Pulsant
Business Unlimited

White Paper
Rethinking Business Continuity with the Cloud

An intelligent approach matching DR strategies to the criticality of business information and services.

Overview from Pulsant

At Pulsant, we see many of our customers moving to more cloud-enabled technology environments, removing the limits and barriers imposed by legacy IT systems and practices. One of the areas we see as central to maintaining an effective hybrid hosting solution, is through business continuity and disaster recovery. Cloud has enabled the creation of many new technologies that make disaster recovery a simple and resilient solution to minimising IT service disruption. The key is understanding how to best plan, structure and consume your disaster recovery service, for better cost-effectiveness and service delivery.

Introduction

Technology developments and virtualisation have created huge potential for what can be achieved with businesses' continuity and disaster recovery plans. Recent developments in enterprise technology means that organisations need to radically rethink their approach to disaster recovery and create new solutions that are more flexible, scalable and cost-effective.

Disaster recovery is now high on the agenda for many businesses and organisations – in a survey conducted by Computer Weekly of over 111 UK IT professionals, 16% said they devoted a large proportion of their time to backup and disaster recovery activities alone, demonstrating the level of importance organisations are starting to place on their information and IT services. When asked about what their predicted projects in the coming year would be to address backup storage initiatives, 45% cited disaster recovery and business continuity projects as being top of the agenda, 30% highlighted cloud backup services yet 0% of respondents said they were looking to implement a tape backup project.

Proactive Planning for Better Risk Management

The risks to business operations are increasing; as cyber-attacks and IT complexity make even the ongoing management of IT operations a complicated activity which is often prone to downtime and outages. And as IT sits at the centre of a business' operations, issues can have an organisation-wide impact on people, processes and customers.

Continued...

Overview of terms

Business Continuity

Keeping your business operating, across IT, people, processes and infrastructure.

Disaster Recovery

Protecting your IT systems from disruption.

Back-up

Protecting your data.

The common misconception is that businesses must plan for large-scale disasters, yet in reality the majority of outage causes are actually more commonplace. A report from Quorum looked at the main reasons that customers logged support for downtime and found that the most common cause was IT hardware failure at 55%, human error at 22%, software issues at 18% and natural disasters at just 5%.

An increasing issue experienced by organisations which can have a long lasting impact on IT services, is disruption to commercial relationships between IT service providers and customers, following high-profile suppliers going into administration.

This results in the cessation of the services they offer, with little access available to customers who have data and services tied to their platforms.

Organisations need to pro-actively plan their disaster recovery strategies as part of a broader business continuity plan, rather than waiting for a disaster to occur before taking action. Many IT suppliers focus on the risks and fear-factors involved in not having a DR strategy in place, however it is more effective to look at how your organisation can **proactively design an intelligent approach to disaster recovery (DR) strategies.**

The Future of Disaster Recovery

Many SMB and Mid-Market businesses are facing the challenge of growing into a larger enterprise and with that comes increased security and DR considerations that have to be managed appropriately. Perhaps previously there was a limited DR solution to cover worst-case scenarios in a particular SMB company, or maybe there was no DR strategy in place at all. Now that the company is growing, decisions have to be made about how best to implement a solution that is fit for purpose whilst being cost-effective.

The good news is that the days of paying for expensive, dormant DR infrastructures housed in purpose-built business continuity facilities are over; expedited by the advent of many cloud and software-defined technologies that can match appropriate DR strategies to workloads, depending on the criticality of services and business requirements.

Likewise, many businesses have made significant investments into their primary IT architectures, creating private cloud environments that are virtualised and flexible in their design, however their DR strategies and systems are not operating to the same level of flexibility and scalability. This creates opportunity but also complexity, as IDC cited in a recent survey of UK organisations that operate virtualised infrastructures, 74.2% of firms are managing two or more hypervisors – another challenge that new DR technologies must contend with.

Organisations now need to capitalise on the investments they have made in their private cloud architectures to develop a DR strategy that works for them, without straining IT budgets or making existing environments even more complex.

The aim of this white paper is to try and clear up some of the confusion around the different types of DR strategies available to SMB organisations, and to also look at how businesses can capitalise on their existing infrastructures and the cloud to rethink how they approach DR and engage with the opportunities created by these new technologies.

We will look at:

- What organisations need to look for when formulating their DR strategy and choosing a DR partner.
- Different technology scenarios that organisations may be facing and the relevant IT DR solutions available to address each situation.
- How to rethink your approach to IT Disaster Recovery by leveraging the cloud and virtualisation technology.

Disaster Recovery Solutions Explored

In-house DR

Many organisations have opted to house their DR IT systems in-house, alongside their primary IT. Businesses with multiple locations may choose to put their primary datacentre at one site, and their DR datacentre at another site for increased resiliency. Smaller organisations located at only one site only may be forced to locate both their primary and DR IT within the same building.

Pros:

- Organisations have full control over their DR systems and processes.
- IT is not shared between different organisations, so businesses are not at the mercy of other organisations' IT issues or commercial arrangements with the supplier.
- Data and systems can be accessed at any time and DR tests can be invoked whenever the IT team desires.

Cons:

- It can be very costly to build a replicated DR infrastructure after factoring in IT hardware, software and support costs, which by its nature will be redundant and unused for the majority of the time.
- Ongoing support of the DR environment requires management and monitoring by IT teams which adds to existing workloads.
- DR infrastructure may not be refreshed and replaced as often as required if IT budgets across the business are constrained.
- Purchasing DR systems redirects budget away from primary IT purchases.
- Teams must find time to run DR tests and have overall accountability and responsibility for administering successful DR solutions within the business.
- More than one datacentre location will usually be required to deliver effective DR services.

Suited to:

- Businesses with more than one datacentre location that has spare capacity and systems available.
- Mainly non-virtualised environments that cannot be managed easily remotely.
- Organisations with specialist teams dedicated to managing the DR and back-up environments.

Offsite Business Continuity-as-a-service

Offsite business continuity service providers specialise in the end to end provision of services, workspaces, infrastructure and IT to ensure your organisation can continue functioning, whatever the eventuality. These types of services go beyond the disaster recovery element within IT, and extend to including the provision of office facilities and desktops should you experience a site-wide outage. However, technology has meant that many businesses now recover IT and office equipment to employees' home locations, enabling staff to continue working remotely despite disruptions at the main office site.

Pros:

- Solutions are comprehensive and can cover a wide range of services to ensure your business continues operating.
- High levels of reliability should your site experience downtime.
- IT systems are often developed to mirror your IT environment to minimise disruption when restoring data and services.

Cons:

- Services of this type typically have high costs to deliver the end to end solution depending on the exclusivity of the target DR platforms to you and other organisations (i.e. multi-tenant or dedicated) and the amount of capacity you choose to have provisioned in the event of a failover.
- This type of solution usually means that organisations have to purchase and pay for IT equipment and services when they are not being used.
- Many SMB organisations are not in a position to contribute large parts of their IT budgets to DR services that may never be used – instead wanting to focus IT spend on development and innovative IT services for the business.

Suited to:

- Organisations who need a comprehensive and traditional approach to business continuity, that takes into account workplace and office infrastructure alongside IT.
- Businesses that have only one location and require the security of another office and datacentre should they experience a site outage.
- Organisations with an approach to risk management which justifies expensive but comprehensive Business Continuity services; e.g. banking, energy sector.

Active / Active Disaster Recovery with a Hosting Provider

Many organisations choose to host their DR systems with a separate hosting provider, who can provide them with colocation or infrastructure-as-a-service solutions for their DR, helping to avoid having to build and manage their own DR facility.

Pros:

- The service is usually paid for on a monthly or quarterly basis so businesses can avoid high upfront costs.
- Organisations do not need to worry about the datacentre or connectivity facilities – they can just focus on their IT.
- Many hosting providers allow customers to choose the level of control and involvement they have in the day to day management of their DR IT – from providing purely colocation services through to fully managed systems.
- Systems run in an active/active model, where data is written to both sites (primary and DR) synchronously so that IT services can switch seamlessly between sites.

Cons:

- This approach is focused purely on IT and does not encompass wider business continuity considerations such as office space.
- If the organisation is housing the infrastructure within a colocation facility, they typically have to pay for the infrastructure they require upfront.
- The organisation will be paying for the overhead of having a fully active DR environment functioning at all times.

Suited to:

- Organisations that require full uptime with a strong focus on Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) within a model where they can be sure their primary and DR systems are running concurrently.
- Businesses who want the peace of mind that they have a copy of their primary IT architecture with near-instant recovery possibilities but do not want to manage the DR systems themselves in-house.

Active / Passive DR Solution with a Hosting Provider

This approach is similar to the active/active approach, however the DR site is active/passive – meaning that the DR element lies dormant until its services are required in the eventuality that the primary site experiences an outage. The infrastructure may still be owned by an organisation and hosted remotely within a 3rd party datacentre, yet the systems will not be actively running or storing data.

Pros:

- This is usually a more cost-effective approach as the DR systems do not require round-the-clock maintenance and support as they lie fairly dormant in between DR tests or live outages.
- Systems can be backed up and restored to pre-agreed RTO and RPO criteria in accordance with a supplier's SLA.
- Customers of this type of solution can 'locate' their systems within a defined datacentre for added control and security.

Cons:

- Systems have typically weaker RTO and RPO targets due to the active/passive nature of the service. Depending on the type of technology used and the approach employed, the restore could involve building new servers from images or restoring from tape drives etc. Organisations need to think about how long they can be without their IT systems before it starts to have a dramatic impact on business operations and end customer satisfaction.
- Businesses may be concerned about the risk associated with having servers and storage on an active/passive datacentre design in case of systems being unable to recover due to faulty back-up tapes or issues with data quality.
- The recovery point objective for data depends on having consistent and effective data policies across your employees, processes and systems – for instance, if your disaster recovery policy depends on restoring systems from tape, yet tape backups are only collected once a week then the business can potentially risk losing nearly a week's worth of data.
- The active/passive scenario relies on employees taking a standardised, regular approach to the management of their disaster recovery at their primary site, for effective recovery at the DR site.

Suited to:

- Organisations who are looking for a hosted DR solution which is more cost-effective than an active/active DR strategy.
- Businesses who can be flexible in their approach to DR and who do not have strict criteria of RPO and RTO targets (i.e. businesses that are not dependent on IT to continue processing customer transactions or that can cope without access to email for a number of hours).

Public Cloud Hosted Disaster Recovery

Many public cloud providers are now offering disaster recovery solutions, hosted remotely within enterprise datacentres, which organisations of all sizes can failover and back-up to providing they have the appropriate levels of connectivity required. Consumers of public cloud hosted disaster recovery services will typically purchase cloud services on demand and build out their DR sites in the cloud to mirror their primary sites' IT.

Pros:

- This is usually the most cost-effective choice, with some providers enabling customers to spin up their own DR compute resources from a self-service portal with just a credit card for payment.
- Organisations have the ability to 'spin-up' and 'spin-down' services as and when they require. This could mean only purchasing servers when the primary site experiences an outage, or having a contract in place where compute and storage space is reserved, ready for a potential failover.
- Services can be delivered globally from certain providers, perfect for businesses that need multi-country DR services which all fail over to a central DR location (or multiple DR locations).
- The public cloud provider takes on the responsibility for managing and supporting the DR infrastructure.

Cons:

- The services offered are typically generic – a one-size-fits-all model operated at scale.
- Services may be delivered from a number of international datacentres without controls on where the data is being held (i.e. not within the UK).
- Design, planning and integration support for the DR solution is typically minimal as the costs reflect the self-service nature so may not be suited to businesses with complex IT environments that need to carefully plan and manage their risk.
- Businesses may not have the ability to invoke DR tests when they choose due to the systems running on shared, multi-tenant IT infrastructure.
- If another tenant on the infrastructure fails over to their cloud DR service it may affect your ability to fail over also – you may be at the mercy of the performance of your cloud service's other tenants.
- Organisations may not be able to define their own SLAs – the services are typically standardised and not bespoke to individual business requirements. In 2014, Amazon EC2 reported only 2.43 hours of downtime, however Microsoft Azure experienced just under 40 hours, so the results and expected uptime levels can vary.
- Usually only works for virtualised environments that can move and manage virtual machines remotely.

Suited to:

- Organisations who are looking for a self-service approach to their DR, without having the infrastructure on site.
- Businesses who are comfortable with their data being located internationally and do not have data residency criteria to comply with.
- Organisations that want to capitalise on the scale that shared architecture can bring for a more cost-effective, on demand service.

Hybrid Cloud DR

Hybrid cloud disaster recovery is a fairly new term and is a way of customers taking the benefits of cloud DR and merging them with onsite DR or private cloud DR solutions. By implementing a hybrid cloud DR solution, customers can intelligently match DR approaches to their IT services and workloads – ensuring that mission critical services have a mission critical DR strategy to match, and that non-critical services are instead paired with a DR solution that matches their own level of criticality. A hybrid cloud DR environment brings together both onsite DR services, hosted remote services and public cloud DR services, under one management solution and commercial relationship for convenience.

Pros:

- Businesses only pay for the DR services they need: by segmenting their IT workloads and assigning necessary DR profiles, they can reduce their DR spend by ensuring that each workload has the most appropriate and cost-effective DR service.
- A hybrid cloud DR solution can encompass both physical and virtual server environments – with on-premise DR services for certain physical servers and off-site cloud solutions for virtualised environments.
- Businesses have the ability to plan in advance how they want each business service and IT workload to be managed in the event of an outage; from defining RTOs and RPOs, through to specifying where the data and virtual machines will be sent to for restoration.
- Software is employed to bring intelligence to the DR layer so information and applications are managed separately depending on their level of importance.
- Businesses can capitalise on the investments they have made in their existing private cloud environments by simply and quickly implementing fluid DR solutions that complement existing IT implementations.
- Organisations have control and visibility over their entire DR strategy, managed centrally through one system or tool but delivered widely across different DR services.

Continued...

Cons:

- Only works effectively if an organisation has some degree of virtualisation across their IT environment.
- For businesses with only one or two applications that require DR it may not be viable to have multiple DR strategies in place.
- Businesses with long-term investments in an existing DR solution may not realise any cost benefit if they cannot extract themselves from a current contract.

Suited to:

- Organisations that have a significant amount of virtualisation across their IT estate.
- Businesses with a mixture of IT services deployed, from mission-critical applications to less-critical services – and require a bespoke approach that is appropriate for each type of service.
- Organisations that have invested heavily in creating an on-premise private cloud environment and now want to capitalise on the automation and flexibility they have built into their IT.

Choosing a Cloud Solution for DR

Many organisations now have elements of private cloud deployments within their IT environments, utilising intelligent management tools to automate some of the repetitive tasks and deploying virtualisation technologies across their IT estate. This opens businesses up to new possibilities when it comes to implementing the foundations of an effective IT recovery solutions, due to the fluid nature of virtual machines that can be moved around and the range of technologies available to spin up virtual machines remotely in different locations, on the fly.

Despite these investments in existing IT environments, organisations often do not capitalise on the flexibility that new technology enables for them, and instead embark on long, costly contracts with providers to deliver a DR solution across their business.

Flexible, hybrid DR models that can integrate cloud DR services with onsite traditional DR, enable organisations that would normally not have the budget available to achieve a comprehensive approach, to instead move their IT into a more resilient position that can cope with outages and downtime, whilst remaining cost-effective.

It is critical when designing a DR strategy, to build in multiple service layers that match the different levels of criticality within your applications and IT systems. It is costly to set up a single DR solution based on the worst case scenario for your most expensive mission-critical systems and apply the same methodology to every service across your IT environment. RPOs and RTOs must be aligned to different areas of the business in order to make the most cost effective and flexible choice for your DR – for example, your recovery objectives for systems affecting the finance department may be much tighter than the objectives you have set for your marketing department.

To do this effectively, an organisation must first critically asses the range of services the IT department is responsible for in order to create an appropriate risk profile for each service element – which can be challenging to achieve depending on the awareness within the IT department of the different services being delivered across the entire business (including shadow IT).

A key area often overlooked at the evaluation stage of many DR service purchases, is the ability to invoke a failover to your DR site for test purposes. Regular testing of the DR solution is critical to ensuring that failovers work when you really need them to, however many DR providers do not permit users to self-test their DR services, for fear it could overload the DR systems if too many users invoke a failover at the same time.

Performing DR tests enables organisations to collect data and insights into how their systems perform under pressure, the time it takes to get services back up and running and the impact that each minute of downtime has on the wider business. This allows the IT department to reassess their DR plan and move workloads to different DR platforms depending on the outcome and insights gained from DR failover tests.

It may be that when a test failover does occur, the marketing department is severely impacted and loses thousands of items containing marketing information regarding how clients are using their website at that moment. This could prompt IT to review their DR policy on marketing applications in order to have better RPO and RTO criteria in the future. Without the test run, many insights about the real (rather than the assumed) impact of downtime on the business would be hidden until a live outage occurred.

Cloud as an Enabler for DR Plans

Cloud technology has been a huge enabler for more innovative approaches to DR to be made available to SMEs who might usually not invest in a full DR solution. The ability to start small and grow with agility and flexibility as the business scales is critical for organisations in the SMB and Mid-Market sector who are experiencing spikes in growth as they transform their businesses into larger enterprises. Cloud DR solutions can scale alongside the organisation.

And, as many small and medium businesses are already consuming services from the public cloud, software-as-a-service, in-house private clouds and traditional onsite IT; they require a disaster recovery solution that can hybridise all of these elements and design a DR architecture that matches the primary IT environment they have today.

Cloud has enabled many new technologies that make the DR process easier and more fluid, however the complexity that has been created within businesses' existing IT environments means that many organisations don't know where to start when it comes to mapping their business services back to a relevant DR strategy.

A survey conducted by IDC highlighted that 37% of organisations have to back-up a mixture of virtual, physical and cloud-based servers – so a single tape-backup strategy alone is now not sufficient for organisations wanting to protect data moving across their entire organisation.

Organisations need to look for DR services that can bring together their complex, disparate IT workloads into one simple model that users can interact with and access from a self-service portal; controlling their DR policies, managing them and testing them with the support of a technology partner in the background. User-enabled DR technologies are critical as enterprise IT begins to look and feel more like consumer technologies.

Distilled down to cloud's core ability, hybrid cloud DR services enable SMBs to access DR solutions normally only available to large corporate enterprises.

Conclusion

Cloud has enabled a more cost-effective and agile approach to delivering DR services that match your organisation's unique risk-profile. Hybrid disaster recovery and back-up solutions can capitalise on the ability of cloud services to scale and flex to meet business demand, whilst combining hosted services with onsite DR solutions for a holistic, hybridised DR service.

This move away from traditional approaches to DR such as warehouses of unused IT systems waiting to be set up should an outage occur, means that the intelligence has moved from the infrastructure layer to the software layer; and many Independent Software Vendors (ISVs) are leveraging cloud technologies to develop solutions that sit above the myriad of cloud services an organisation may have deployed, combining them under one DR strategy that can apportion risk profiles and prioritisation to different workloads.

In conclusion, organisations should be looking for a DR solution that can address the demands of a hybrid cloud environment, and has the ability to prescribe multiple layers of criticality and functionality to suit each business service.

About Pulsant

Experts in cloud, datacentre and infrastructure services, Pulsant specialises in highly resilient network, colocation, managed application and cloud hosting services. Through our partnership with Disaster Recovery software leader, Zerto, Pulsant offers customers a different route when it comes to DR planning. With the ability to prioritise and categorise IT services down to virtual machine level, Pulsant's Cloud DR solution enables clients to decide where, when and how their DR is handled and routed; for ultimate convenience and peace of mind when it matters most. Find out more about Pulsant's Cloud DR solution.

References

Computer Weekly (2015) IT Priorities 2015 – UK [Online] Available from: http://www.computerweekly.com/ehandbook/IT-Priorities-2015-UK [Accessed 23rd March 2015]

Cloud Pro (2014) 2/3 SMBs use cloud-based storage for disaster recovery [Online] Available from: http://www.cloudpro.co.uk/iaas/cloud-storage/4296/23-smbs-use-cloud-based-storage-for-disaster-recovery [Accessed 23rd March 2015]

TechTarget (2014) Cloud outage audit 2014 reveals AWS on top, Azure down [Online] Available from: http://searchcloudcomputing.techtarget.com/news/2240237323/Cloud-outage-audit-2014-reveals-AWS-on-top-Azure-down [Accessed 23rd March 2015]

Continuity Central (2013) The top causes of downtime explored [Online] Available from:

http://www.continuitycentral.com/news06645.html [Accessed 23rd March 2015]

Find out how we can help your business:
call **0845 119 9911**

BY APPOINTMENT TO
HER MAJESTY THE QUEEN
HOSTED IT AND DATA CENTRE SERVICES
PULSANT LTD
READING, BERKSHIRE