IDC TECHNOLOGY SPOTLIGHT

The Cloud Continuity Platform: Examining the Many Use Cases

June 2015

Adapted from *Disaster Recovery as a Service Builds Momentum as Businesses Reap the Economic Benefits of the Cloud Model* by Paul Hughes and Phil Goodwin, IDC #254455

Sponsored by Zerto

Virtual computing enables unprecedented flexibility and agility for application availability. However, many organizations have disaster recovery (DR) plans that don't adequately meet business requirements or don't fully exploit the opportunities that cloud computing presents. The deployment of hypervisor-based replication can reduce the complexity of business continuity and DR to enable service-level attainment. This Technology Spotlight examines the challenges of rapid data recovery for cloud business continuity and how Zerto's Cloud Continuity Platform may help address them.

Drivers and Inhibitors of Cloud-Based Continuity

Application service levels are becoming increasingly stringent in terms of uptime, performance, and recovery time. Users simply expect that applications will always be available and have little tolerance for downtime, especially unplanned downtime. A recent IDC survey of small and medium-sized business (SMB) users revealed that 67% have a recovery time requirement of less than four hours, and 31% have a recovery time requirement of less than two hours.

Expectations for rapid recovery under any circumstances have created a gap between what users desire and what IT is prepared to deliver. Certainly, IT professionals know that such service levels are attainable — they just aren't given the budget to buy the necessary infrastructure to do so. Moreover, business continuity projects, in general, and disaster recovery projects, in particular, tend to be funded last. IDC estimates that as many as half of all organizations have insufficient business continuity and disaster recovery plans to meet business requirements, or to even survive a disaster.

Although business continuity is perhaps the top use case for cloud computing, simply focusing on this one use limits the broad potential of cloud, especially in a hybrid cloud context. At its most basic level, application business continuity is simply the transfer of application workloads from one infrastructure to another, triggered by a specific event. There is no reason that this philosophy cannot be extended to any workload for any reason. For example, workloads could be transferred between a private cloud and a public cloud for test/dev, "burst" performance reasons, or business analytics.

Despite the benefits of hybrid cloud deployments, some organizations have been reluctant to adopt the technology, primarily because of two barriers:

- **Complexity of infrastructure.** Matching the entire application stack (i.e., servers, networks, storage, databases, APIs, drivers) between a private cloud and a public cloud can be very difficult. Without a way to match or dynamically translate the infrastructure, transitioning an entire workload can be a relatively complex and high-risk endeavor. To overcome this issue, IT organizations need a simple method of transitioning entire workloads from one cloud to another without having to account for differences in infrastructure.

- **Cost.** DR and business continuity have been typically expensive propositions. Organizations are reluctant to invest in a duplicate infrastructure, often at nearly 2x the base cost, only to see that investment lie largely fallow simply waiting for something bad to happen. If IT organizations could leverage this investment to satisfy the requirements of everyday workloads, then business continuity/DR would essentially be self-justifying.

Because hybrid cloud enables capabilities not previously available to IT organizations, IDC recommends the following:

- Consider hybrid cloud deployments for cost-effective business continuity and to give the organization the agility to meet unforeseeable application performance or recovery requirements.
- IT organizations need to look beyond traditional storage replication methodologies to enable hybrid cloud deployments because traditional methods do not adequately support the dynamic nature of virtual computing.
- It's not possible to be a best-practice organization without an adequate business continuity/DR plan, and having such a capability is an imperative.

Definitions

Hybrid cloud: A composition of both on-premise datacenter and private cloud infrastructure integrated with public cloud infrastructure using technology that allows the seamless passing of data and/or entire workloads from one to the other bidirectionally

Recovery time objective (RTO): The time that is needed to restore application services from the time those services are lost (It is important to note that data recovery is a subset of RTO, which also includes the time to restart servers, networks, and applications.)

Recovery point objective (RPO): The measure of how much data loss can be tolerated in the event of a service loss (For example, if a data set is protected from loss every four hours [i.e., using a snapshot], then the RPO is four hours. A daily backup of data [i.e., backup and recovery] has an RPO of 24 hours.)

Benefits of Automated Recovery in the Cloud

Successful application workload migration in general, and business continuity in particular, involves the classic triad of people, process, and technology. In the absence of sufficient technological capabilities, organizations are compelled to compensate with people and process. With regard to workload recovery, this often means reliance on "smart" people who know the ins and outs of the specific environment. This scenario increases risks for organizations because they may have difficulty recovering if these individuals are not available for any reason. While people and process are necessary, organizations that automate recovery to the greatest extent possible will have the highest probability of recovery.

In addition to insufficient recovery automation, organizations often must overcome infrastructure complexity during a recovery. Common areas of complexity include:

- **Multiple hypervisors.** For reasons that include software dependencies, acquisitions, or decentralized application development, organizations may find themselves with multiple hypervisors, including ESXi, Hyper-V, KVM, and others. Replicating this environment in a recovery site can be enormously complicated and difficult to keep current.

- **Various storage array replication apps.** Most organizations use several storage vendors, each with its own unique data replication capabilities. Using traditional recovery schemes, each would need to be operating in the source and target datacenters.
- **Traditional storage replication.** Traditional replication methods cannot support the dynamic nature of virtual computing.
- **Executing test plans regularly.** Moving application workloads can be very disruptive to the organization. Consequently, many IT groups simply don't test application migration and DR regularly, or even at all.

Cloud, and hybrid cloud specifically, enables the solutions that solve the traditional challenges to workload migration and business continuity. By binding a public cloud infrastructure to the organization's private infrastructure, IT organizations can create a highly malleable infrastructure that replaces the rigidity of duplicated datacenters.

Public cloud has several advantages that private infrastructure simply cannot match. Cloud providers offer capacity on demand that reduces the huge capital outlays necessary for business continuity, and they are responsible for keeping that infrastructure current. Systems can be activated on demand, and they can be deactivated when the organization is finished with them. For example, organizations with cyclical or seasonal compute requirements can engage the cloud compute capacity for those peak periods. The application may reside on the private infrastructure nine months out of the year, be transferred to the cloud during the busy holiday season where much greater compute capacity is available, and then transferred back after the rush is over.

IDC research indicates that application downtime costs organizations approximately $100,000 per hour, although the cost can be as high as $1.6 million per hour for some organizations. This downtime cost is irrespective of whether the cause is planned, unplanned, or a disaster. Thus, when organizations look to justify the ability to migrate workloads, downtime avoidance is a very easy vehicle to compare the cost of downtime with the cost of application migration.

Hybrid cloud deployments for application migration also enable organizations to better fulfill service-level requirements without deploying highly available (HA) infrastructure. HA infrastructure is not only expensive (often more than two times the cost of the base infrastructure) but also very complex to manage. Application migration in the cloud can result in higher application availability without the complexity of managing the switches, routers, load balancers, and failover mechanisms of HA infrastructure.

Key Trends

IDC research has established that 69.7% of x86 infrastructure is virtualized, growing to 71.7% by 2018. In conjunction, more and more compute services are being hosted on virtual machines (VMs). This includes software-defined storage, switches, and datacenters. Given the mobility and agility of VMs to move across physical infrastructure and geographies, this capability offers the potential to move entire workloads easily between virtual infrastructures regardless of location or hosting model.

From a practical business perspective, these developments usher in a new era of availability beyond just user concerns. Moving to an "always on" capability benefits the IT organization as well. Late-night calls and long hours of system recovery are the bane of an IT staff. To the extent that IT groups can deliver seamlessly available systems for the satisfaction of users, they also reduce the need for extraordinary efforts at system recovery. This does not mean that systems won't fail — they surely will — but IT operations teams will have the luxury of resolving problems without the crisis mode that occurs after systems have crashed.

IT organizations are also looking for ways to leverage their investment in systems; the ultimate efficiency is reuse. As a result, senior IT managers are always on the lookout for resources to optimize existing investments. Hybrid cloud is part of the solution but requires something that orchestrates the workload movement between private clouds and public clouds and translates between different infrastructure types.

Considering the Zerto Cloud Continuity Platform

The Zerto Cloud Continuity Platform is designed to enable workload migration and orchestration across a cloud environment that can include both public and private compute infrastructures. Cloud Continuity Platform has been designed from the ground up to exploit both virtual infrastructure and cloud facilities.

A major differentiator of Zerto's product is its ability to provide "anything to anything" replication and recovery. This feature shields IT groups from the complexity of ensuring the compatibility of different infrastructures; entire workloads can be migrated even between disparate infrastructures. This opens the IT organization to considering almost any cloud infrastructure in its hybrid configuration. Because entire workloads can be easily migrated from one cloud to another, cloud vendor lock-in risks are substantially reduced. Organizations can shift between cloud providers based on superior capabilities or better prices.

Key use cases for Cloud Continuity Platform include:

- **Business continuity.** Entire workloads can be migrated from the private cloud to the public cloud for rapid recovery in the event of unplanned downtime, or they can be migrated to alternate infrastructure in preparation for planned downtime of the primary system.
- **Disaster recovery.** Workloads can be recovered to the cloud for long-term operations in the event of a datacenter loss for any reason. Recovery can be 1:1 or N:1, permitting DR planning for multiple datacenters or locations to a single DR site in the cloud.
- **Application or datacenter migrations.** Applications or entire datacenters can be migrated across different hypervisors and storage with minimal downtime; organizations can leverage new hardware and infrastructure or even migrate to cloud service providers and public cloud resources.
- **Test/dev environments.** Production workloads can be replicated into the cloud, where testing, bug resolution, or other development activities can take place without impacting the production systems.
- **"Burst" computing.** When seasonal business increases or unexpected workload spikes occur, workloads can be migrated to the public cloud to take advantage of additional on-demand computing capabilities.
- **Agility.** IT organizations can easily rehost applications on alternate virtual infrastructure to avoid vendor lock-in at either the virtual level or the physical level.
- **Integration of acquisitions.** When organizations merge or are acquired, integrating systems into a common infrastructure can be a Herculean task lasting months or years. Cloud Continuity Platform can be used to combine virtualized workloads onto a common virtualized infrastructure.
- **Workload or data archiving.** If an organization needs to archive an application and associated data for regulatory or historical reasons, a tertiary copy can be made to any cloud repository. While this third copy cannot be used for other purposes, it can be sent to a cost-optimized infrastructure. Recovery will be facilitated by replicating the archive back to an active workload location.

The "anything to anything" nature of Cloud Continuity Platform means that application workloads can move from one hypervisor environment to another. For example, an application running on VMware ESXi can be moved to an environment that uses Microsoft Hyper-V. So regardless of what x86 hypervisor may be supported by the cloud provider, it is a target candidate for a workload encapsulated by Cloud Continuity Platform.

This workload encapsulation works by grouping associated virtual machines, along with all of the related data, interdependency rules, and boot order plus network settings and so on. Everything necessary to establish application services is designed to be migrated in most cases. Zerto refers to this as a Virtual Protection Group, analogous to a consistency group. This includes both the VM and the virtual disk (VHDX or VMDK) and supports the underlying virtual infrastructure's capabilities like vMotion, HA, and vApp.

Replication from one repository to another can be fully orchestrated enabling one-touch automated recovery. Cloud Continuity Platform is designed to offer near-synchronous, continuous replication, which the company says enables an RPO measured in seconds and an RTO measured in minutes.

One intriguing capability of Cloud Continuity Platform is its ability to recover to a particular point in time. The product's replication writes data immediately and retains a journal of writes for up to five days while maintaining write-order fidelity. Recovery can be similar to that of a DVR where a rollback to a specific point in processing can be established. The most obvious use for this is rolling back to a point where the system was at a consistent state, perhaps before a virus attack or an accidental deletion.

However, it can also assist in application problem resolution. In this use case, an application experiencing an error could be replicated to a cloud test/dev environment, rolled back to the point just prior to the error, and then put in debug mode to exactly replicate the conditions of the failure. Replicating error conditions into an isolated test environment is often the most difficult part of debugging, and Cloud Continuity Platform is designed to simplify this task.

Cloud Continuity Platform can be used for more than replicating an application workload. The product also orchestrates workloads and can change IP addresses (re-IP), reorder boot sequences, and the like. By using the platform to automate workload recovery, organizations will rely less on runbooks for recovery and can automate DR testing. By reducing the manual effort associated with testing and by moving the test platform to the cloud, organizations are more likely to regularly test recovery capabilities.

From a management standpoint, Cloud Continuity Platform attaches to vCenter or SCVMM. One platform server can provide a soft limit of workload management for up to 5,000 VMs; multiple servers can be configured when more than 5,000 VMs are in use. IT managers can access audit reports, performance reports, and backup reports. The platform also includes a resource planning feature to ensure that recovery targets are appropriately matched with the source system.

Challenges

Cloud Continuity Platform has very strong workload recovery capabilities for virtual environments, but as IDC research illustrates, approximately 30% of x86 infrastructure remains unvirtualized. IT organizations will still need to manage workloads on these systems, as well as non-x86 workloads, separately. Disaster recovery operations will thus necessarily require more traditional methods for nonvirtual systems. Even so, reducing the DR effort on 70% of the infrastructure is a substantial improvement for most organizations.

IT managers should also be aware that the platform is not an HA system. There are no facilities for managing heartbeats between systems or failures of individual components within an infrastructure environment. Failover using Cloud Continuity Platform is all or nothing; the workload moves from one location (or infrastructure) to another in its entirety. Thus, organizations looking for automated failover

at the system or component level will still want to deploy HA hardware and software. Failover procedures and workflow can be automated but must be triggered by the operations staff. On the plus side, this eliminates the possibility of automated "false positives" that often plague HA operations across geographic distances.

In this same vein, the system does not provide coordinated processing or load balancing across cloud repositories. The workloads are maintained separately and are connected via replication. This should also not be confused with a clustered file system; compute resources cannot be simply pointed to the secondary storage systems in the cloud — the workload must be migrated.

Conclusion

IT organizations have avoided complete disaster recovery deployments for too long largely because of the associated cost and complexity. Now, with hybrid cloud, business continuity and DR are more affordable and achievable than ever. Initial capital outlays are dramatically reduced, and virtualized workloads lessen the environmental complexity. Zerto has designed Cloud Continuity Platform to reduce that complexity even further.

Disaster recovery may be the top use case for hybrid cloud computing and specifically workload migration. However, organizations that limit their hybrid cloud deployment to DR are failing to take advantage of significant opportunities to leverage that investment in other areas. The reality is that DR tends to be one of the last IT tasks funded. When IT leaders can combine multiple use cases into a single purchase, the odds of funding approval increase as does the value delivered to the organization.

Hybrid cloud certainly opens the door to application workload migration. However, cloud mostly solves the cost issue associated with infrastructure replication. Virtualization solves some of the complexity of migration, but only within a single hypervisor environment. Single product environments create lock-in and limit IT's choices regarding potential cloud providers. Using a product like Cloud Continuity Platform may help IT organizations take the next step in maximizing the value of a hybrid cloud investment while reducing the complexity of such a solution.
