Ibm global technology services

Technology Services Thought Leadership White Paper January 2012 Brutalizing disaster recovery using cloud computing Transition your applications quickly to a resilient cloud Contents 2 Executive summary 3 Traditional disaster recovery? a choice between cost and speed 4 The pressure for continuous availability 4 Thinking In terms of Interruptions and not disasters 5 Cloud-based business resilience? a welcome, new approach 6 Facilitating improved control with portal access 7 Helping to build confidence and refine disaster recovery plans with more frequent testing 8 Supporting optimized application recovery times with tiered service levels 9 More efficiently supporting mixed environments with brutalized disaster recovery 9 Enabling bandwidth savings with a local presence 10 Coexisting more effectively with traditional disaster recovery 10 Conclusion Fast forward 50 years to today’s “ always-on” world. The flow of information and commerce in our global business environment never sleeps. With the demands of an around-the-clock world, organizations need to start thinking in terms of application continuity rather than infrequent disasters, and disaster recovery service providers deed to enable more seamless, nearly Instantaneous failover and fallback of critical business applications.

Yet given the reality that most IT budgets are flat or even reduced, these services must be provided without incurring significant upfront or ongoing expenditures. Cloud-based business resilience can provide an attractive alternative to traditional disaster recovery, offering both the memorized recovery time associated with a dedicated infrastructure and the reduced costs that are consistent with a shared recovery model. With pay-as-you-go pricing and the ability to scale up s conditions change, cloud computing can

help organizations meet the expectations of today’s frenetic, fast paced environment where IT demands continue to increase but budgets do not.

This white paper discusses traditional approaches to disaster recovery and describes how organizations can use cloud computing to help plan for both the mundane interruptions to service? cut power lines, server hardware failures and security breaches? as well as more-infrequent disasters. The paper provides key considerations when planning for the transition to cloud-based Executive summary Not long after the widespread adoption of computers, it became apparent that disaster recovery would become a necessary component of organizations’ IT plans. Business data must be backed up, and key processes like billing, payroll and procurement need to continue even if an organization’s data center is disabled due to a disaster.

Over time, two distinct approaches to disaster recovery models emerged: dedicated and shared models. While effective, these approaches often forced organizations to choose between cost and speed. IBM Global Technology Services 3 Traditional disaster recovery? a choice between cost and speed When choosing a disaster recovery approach, organizations have traditionally relied on the level of service required, as measured by two recovery objectives: Recovery time objective (ROOT)? the amount of time between an outage and the restoration of operations Recovery point objective (RPR)? the point in time where data is restored and reflects the amount of data that will be ultimately lost during the recovery process.

RPR Data Image ROOT Recovery Recovery Point Objective How much data is lost Days Hours Minutes Recovery Time Objective How long to recover

Minutes Hours Days In a dedicated model, the infrastructure is dedicated to a single organization. This type of disaster recovery can offer a faster time to recovery compared to other traditional models because the IT infrastructure is mirrored at the disaster recovery site and is ready to be called upon in the event of a disaster. While this model can reduce ROOT because the hardware and software are preconceived, it does not eliminate all delays. The process is still dependent on receiving a current data image, which involves transporting physical tapes and a data restoration process.

This disaster recovery. Some organizations use the backup infrastructure for development and test to mitigate the cost, but that introduces additional risk into the equation. Finally, the data restoration process adds variability into the process. As illustrated in Figure 3, data restoration can take up to 72 hours including the tape retrieval, travel and loading process. Dedicated Figure 1: Measuring level of service required by RPR and ROOT 6 hrs or less Data Restore 4 – 72 hrs In traditional disaster recovery models? dedicated and shared? organizations are forced to make the tradeoff between cost and speed to recovery, as illustrated in Figure 2.

Interruption Declaration HOW Setup SW Setup Data Restore Figure 3: Time to recovery using a dedicated infrastructure High Cost Shared Low Weeks Speed to Recovery In a shared disaster recovery model, the infrastructure is shared among multiple organizations. Shared disaster recovery is designed to be more cost effective, since the off-site backup infrastructure is shared between multiple organizations. After a disaster is declared, the hardware, operating system and application software at the disaster site must be configured from the ground up to match the IT site that has cellared a

disaster, and this process can take hours or even days. On top of that, the data restoration process must be completed as shown in Figure 4, resulting in an average of 48 to 72 hours to recovery. Oodles 4 Shared Declare Min 4 hrs HOW Setup Min 8-24 hrs SW Setup Min 4 hrs Declaration Thinking in terms of interruptions and not disasters HOW setup SW setup Data Restore Figure 4: Time to recovery using a shared infrastructure The pressure for continuous availability According to the IBM 2011 CIO study, organizations are being challenged to keep up tit the growing demands on their IT departments while keeping their operations up and running and making them as efficient as possible. Their users and customers are becoming more sophisticated users of technology. Research shows that usage of Internet-connected devices is growing about 42 percent annually, giving clients and employees the ability to quickly access huge amounts of storage. In spite of the pressure to do more, they are spending a large percentage of their funds to maintain the infrastructure that they have today. They are also not getting many significant budget increases; budgets are essentially flat.

With dedicated and shared disaster recovery models, organizations have traditionally been forced to make tradeoffs between cost and speed. As the pressure to achieve continuous availability and reduce costs continues to increase, organizations can no longer accept tradeoffs. While disaster recovery was originally intended for critical batch “ back-office” processes, many organizations are now dependent on real-time applications and their online presence as the primary interface to their customers. Any downtime reflects directly on their brand image and interruption of key applications such as e- amerce, online banking and customer self service is viewed as

unacceptable by customers. The cost of a minute of downtime may be thousands of dollars.

Traditional disaster recovery methods also rely on “ declaring a disaster” in order to leverage the backup infrastructure during events such as hurricanes, tsunamis, floods or fires. However, most application availability interruptions are due to more mundane everyday occurrences. While organizations need to plan for the worst, they also must plan for the more likely? cut power lines, server hardware failures and customers respond to over the past few years. While weather is the root cause of Just over half of the disasters declared, note that almost 50 percent of the declarations are due to other causes. These statistics are from IBM clients who actually declared a disaster. Think about all of the interruptions where a disaster was not declared.

In an around-the-clock world, organizations must move beyond disaster recovery and think in terms of application continuity. You must plan for the recovery of critical business applications rather than infrequent, momentous disasters, and build resiliency plans accordingly. Power HOW/SW weather 54% other Figure 5: Types of business interruptions 5 Cloud-based business resilience? a welcome, new approach Cloud computing offers an attractive alternative to traditional disaster recovery. “ The Cloud” is inherently a shared infrastructure: a pooled set of resources with the infrastructure cost distributed across everyone who contracts for the cloud service. This shared nature makes cloud an ideal model for disaster recovery.

Even when we broaden the definition of disaster recovery to include more mundane service interruptions, the need for disaster recovery resources is sporadic. Since all of the organizations relying on the cloud for backup and recovery are very unlikely to need the infrastructure at the same time, costs can be reduced and the cloud can speed recovery time. Shared Brutalized Using Cloud Low Weeks Days Hours Minutes Figure 7: A cloud-based approach to business resilience Brutalized using Cloud Recovery Interruption HOW setup SW setup Figure 6: Speed to recovery using cloud computing Cloud-based business resilience managed services like IBM Smallwood Brutalized Server Recovery are designed to provide a balance of economical shared physical recovery with the speed of dedicated infrastructure.

Because the server images and data are continuously replicated, recovery time can be reduced dramatically to less than an hour, and, in many cases, to minutes? or even seconds. However, the costs are more consistent with shared recovery. Cloud-based business resilience offers several other benefits over traditional disaster recovery models: More predictable monthly operating expenses can help you avoid the unexpected and hidden costs of do-it-yourself approaches. Reduced up- front capital expenditure requirements, because the disaster recovery infrastructure exists in the cloud. Cloud-based business resilience managed services can more easily scale up based on changing conditions. Portal access reduces the need to travel to the recovery site which can help save time and money. While the cloud offers multiple benefits as a disaster recovery platform, there are several key considerations when planning for the transition to cloud-based business resilience and in selecting your cloud partner. These include:

Facilitating improved control with portal access Disaster recovery has traditionally been an insurance policy that organizations hope not to use. In contrast, cloud-based business resilience can actually increase IT’s ability to provide service continuity for key business applications. Since the cloud-based business resilience service can be accessed through a web portal, IT management and administrators gain a dashboard view to their organization’s infrastructure. For example, clients can access the Compactors Brutalized Server Recovery portal via the Internet and identify their servers to be protected and replicated.

Through this portal, customers can download the Compactors Brutalized Server Recovery client software to install on their covered servers. Once the environment is defined through the portal, the client can view the protection status administrative view through the portal is useful, it is critical to evaluate cloud-based business resilience services to help ensure that the portal is not merely an administrative configuration tool but that it also provides the opportunity to initiate a failover and fallback. With Compactors Brutalized Server Recovery, clients can use the portal to failover in near real time (for the “ Always Available” service-level protected servers described later), reducing the need to contact the cloud service

Portal access with failover and fallback capability Support for disaster recovery testing Tiered service levels Support for mixed and brutalized server environments Global reach and local presence Migration from and coexistence with traditional disaster recovery The next few sections describe these considerations in greater detail. Client IBM Compactors Brutalized Server Recovery portal Servers/Storage Cloud hosted at IBM Resiliency

Centers Figure 8: IBM Compactors Brutalized Server Recovery portal 7 Figure 9: An administrative view of the recovery portal Figure 10: DRY Testing view with IBM Compactors Brutalized Server Recovery reviver (IBM in this case) to “ declare as disaster” or to initiate the failover. Without the need for a formal declaration and the ability to fail over from the portal, IT can be much more responsive to the more mundane outages and interruptions described above. Average once or twice per year, which is hardly sufficient, given the pace of change experienced by most IT departments. This lost sense of control has caused some organizations to bring disaster recovery “ in house,” diverting critical IT focus for mainline application development. Cloud-based business resilience provides the opportunity for more control and more frequent and granular testing of disaster recovery plans, even at the server or application level. Compactors Brutalized Server recovery provides a DRY Testing view in the portal so that IT can test the failover and fallback process more frequently. One traditional challenge of disaster recovery is the lack of certainty that the planned solution will work when the time comes.

Typically, organizations only test their failover and recovery on 8 Compactors Brutalized Server Recovery Service Level Gold Always Available Virtual Machine Recovery Time Objective (until system boot start) minute failover Description For mission-critical applications that require near-zero ROOT/RPR and that need a recovery infrastructure with near-continuous availability for use beyond recovery services For applications that need rapid recovery in minutes and that need a cloud recovery infrastructure that is remotely accessible at the time of disaster For clients that want to import server images and data from tape/disk/NAS into our cloud infrastructure at time of

disaster for failover and fallback Provides migration path for Infrastructure Recovery Service clients to cloud recovery services

Silver Disaster and Test Virtual Machine Bronze Imported Media Virtual Machine 30 minutes failover 6 to 24 hours or best effort basis, assisted failover, and assisted fallback Clients can generally tailor testing to their schedule. For example, a critical e- Commerce application can be tested prior to a peak online shopping period such as Cyber Monday. Or an online banking system can be tested after a version upgrade in order to ensure that the failover and fallback process still works seamlessly. Bronze. These tiers enable organizations to optimize their budget, paying more for heir mission-critical applications to have nearly continuous availability and paying less for non-critical applications. With Compactors Brutalized Server Recovery, the frequency of the data replication and the resulting RPR/ROOT is based upon the service level assigned to the server.

Multiple servers supporting the same application and business process can be collectively assigned the same group and service level to help ensure consistency and synchronization for failover and fallback operations. Based business resilience offers the opportunity for tiered service levels that enable o to differentiate applications based on their importance to the organization and the associated tolerance for downtime. For example, Compactors Brutalized Server Recovery provides three service level options: Gold, Silver and 9 Efficiently supporting mixed environments with brutalized disaster recovery The notion of a “ server image” is an important part of traditional disaster recovery.

As the complexity of IT departments has increased, including multiple server farms with possibly different operating systems and operating system (SO) levels, the ability to respond to a disaster or outage becomes more complex. Organizations are often forced to recover on different hardware, which can take longer and increase the possibility for errors and data loss. Organizations are implementing fertilization technologies in their data centers to help remove some of the underlying complexity and optimize infrastructure utilization. The number of virtual machines installed has been growing exponentially over the past several years. According to a recent IBM survey of Chief Information Officers, 98 percent of respondents either had already implemented fertilization or had plans to implement it within the next 12 months.

Cloud-based business resilience solutions must offer both physical-to-virtual (POP) and virtual-to-virtual (VI) recovery in order to support these types of environments. Compactors Brutalized Server Recovery supports brutalized, unventilated and mixed environments, including those with multiple operating systems. Enabling bandwidth savings with a local presence Cloud-based business resilience requires ongoing server replication, making network bandwidth an important consideration when adopting this approach. A global provider like IBM offers the opportunity for a local presence, thereby reducing the stance that data must travel across the network.

With Compactors Brutalized Server Recovery, the client’s server configuration, operating system, application software and associated data are replicated to the IBM Resiliency Center across the Internet or designated network connection. While data will be replicated to the closet IBM Resiliency

Center running Compactors Brutalized Server Recovery, added resiliency and backup is provided within the IBM network of secure centers. IBM offers a Compactors Brutalized Server Recovery Synchronization and Bandwidth Estimator to assist with the assessment of network bandwidth requirements. While many of our clients will not need to increase capacity, the Estimator can confirm your capacity needs. 0 Brutalizing disaster recovery using cloud computing Clients should identify all servers that support a single business application and assures cross-server consistency across those servers for failover and fallback, helping to enhance security and reduce risk. Conclusion Cloud computing offers a compelling opportunity to realize the recovery time of dedicated disaster recovery with the cost structure of shared disaster recovery. However, disaster recovery planning is not something that is taken lightly; security ND resiliency of the cloud are critical considerations. Compactors Brutalized Server Recovery is hosted within the IBM network of Resiliency Centers? so clients can feel confident that IBM is helping to protect their sensitive data.

Second, there is no need to rush in? clients can start to work with Compactors Brutalized Server Recovery with as few as five virtual machines under managed contract? so getting started is easier and relatively risk free. With more than 1, 800 dedicated business continuity professionals and more than 160 business resilience centers located around the oral, respected industry analysts recognize IBM as a leader in business continuity and resilience. Our virtually unparalleled experience is based on more than 50 years of business resilience and disaster recovery experience and more than 9, 000 disaster recovery clients. Further, IBM has been in the systems

business for 60 years, and Just about no other company understands systems like IBM does.

Using our vast business process and technology expertise, we can help you design and implement a business resilience solution that meets your organization’s needs. Coexisting more effectively with traditional disaster recovery While cloud-based cuisines resilience offers many advantages for mission-critical and customer-facing applications, an efficient enterprise-wide disaster recovery plan will likely include a blend of traditional and cloud-based approaches. The Bronze level service of Compactors Brutalized Server Recovery can help ease the transition from traditional methods. Clients can also use this approach when integrating their cloud-based business resilience with data back-up solutions like IBM Compactors Managed Backup.