for a firm to tier its applications based on availability, performance, and recovery objectives. Typically, the more mission critical an application is, the more it would rely upon technologies that enable business continuity. With the profound reliance that businesses of all types have on information and information technology to produce revenue, serve customers, communicate with suppliers, and the like, business continuity is of increasingly paramount importance.

What's Changed?
Business continuity was the purview of only the largest enterprise firms because of the infrastructure cost required. Material cost components included remote datacenters, networking bandwidth, software licensing, and hardware infrastructure. Small enterprises, midmarket, and SMB accounts had to rely on server reimaging and data restoration from backups as a form of business continuity to reconstitute an application environment. If the problem was localized, existing on-premise hardware
infrastructure might be leveraged. However, in the case of a site-wide problem, these firms required a remote site where IT operations could recover to. This is where DR service providers such as SunGard, Comdisco, and IBMGS offered different levels of disaster recovery including cold, warm, and hot DR services offerings. These services were also quite expensive as they were standby hardware infrastructure allocated either to a dedicated customer or to groups of customers. Customers paid the service provider to hold, leverage, and configure the infrastructure to restore a customer's primary systems, if needed. The highest level of service, a hot disaster recovery option, was the only one that really enabled business continuity. Alternatively, large companies provided their own internal disaster recovery capabilities, in which different regional datacenters could provide warm standby sites, where data recovery and application restart could take place.

**Legacy DR Service Provider Options**

Cold disaster recovery was the least expensive in that it did not have hardware, infrastructure, or configuration immediately available. Upon disaster, the infrastructure would need to be built by leveraging standby equipment and some form of local backup. However, with a cold DR service, providers would have electrical, environmental, and telecommunications services available. Often a concern for firms relying on a cold DR service was, in the event of a regional disaster, they would be among one of many firms queued up in a rebuild process. That is a major reason why the larger firms decided to provide their own, internal, recovery capabilities because they could avoid contending with other organizations regarding priority of restart of key applications and databases.

Providers offering warm disaster recovery would have the necessary hardware infrastructure configured in a standby mode and ready. The equipment would be configured in the same manner as in the production site with the necessary applications, operating systems, file system configurations, and so forth but might require a data restoration process.

Hot disaster recovery had everything required for failover of operations from a production site to the DR site. This scenario not only had all the infrastructure, applications, and configurations but also had the data required, by relying on replicated data. A hot plan relied on some form of continuous replication process to replicate data (and configuration changes) to the remote site. A hot disaster recovery site and plan did provide for business continuity. In the event of an outage, users could be redirected to the application, compute, and storage services running in the DR site.

**New Technologies and Cost Reductions**

Today, new technologies such as virtualization and the encapsulation of applications within virtual machines (VMs), as well as shared infrastructure and cloud services, have changed the landscape for achieving business continuity. Virtualization and cloud services provide the compelling components to make business continuity for a broader set of applications and users more viable. At the same time, IT and LOB organizations are facing pressure to provide higher levels of availability for critical tier 1 systems because of the increasing importance of data and information in running
the business. Continuity in the cloud is an opportunity on the horizon that can help businesses mitigate the legacy challenges of cost, complexity, and dedicated infrastructure traditionally required to achieve business continuity.

Important elements of technology that will contribute to the expansion of continuity into the cloud are:

- **Shared infrastructure.** While the old model of continuity required dedicated infrastructure, today both server and storage virtualization enable the sharing of infrastructure across organizations, departments, and businesses. The leveraging of shared infrastructure allows for the amortization of hardware cost across a pool of organizations with similar performance, availability, and continuity objectives, thus enabling price reductions without commensurately increasing risk.

- **Network bandwidth.** Costs for network bandwidth between a primary production site and a remote datacenter continue to trend downward. During networking service renewals, firms can typically upgrade network bandwidth for nominal differences in pricing. Moreover, IT efficiency technologies like deduplication, compression, thin replication, and network optimization services make leveraging bandwidth more optimal.

- **Virtualization.** Server virtualization enables the encapsulation of an application workload inside a file, which can then be moved among a pool of servers. In addition to moving the workload itself, the disk file associated with the storage LUN for the virtual machine can also be moved. Thus, the virtual machine and its data can be moved from one datacenter to another, in response to different events, providing a component of business continuity. Often, critical applications and production data can be moved prior to any disaster taking place, during a period of planned migration for those workloads — and their safekeeping at more than one primary site.

- **Cloud services.** Service providers can leverage shared infrastructure, increased network bandwidth, and virtualization to provide a cost-effective, IT-efficient way to offer recovery (or continuity) in the cloud. Cloud service providers can provide a shared remote datacenter environment and shared infrastructure to either failover or stand-up application and data services for customers.

**Cloud Scenarios to Consider**

**Backup to the Cloud**

There are a myriad of different online backup suppliers offering public cloud backup services for both consumers and commercial businesses alike. In this scenario, a backup agent is typically deployed on on-premise servers that hold data to be backed up. Data associated with on-premise systems is backed up to hosts in the cloud. Some online or public cloud backup services will store the data in the cloud in native file format, meaning there is really no restoration process required. Instead, users or administrators can browse for files and copy them back as needed. Other services will encapsulate the backup into a proprietary format for additional functionality. This
requires a local instance of the backup application in order to perform a restoration of
the data that resides in the cloud. A full restore of data from the cloud back to an on-
premise compute environment is dependent upon network speeds.

However, both options do provide server or application resources, which may not be
available in the event of a disaster. These services merely copy your data to the
cloud, requiring the user to establish or re-establish compute and application
services. Some service providers offer a bare metal restore (BMR) or system
recovery option whereby the server operating system application executables and
data are all encapsulated in a backup image, in which case, recovery or restoration
will lay back down the entire server environment. The benefit here is in the ease of
the recovery process. However, BMR images are larger and require updates to
accommodate a server’s configuration changes. BMR process still requires compute
power for the image to run.

Recovery in the Cloud

With the advent of virtualization, service providers can now leverage virtual servers
and use a configuration management tool (e.g., Puppet) to provision the servers with
the appropriate software. Some suppliers have implemented some unique methods to
integrate with virtual machine environments to quickly stand up a master virtual
machine image. Then, the backup image can be restored to the new virtual machines.
The time to recover is dependent upon the time taken to commission the new virtual
servers and perform any data transfer/restore from backup. Database/file replication
techniques can help reduce the time to recover. And restore is done locally within the
service provider location so that copy functions occur at LAN speeds.

However, this scenario of recovery in the cloud is typically offered as a service
engagement. And the process is still a recovery process, not a failover process.
Some may call this continuity in the cloud, but if continuity is measured in seconds
and makes use of HA functions such as failover or switch over, this approach will not
meet those expectations. Nonetheless, recovery in the cloud is an order of magnitude
faster and less expensive than traditional DR and business continuity scenarios,
respectively. Recovery in the cloud would very likely be considered good enough for a
large set of customers and application workloads.

Early Forms of Continuity in the Cloud

For continuity in the cloud, there are preconfigured server instances, either virtual or
physical, in the cloud running the business-critical systems combined with data
replication. In the event of a disaster at the primary operating location, the systems
are failed over to the cloud instance (this can be manual or automated). Continuity in
the cloud requires that the application be failover aware. Additionally, a combination
of failover and data replication services needs to be instantiated. Within the cloud, the
provider is ideally leveraging shared, virtualized infrastructure at both the server and
the storage layer. Continuity in the cloud is being offered by several constituents in
the industry including those discussed in the section that follows.
Cloud Supplier Types

Traditional hosting, IT, or DR service providers have taken their legacy architectures and services and re-platformed them to drive reduced cost and price for business continuity. These suppliers have historically offered business continuity services utilizing a dedicated infrastructure, and thus these services have been cost prohibitive for a large number of firms. These suppliers have had to transform their operating model for a 1:1 dedicated infrastructure to a shared infrastructure model. They also need to build or leverage a cloud services platform for components such as billing, chargeback, and customer portals.

Another category of suppliers are those offering Web services or SaaS pure-plays targeting continuity in the cloud with a new set of services. A number of these suppliers have focused on SaaS-based services for email, including security, archiving, and continuity. For example, Dell MessageOne and Mimecast both offer a range of services, including continuity, for the email application and data. Here, the service and the data are managed by the SaaS service provider that typically runs its own datacenter and manages its own infrastructure.

Last, there is a new breed of continuity service providers (that may use cloud wholesalers). These are emerging service providers such as Zetta, Geminare-powered MSPs, and Doyenz that are starting to offer various levels of recovery or continuity in the cloud. There are two predominant methods for recovery and/or continuity in the cloud. The first will leverage or rely on backup images and standby infrastructure, while the second will rely on continuous replication and active infrastructure.

Cloud Recovery/Continuity Solutions in the Market

Doyenz ShadowCloud

Doyenz is a privately held software company that has developed cloud-based disaster recovery services designed to improve the efficiency and reliability of IT services. By converting the clients' server images to a network of virtual machines on demand, Doyenz offers its customers cloud services such as automated disaster recovery and failover, testing of every patch, upgrade and change accurately against a copy of production, and automated migrations of operating systems and applications with zero downtime. These services are available via an easy-to-use Web portal, with no hardware or software purchases required and a minimal level of training needed.

Geminare Cloud Recovery

Geminare is focused on enabling service providers to white label and resell server replication offerings delivered through their own cloud compute and storage platforms. With the Geminare solution, when an outage occurs, users are instantly redirected to a mirror version of their servers in the cloud. The whole process can take less than 60 seconds. Business continues as usual by leveraging real-time replication and failover/failback services. With the Geminare Cloud Recovery and
Cloud Storage Assurance service, customers can leverage public clouds including Amazon S3, Atmos-based partners, among others. Market focus for Geminare is on licensing its technology to MSPs and service providers including cloud hosting companies (Hosting.com), telecommunications companies (Qwest Communications), VARs (CA Technologies Inc.), and MSP (Ingram Micro Seismic) channels.

**IBM SmartCloud Virtualized Server Recovery**

IBM's Virtualized Server Recovery is a new service that helps recover a VM or a server after a disruption. On-premise VMs or physical servers can be recovered to VMs in IBM's cloud or to their own servers in their datacenter. There are several service options depending on the speed of recovery required. The gold-level service can do rapid failovers, mimicking clustering in the physical world with much faster restores and without the hassle of dealing with the customized hardware involved in clustering. The service will be available for Microsoft Windows, Linux, and IBM AIX servers initially. The IBM SmartCloud Virtualized Server recovery is part of IBM's new cloud resilience program. Pricing is based on a per-use case for each running VM and data stored in the cloud. The services will go live later this summer, depending on the customer's geographic location.

**Zetta Data Protect**

Zetta provides immediate, offsite data protection for enterprise data. Zetta offers services directly to end users to enable businesses to quickly adopt storage as a service, protecting and recovering their data without expensive or risky changes to information technology environments. The Zetta Data Protect solution utilizes replication technology to, in near real time, mirror or replicate file data offsite to a Zetta-managed datacenter. Leveraging mirroring, the primary Zetta copy and the offsite Zetta copy are always in sync. Within the Zetta-managed datacenter, a mountable file system called a Zetta Virtual Volume serves as the target for the mirrored data. The Zetta service also provides versioning through periodic snapshots. These snapshots are important as they can serve as a source for recovery in the event a logical application corruption or user deletion is inadvertently replicated from the Zetta source to the target. Zetta maintains mountable snapshots of mirrored data not only for instant access in the event of a failure, deletion, or corruption but also for reuse by other users and applications.

**FUTURE OUTLOOK**

While firms invest in backup, in many cases what they really need are application and data availability. There is the perception that backup to the cloud gives you access to your data. Depending on the services and how the data is stored, that may not be a correct assertion. So, if continuity, application, and data access 24 x 7 are the goals, why is there not more continuity in the cloud offerings? Continuity in the cloud is challenging on several fronts. Challenges in achieving continuity in the cloud include:

- Application must be high availability aware.
- Continuity in the cloud requires dealing with network latency when performing failover from private to public cloud.
Infrastructure requirements (site, compute, storage, bandwidth, etc.) are significant.

Data volumes requiring continuity are often quite large and thus need considerable amounts of bandwidth.

Process is complex and integration is required between application, virtual, and storage layers.

Services or scripts used to redirect users/application access can be complex and disruptive to deploy.

Providing a remote site that is at an acceptable geographic distance from production site is not easy.

Continuity in the cloud calls for a frequent need for commonality of hardware and software configurations in production and remote sites (although virtualization can help reduce this challenge).

Continuity requires managing to differing, application-specific SLAs.

Current cloud service providers including Amazon, Google, and HP offer availability SLAs of 99.9% uptime, which is approximately 10 hours per month.

ESSENTIAL GUIDANCE

Service providers can improve upon their current offerings and differentiate themselves in a highly fragmented, public cloud backup services market by innovating within the cloud recovery/continuity market. IDC believes there is a pent-up demand for cost-effective continuity services, where the resilience of the business is tied to IT and continuous access to critical data and corporate information. The consequences of unplanned downtime, financial and reputational impacts, customer attrition, and loss of stakeholder confidence can be material. With so much in business outside of an organization’s control including economic, political, legal, and regulatory factors, business continuity is one thing that is within a firm’s control. The cloud is a perfect vehicle for firms to leverage for lower-cost business continuity in the future.

LEARN MORE

Related Research

- The State of Business Continuity in End-User Environments in 2011 (IDC #227783, April 2011)
- Cloud Storage Impacted by Datacenter Transformations and the Changing Role of IT (IDC #226214, December 2010)
- Worldwide Availability and Clustering Software 2009 Vendor Shares (IDC #223991, July 2010)
Storage in the Cloud: Overview of Key Players and Service Offerings (IDC #224244, July 2010)

Worldwide Data Protection and Recovery Software 2009 Vendor Shares (IDC #223755, June 2010)


Synopsis

This IDC study looks at the opportunity for continuity in the cloud and identifies key players that are early movers in this market.

“There are a myriad of different online backup suppliers offering public cloud backup services today. While these backup to the cloud services are useful, they do not provide a firm with business continuity in the event of a local- or site-level failure. Increasingly, smaller enterprise and SMB firms want to leverage public cloud infrastructure for achieving cost-effective continuity or recovery services in the cloud,” said Laura DuBois, program VP at IDC.

"Organizations of all sizes are seeing considerable growth in mission-critical data while also experiencing continued pressures to reduce IT-related costs," said Eric Sheppard, research director at IDC. "The rise of cloud-based continuity and recovery offerings is creating new options for these organizations to ensure near-continuous access to this ever-growing set of data in a cost-effective manner."

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2011 IDC. Reproduction is forbidden unless authorized. All rights reserved.