**SURVERY REPORT**

**COMPARITIVE ANALYSIS AND IMPLEMENTATION OF DISASTER RECOVERY IN CLOUD COMPUTING IN THE PERSPECTIVE OF PAKISTAN**

A disaster can strike anywhere, any time. Disaster recovery has a vital role to guarantee business continuity. This research based upon the issues faced by cloud customer in case of any disaster natural or manmade. Private cloud is established when the organization does not want any compromise on its organizational data and resources. The most common causes of disasters in Pakistan are; Cyber Attacks, flood, earthquake Terrorism, power loss and network connectivity. In this thesis, existing disaster recovery approaches are compared , analyzed for cloud computing and a new hybrid disaster recovery approach is developed in the perspective of Pakistan having better performance parameters such as RTO, RPO, Cost , security ,reliability and availability as compared to existing approaches.

….

Disasters happen. Fires, floods, earthquakes, hurricanes – and the more likely power outages, viruses and human errors – are facts of life that can cripple any organization. Yet, despite these very real threats, business leaders are slow to allocate resources for disaster recovery. Budgets are tight with fierce competition for precious dollars. Too often, executives choose to roll the dice and not invest in disaster recovery. Yet the advent of the cloud has helped reduce DR costs and simplify the DR process. A managed disaster recovery service allows you to sleep at night knowing that your experienced, cloud-based DR vendor will execute and manage the recovery process for you.

Introduction

Climate change has the potential to seriously harm Pakistan, with its tremendous social, environmental and economic impacts. The effects of global warming and climate change are relatively more pronounced in the country due to its over-reliance on the environment for basic survival, high population growth rate and density, low capacity to adapt to the negative impacts of climate change, and poverty. Realizing the high vulnerability to climate change, the country has developed national policy to combat climate change and is now to embark on developing an action plan to effectively implement climate change concerns in the planning process. This paper reviews the potential impacts of climate change and Pakistan’s experience in addressing the related issues. The paper has been divided into five sections. This brief introduction is followed by the section on climate trends in Pakistan. The next section highlights country’s vulnerability to climate change, followed by a section on major steps that have been or are being undertaken in the country to address the challenge of climate change as an on-going rocess. The way forward is next and the concluding section sums up findings of the study.

Climate trends in Pakistan

Substantial work has been conducted on climate indicators and their trends in Pakistan. The studies carried out by Global Change Impact Studies Centre (Shakoor et al. 2009;

Ali et al. 2009) and Pakistan Meteorological Department (Husain et al. 2005; Gadiwala and Sadiq 2008; Zahid and Rasul 2009; Ahmad et al. 2010) in particular are quite significant in this regard. The findings of these studies and analysis reveal that the climate of Pakistan is changing.

**Geographically Dispersed High Availability –**

Get instant backups of the duplicated environment in real-time with geographically dispersed high availability site. Instant backup can be achievable via applicative and network load balancing but only if advanced Domain Name System (DNS) servers management process is available.

**Introduction:**

Traditional Disaster Recovery (DR)

Every company with IT resources in the northeastern US understands very well the risk of disaster caused by hurricanes. Hurricane “Super storm” Sandy in 2012 was the second-costliest hurricane in United States history. Businesses are still trying to recover, with many resorting to bankruptcy protection. Thankfully, natural disasters are the least common. More commonly, service outages are caused by hardware or software failures, network outages, power outages, and human error, or physical damage to a building like fire or flooding. Companies stand to lose tens of thousands of dollars for each hour of downtime caused by some type of disaster.

Whether caused by technical problems or natural phenomena, it is the responsibility of IT organizations to restore business to a fully operational state. Traditional DR involves sending a tape backup or the replication of data and infrastructure to an offsite location. This offsite location must be far enough away from the primary location to protect against any unplanned problems impacting both locations simultaneously. For organizations in the eastern part of United States, this means having a DR location that is at least 100 miles away in the event a hurricane strikes. Organizations that have multiple, widely dispersed locations can leverage existing facilities that are at a geographically safe distance for DR.Other organizations must purchase or rent such facilities. Colocation data centers are a popular third-party service for DR. Traditional DR services replicate application state between two data centers. For successful application failover, the entire application stack is duplicated in the offsite location. (Figure One.) This includes the server and storage hardware, application software, supporting software (i.e. load balancers, DNS servers, directory servers), and networking infrastructure. Every piece of the application infrastructure must be duplicated for failover to succeed. If the primary data center becomes unavailable, the offsite can take over and activate a new copy of the application using the most recently replicated data. IT organizations are responsible for set up and maintenance of the offsite location and regular testing.

Disaster Preparedness

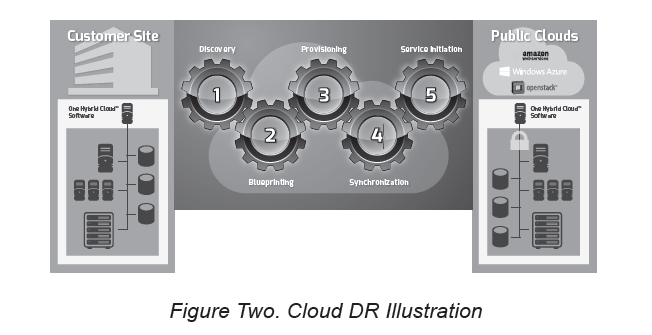
Disaster recovery is all about preparing for and recovering from a disaster. Any unplanned event that can have a negative impact on your business can be termed a disaster. Key to disaster preparedness is having a good DR plan. The absence of a DR plan exposes your organization to significant risk and potentially huge losses in productivity. To create a basic DR plan, organizations need to identify critical application(s), determine an acceptable recovery time, and build an appropriate DR solution. A typical solution involves building a duplicate infrastructure with enough spare capacity to failover applications in a disaster scenario. This infrastructure needs to be procured, installed, and maintained to support anticipated capacity requirements. DR costs include the purchase and maintenance of the additional server, storage, and networking infrastructure. It also includes the rental fees for data center floor space

and energy to power and cool the systems. IT staff time is substantial and may warrant an entire IT practice unto itself. IT staff must plan, prepare, rehearse, document, train, and update processes to deal with unplanned events. The total investment for disaster recovery planning can vary dramatically depending on the cost of the potential outage. For most organizations, traditional disaster recovery is considered too expensive, complex, and unreliable for all but the most mission-critical applications. This cost and complexity (of traditional disaster recovery) has discouraged many organizations from investing in DR planning and processes.

Cloud Disaster Recovery

Cloud-based Disaster Recovery (Cloud DR) takes a very different approach to disaster recovery based on virtualization. Using Virtual Machines (VM) to run replicas of physical or virtual servers at the primary data center, Cloud DR delivers a fully functional virtual infrastructure ready to take over should an outage disrupt primary services. With Cloud DR, the entire server, including operating system, applications, patches, and data is encapsulated into a virtual storage image. The virtual storage image is housed in an offsite public cloud where it remains in standby ready for failover. Data synchronization

operates in the background to keep data up-to-date. The entire system can be spun up in minutes, saving the organization from costly service interruption.



From an application and user point of view, Cloud DR is identical to traditional DR. When an outage occurs, whether planned or unplanned, the failover process transfers operations to the standby application servers and with minimal downtime; users regain access to business critical applications. Where Cloud DR has a significant advantage over traditional DR is in the following areas:

• Elastic and Scalable Application Infrastructure

• Economics of deployment models

• Management of the infrastructure at the second site

• Agnostic to production hardware infrastructure, and most importantly:

• Rapid, reliable and economical testing

Application Infrastructure

With traditional DR, the organization is fully responsible for the infrastructure procurement, setup and installation, and maintenance. Traditional DR requires an offsite data center to host the secondary infrastructure. Companies who already have multiple data centers can save the cost of having to secure additional data center space. Companies without an existing offsite data center often turn to colocation vendors to lease data center space. No matter which offsite data center is deployed, the organization still incurs the cost of installing and maintaining the server infrastructure. Furthermore, if the resources have to be expanded to address additional servers at the production site, the company must go through an entire procurement cycle that can often result in spending of valuable CAPEX and delays in implementation. Cloud DR is built on resources that are elastic in nature and can be allocated and reallocated on the fly with minimal delays.

**Economics of Deployment**

Cloud DR has a significant advantage over traditional DR when it comes to the cost of installing and maintaining the server infrastructure. Savings can exceed 50% over traditional DR. And the benefits don’t end there, either. Because Public Cloud service providers charge on a per use basis, virtual servers can be configured and held in standby, ready to take over primary service when an outage occurs. During the time between planned or unplanned outages, costs are minimal. The only costs

typically incurred are to store application data, which is charged on a capacity per month basis. The cloud service provider is responsible for the server infrastructure. The application servers, DNS servers, load balancers, etc. are maintained by the service provider staff. This takes a huge responsibility off the hands of the organization IT staff.

**Management of Infrastructure**

Traditional DR servers in the offsite data center must be loaded with the operating system and application software and patched to the last configuration used in production. It is the responsibility of the IT staff to keep the DR servers up-to-date when changes occur on the primary servers.

Server maintenance is a complex and costly process that consumes a considerable amount of IT staff time and resources. With Cloud DR this costly process can be eliminated. Because Cloud DR is hosted in the public cloud “infrastructure-as-a-service”, the cloud service provider is responsible for maintaining the server hardware. This way the company’s IT staff can focus its time and energy on the applications themselves and not worry about the server and storage hardware.

**Rapid, Reliable, and Economical Testing**

Cloud DR allows for fast and reliable failover testing which is an important part of a successful DR plan. The secret for this success is the virtual server infrastructure that Cloud DR is deployed on. The virtual servers that make up the Cloud DR infrastructure can be spun up in minutes and tested without touching the primary environment. Starting (and stopping) VMs takes only a simple “one-click” operation, reducing the overall DR process. This automation reduces the failover time and improves failover reliability as compared to traditional DR which relies on manual processes. With Cloud DR it is

possible to automate the entire failover process through the right setup and proper planning. All the application servers and supporting servers (i.e. database servers, DNS servers, directory servers, load balancers, etc.) are pre-configured and ready-to-launch.

**Cloud DR Operating Models**

Multiple deployment options are available with Cloud DR, the same as traditional DR. In general terms, increased readiness and greater geographical distance are both more costly. Actually, with traditional DR, readiness and geographic distance are intertwined. Increased readiness implies a shorter recovery time (RTO) and less data loss (RPO). The distance between data centers increases latency and drives up network connectivity costs.

**Traditional DR configurations which have the highest**

RTO/RPO requirements are located as close to the primary data center while still far enough away to avoid an identical natural disaster and to be on an independent power source. Financial service companies located in Manhattan typically house their offsite data centers in New Jersey, for example.

**Warm Standby Warm Standby** in a Cloud DR operating model closely resembles that in traditional DR. Warm Standby systems in the Public Cloud are always configured and up and running. Depending on the frequency of data replication, they can also provide the least amount of data loss. Warm Standby configurations can failover in a short amount of time, requiring just that the services be started on the

replicated data. Warm Standby is for your more business-critical systems. It goes without saying that

Warm Standby is a costly Cloud DR operating model. With VMs always in a running state, charges are incurred on an hourly basis and storage incurs charges on a capacity per month fee schedule. Keep in mind that multiple VMs may be required including the application servers, database servers, load balancers, directory servers, DNS servers, and others.

**Pilot Light DR**

Pilot Light DR is a Cloud DR operating model that gets its name from your household gas heater. A small idle flame that’s always on can quickly ignite the entire furnace to heat up a house. This example is similar to a DR scenario where you have all the elements of your application (VMs) already configured and ready to run. For recovery, you can rapidly spin up the VMs to deliver services during an

unplanned or planned outage. As compared to Warm Standby, the recovery time is greater but the cost savings are significant. With Pilot Light, the only costs that you incur continuously are for data storage. Charges for CPU compute time are only incurred during the outage or during tests or dry runs, not for the greater amount of time between outages. (Figure Three.)

Pilot Light DR allows you to scale up your infrastructure on an as-needed basis. If your DR plan calls for a minimal infrastructure capable of delivering a reduced work load during an outage, then you can configure your VMs on a minimum-sized set of instances. Recall that all Public Storage service providers provide a wide range of compute and storage options that vary greatly by performance and cost. With Pilot Light DR you can provision a fully functional system and not absorb the cost of a full-scale production environment. This allows for more agility, or the ability to change and optimize

resources during a DR scenario. Pilot Light DR may also be used for non-production work, such as testing, quality assurance, and internal use, etc.

**Region-to-Region**

Region-to-region DR is system failover across great distances, such as across North America or across

continents. DR strategies that require a geographically remote site incur the considerable cost of long distance network connectivity, and in general terms, increased complexity and management cost. Cloud DR enables region-to-region failover by replicating systems and data across multiple geographies by leveraging Public Cloud infrastructures that are already in place. Public Cloud service providers, such as Amazon AWS, already have multiple data centers on every continent. It takes little effort to extend your DR strategy to a remote location since you do not have to acquire the remote-site, install servers, and build a network. Cloud DR makes the region-to-region DR platform geographically agnostic, eliminating time constraints and making the location of equipment irrelevant.

**Cloud DR Business Case**

Cloud-based disaster recovery presents a less costly and more agile alternative to traditional DR. It is also easier to extend protection to apps not well served by traditional DR protection, due to cost or required management resources. By leveraging virtualization and cloud storage technologies, it is possible to implement a very functional cloud-based disaster recovery plan for a fraction of the

cost of a traditional DR plan. One important advantage of Cloud DR is the automated provisioning available through virtualization. VMs can be configured and running in just minutes as compared to the hours it takes to setup physical machines. Considering the multiple servers that make up a basic application infrastructure, this difference is significant. Secondly, physical servers are the responsibility of the IT staff to install and maintain. IT Administrators are frustrated by the amount of time their

staff must spend simple keeping servers patched and up-to-date. When you potentially double the number of servers with a physical DR site, the problem only gets worse. With the Public Cloud, maintaining servers and the data center is the responsibility of the service provider, thus freeing the organization to focus all of its IT resources on more critical application-related initiatives. It is not surprising that organizations are cautious about

placing production services in the cloud. They are justifiably concerned about security, access, and control of their data resources. Cloud DR is a good stepping stone for these organizations. When a virtual or physical application running in the primary data center is cloned and configured in a Public Cloud, it can be tested and modified without any risk to the primary instance. With Cloud DR live production data remains on production site. An organization can test different configurations with

varying amounts of cloud resources (i.e. compute power, storage performance) until they are comfortable with a configuration that can failover, providing a sufficient level of performance based on expected workload. Virtualization makes testing fast and simple as compared to manually configuring physical server and storage hardware. Virtualization allows you to scale up (and down) your DR infrastructure on an as-needed basis.Cloud Service Providers offer a range of storage options

and compute offerings, which makes cloud-based disaster recovery a faster and more simplified process. IT managers have the opportunity to use the new service offerings to extend DR services to additional workloads, further reducing their exposure to business interruption.

**Small organizations find that Cloud DR makes DR** possible for the first time. Cloud DR gives enterprises and SMBs the tools to quickly and efficiently recover from planned and unplanned outages. Cloud DR also enables the agility to change and optimize resources during a DR scenario, which leads to significant cost reductions. Cloud DR is one of the most powerful use cases for taking advantage of the cloud.

**Cloud DR Adoption**

How many companies are deploying cloud storage for DR purposes today? A 2010 survey of 100 organizations by the Aberdeen Group revealed that the heaviest users of cloud disaster recovery are small and midmarket businesses with annual revenue of $50 million to $1 billion.2 Enterprises with more than $1 billion in annual revenue typically have data centers in multiple locations, and have less need to use the cloud for disaster recovery. The survey found that organizations that had moved at

least part of their storage to the cloud recovered four times faster than those with no formal cloud storage program. Cloud storage users met their RTOs more often than those who kept data in-house.

The survey reported the following:

• Companies with Cloud DR reported an average of 2.5 downtime events in the past year, and resolved those in an average of two hours.

• Companies with no Cloud DR strategy reported an average of 3.5 downtime events in the past year, and took an average of eight hours to recover from them.

• 55% deploy a secure connection to the cloud.

• 40% utilize server failover to the cloud.

• 22% use continuous data replication to the cloud.

• 10% use multiple cloud providers.

The Aberdeen Group survey reveals that Cloud DR is growing as the preferred solution because it reduces the risk of losing critical business data and experiencing a business interruption; critical applications can be up and running in minutes, not days; and it's a faster way of bringing the business back to normal.

**Cloud DR Economics**

Cost is a major reason organizations of all sizes should consider Cloud DR for their disaster recovery plans.

Small- to medium-sized organizations that cannot afford traditional DR can benefit from Cloud DR. Large organizations who are adopters of traditional DR are finding that the costs of hosting their own offsite data center are skyrocketing because of data growth. A physical DR site means investments in additional data center space, connectivity, and servers. Additional operational costs include power and cooling, site maintenance, and manpower requirements. With cloud-based computing and storage, organizations have access to a DR platform without building one. They don’t need additional corporate-owned infrastructure assets like servers and storage arrays. Organizations can focus their IT resources on applications instead of spending time managing general infrastructure resources.

Cloud DR operates only during data replication, or in the event of an actual disaster. The organization pays for storing the application snapshots and application data in a suspended state, and replication of data from primary to the secondary (Cloud DR) site for data synchronization. The full complement of resources required to actually run the application need only be provisioned and paid for when disaster strikes. The usage-based cost of Cloud DR is well suited for DR where the secondary infrastructure is

parked and idling most of the time. Staffing costs are minimized since the responsibility for purchasing and managing the DR infrastructure is outsourced to a cloud service provider. Monthly payments are based on services used; meaning customers only have to pay for the resources consumed. Cloud DR radically changes the economics of disaster recovery.

**Cloud DR Agility**

The automated provisioning of the virtual infrastructure makes Cloud DR more agile as compared to traditional DR. Using Cloud DR, organizations can fail back from a disaster to the original location or to a new one, in the cloud or onsite. Failover / failback to a cloud infrastructure make DR processes simpler and reduce recovery time

(RTO). The flexibility of Cloud DR means applications and servers that are less critical in a disaster can be tuned down with fewer resources. Critical applications get the resources they need during the disaster. IT staff can monitor, test, and adjust DR infrastructure without

affecting production systems. Cloud DR gives the ability to finely tune the costs and performance for the DR platform.

**Cloud DR Planning Considerations**

Cloud DR planning entails Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) based on business considerations and well-defined processes for recognizing and declaring a disaster. Good DR planning involves tight integration between the network, directory system, firewalls, and load balancers, and the Web, database, and storage tiers. The virtual machines created to recover the primary environment are same as VMs you would bring up in a dedicated facility using physical machines. With Cloud DR these VMs are hosted in a third-party facility and are essentially operating from the cloud. When the lights go out at the protected facility and disaster protocols are invoked, those VMs take over as production machines. The first step is finding the right cloud service provider to help your organization meet your RTO and RPO requirements. Once decided, a thorough DR plan must then be created and measured by testing the system repeatedly for availability and completeness. The plan should then be shared with key personnel so everyone knows their roles and responsibilities when

downtime occurs.

**Bandwidth**

It is important to have the proper amount of bandwidth and network capacity to support application workload during a disaster. Typically, a company’s physical DR site is located at the nearest feasible geographical location. A cloud service provider may base data center(s) across the United States or in a different continent, which may be located far from the users of the workload. This distance can increase latency and cause performance issues for users if the application has high latency sensitivity. Cloud

DR may not be suitable for a company which has critical applications that demand low response times and low latency. If you plan to restore from the cloud to on-premises infrastructure, consider carefully the location and test the network performance to make certain you can deliver adequate application performance during a disaster.

**Data Redundancy**

Having running systems and applications are great, but without current data in place the DR recovery will not be effective. It is important when planning DR to consider how much data you can live with re-entering. This will help you determine the recovery point objective (RPO) which in turn will help you implement the appropriate replication process. Keep in mind that with Cloud DR redundancy

can be automatic, with stored objects replicated across multiple geographies thus decreasing data loss.

Data redundancy is going to be among the most important decisions and processes you will undertake in

the DR planning process.

**Network Redundancy**

Cloud DR not only replicates the servers between data centers, but also replicates the entire network configuration. Network replication is a critical path for successful DR. A solid DR plan includes IP address mapping, firewall rules, and VLAN configuration. It uses a change management process to replicate production site network changes to the DR network configuration. Failure to provide network change management is a primary reason why DR fails to work. A proper Cloud DR solution will use

automation to first duplicate network settings and to capture any subsequent changes.

**Cloud DR Testing**

It is important to test your DR capabilities on a regular basis to make sure it performs as expected. Testing at least twice a year is recommended. Some Cloud DR users test quarterly, taking full advantage of the high levels of automation. Planned failover may also be a compliance requirement for your industry. Cloud DR makes frequent testing less expensive and less disruptive. Testing can be performed quickly and easily without touching the production environment. Consider DR roles for each staff member and make certain everyone receives adequate training. Make certain the DR plan, including the steps to follow in the event of a disaster, are kept in a location that is accessible.

**Selecting a Service Provider**

When selecting a cloud service provider, pricing is not the only consideration. Reliability, availability, and its ability to serve are also key considerations. Recall the shock in 2013 when cloud storage provider Nirvanix told its customers that they had two weeks to find another home for their terabytes of data because the company was closing its doors. Selecting the wrong service provider can easily put you in the doghouse or even get you fired. You may request the right and the means to take a regular

backup data in the cloud. Ready access to your data can speed up migrations and meet regulatory compliance independently of service provider business circumstances.

**Cloud DR Success Factors**

Automation is the key to successful cloud-based disaster recovery. Considering the number of steps that are required to start virtual machines, capture network configurations, and host names, etc. there are too many chances for error if done manually. Cloud DR uses high levels of automation for fast failover with increased reliability. Take advantage of the easy access of cloud services to test frequently and confirm infrastructure performance. Consider deploying multiple clouds for failover for added redundancy. If you service customers in different continents, take advantage of geographic locality that cloud service providers can provide. Regular testing, staff training, and thorough DR planning are all hallmarks

of a successful DR plan.

**CloudVelox Pilot Light DR for Amazon Web**Services

CloudVelox Pilot Light DR for AWS™ offers the fastest, safest, and most cost-effective way to automate disaster recovery services leveraging the AWS public cloud. The CloudVelox (CV) Pilot Light solution analyzes each data center app and provisions the required compute, memory, and storage resources in AWS and continually updates them with any changes made to the primary systems

running the application. The synchronization processes copy each systems configuration, meta-information, and file systems to the cloud, and then continually updates the cloud information with any changes that occur on the primary systems. Any changes made on the systems, whether to executables, data, home directories, or any other part of the system, are automatically synchronized into the cloud. CV software ensures that in the event of a disaster (or planned failover), the application systems in

the cloud are up-to-date and ready for failover.

• With CloudVelox, systems run interrupted – installation and the various processes work on the “live” production systems with all services available (no reboot, etc.)

• With CV Pilot Light DR, setting up a centralized and automated recovery plan is simple and can be done in a matter of minutes.

• Automated failover and site migrations – CV software automates the entire site recovery and migration

process.

• Upon initiating a disaster failover, business services are automatically recovered with limited or no manual intervention.

**Launching systems** in the cloud can be done at any time, while production systems continue to run and

provide service, allowing for testing of the failover environment as desired.

In the event of a disaster or planned failover, all it takes to failover each application is a single mouse click.

When failover is initiated, the CloudVelox solution ”ignites” the AWS VM images and transfers data center services to them. In just minutes complete applications can be up and running in the cloud. To minimize cost, CV software ensures that all of the up-to-date virtual images in the cloud are kept ready without any burden to the IT staff.

For the majority of time spent between system outages or planned failovers, cloud service expenses are kept to a minimum. Increased cloud service expenses only occur during the actual disaster event or planned failover.

• Non-disruptive testing – with CV Pilot Light DR, failover testing can be performed as frequently as

required and does not affect production systems.

• Organizations are able to quickly identify any problems with recovery plans to enable fast resolution.

• Hybrid cloud compatible business continuity and disaster recovery (BC/DR) capabilities at your

fingertips through CV Pilot Light DR.

Disaster recovery solutions benefit from thorough testing and monitoring. CV Pilot Light DR for AWS enables companies to easily test failovers for various purposes, such as system verification, compliance, staff training, and performing maintenance on primary systems. The CV Administrator console provides a single-pane view of all the replicated systems running in the data center and the

**AWS cloud environment.**

**Application services can be** started or stopped in just a matter of minutes, with no specialized skills required or knowledge of AWS. IT staff will enjoy the ease at which applications can be tested for

failover without the need for lengthy disaster recovery instruction plans.

**CloudVelox software delivers automated cloud-based** disaster recovery for multi-tier, physical, and virtual production apps. It removes the complexity of performing an application failover or a complete disaster recovery, resulting in more reliable DR, reduced demand on IT staff, and reduced cost.

**Case Study: City of Asheville, North Carolina**

**CloudVelox Enables Pilot Light DR on AWS**

The City of Asheville’s IT Services department, located in North Carolina’s picturesque mountains, serves a city with a daytime population of 120,000. The team manages the nerve center for critical city services for 43 square miles of facilities, four public safety telecommunications towers, and everything from water to sanitation and key facilities, including the 7500-seat US Cellular Center. CIO Jonathan

Feldman has been at the helm for roughly ten years, overseeing several initiatives that have positioned

Asheville as a leader in public service IT, especially for state and local governments.

Excellence in DR wasn’t Easy with Traditional IT In recent years, the city was unable to prioritize disaster recovery support for two key apps, one for asset management and the other for arena point of sale transactions. While urgent systems like ERP were protected, important systems weren’t. Virtualization gave the team some flexibility, but there were still many complex manual processes that limited the team’s ability to conduct dry runs to test their DR readiness.

“Excellence in DR was certainly a challenge,” commented CIO Jonathan Feldman. “Although we had a basic level of DR, we thought there must be a better way to protect more systems while still remaining fiscally responsible to City Council and taxpayers.” All potential and implemented solutions required upfront capital investments in hardware, geographic compromises (DR site within two blocks of City Hall) and suffered from very limited automation. Under that scenario the city could afford protecting urgent systems; yet like other cities, important systems were not protected.

**Cloud DR Appeal**

“The concept of ‘Pilot Light’ DR intrigued us, to say the least. If it worked, it could allow us to extend protection to otherwise unprotected systems, enhance agility, and give us the geographic diversity enabled by the AWS IaaS cloud,” continued Feldman. The City of Asheville team originally had an RTO of 12 hours and a restoration point that was typical to the municipal government industry: a

restoration of the last night’s backup. This meant an RPO of somewhere between 3-9 hours. With Pilot Light DR they would also have an opportunity to improve their overall disaster recovery process. While they were familiar with AWS and other IaaS providers, they had held off due to the considerable up front cost and resource requirements of cloud deployment. Then they discovered the CloudVelox One Hybrid Cloud™ platform and the promise of hybrid cloud automation. “The CloudVelox

platform was a game changer. Compared to any other option, we were able to deploy our important apps on AWS for DR with minimal budget impact and maximum compatibility.”

**CloudVelox Delivered**

CloudVelox software integrated Asheville’s multitier systems with AWS compute, storage, networking, and security APIs, resulting in a very high level of automation when it came to secure, ongoing updates between the data center and the environment in AWS, and greatly simplified, automated deployment of key systems in the cloud. The results were substantial. The city was able to extend disaster recovery protection to important, yet previously unprotected systems within ongoing operating funds while improving its ability to conduct regular DR testing. Cloud DR also increased agility and allowed more

regular testing of disaster recovery systems, which further encouraged operating efficiency.

Last but not least, the city was able to achieve unprecedented geographic diversity by leveraging AWS IaaS in the west region, versus a dedicated facility two blocks away from the data center. “CloudVelox and AWS allowed us to be better stewards of the Asheville’s important technology services as well as taxpayer resources,”commented CIO Feldman. “What we accomplished together here in the mountains of North Carolina should serve as an example of the higher standards of service and system protection now possible in state and local governments trapped in the costs and complexities of traditional approaches to DR.”

**Cloud DR Checklist ✔**

CloudVelox offers the fastest, safest, and most cost-effective way to automate disaster recovery services

leveraging Public Cloud Services from AWS. The major benefits that CloudVelox Pilot Light DR delivers can be used as checklist for any Cloud DR solution.

**✔Compatible with Existing Data Center Infrastructure**

A proper Cloud DR solution such as CloudVelox Pilot Light DR for AWS supports both physical and virtual servers. It is a common myth that only virtual machines can be migrated to a public cloud. The same solution should support all types of virtualization. A solution that only supports VMware, for example, will hinder you if your data center has also deployed Microsoft Hyper-V, Citrix

Xen, or one of the many other virtualization software solutions. Finally, the Cloud DR solution should be storage agnostic, meaning it should replicate data at the application level; thereby removing any dependencies on the type of storage.

**✔ Full Automation**

Automation is the key to a successful Cloud DR deployment. The CloudVelox Pilot Light DR for AWS

solution, for example, provides automatic detection of all servers and interconnected services for a given

application. After the IP Address or Host name of a single server in a group is identified, it then automatically detects the remaining servers in the application group. Once an application is configured (referred to as the “system blueprint”), the cloning and replication processes begin automatically. Considering the amount of data included with each system blueprint, automation is clearly better

than manual documentation and configuration.

**✔ Automated Cloning and Replication**

CloudVelox Pilot Light DR for AWS replicates the entire application and all its dependent services together as a single application group. For compute services, CloudVelox software automatically detects the number of cores and amount of memory for each server. It also performs a calculation to determine CPU performance. For data replication, CloudVelox software replicates changed blocks for Windows systems using Windows VSS at a rate that is configurable. A four-hour RPO is the default. For Linux systems the replication is continuous. CloudVelox automatically replicates the storage environment, including Network File System mounted volumes. For network cloning, it automatically creates a

VPC (virtual private cloud) in AWS for secure communication.

**✔ Automated Change Management**

Changes occur very often, so a change management process is an important and challenging part of every DR plan. Using automation, CloudVelox software detects all changes in the source data center and transmits the changes to the clones running in AWS. These changes include data (of course), network, and compute. This automation greatly reduces management time and greatly improves failover reliability.

**More Frequent DR Testing**

A sound test plan is vital to a successful DR plan. Because of automation, Cloud DR can be tested more

frequently and there is no disruption to production systems because the failover is performed on the application infrastructure that is running in AWS. With CloudVelox Pilot Light DR for AWS it is easy to test monthly rather than twice annually. The total test time can be as quick as 1-2 hours, versus 1-2 days for traditional DR.

**✔ Easy Management**

Many IT staffs do not have the skills and experience to provision an application in AWS. AWS has its own set of terminology, methods, and practices that can be very intimidating to a new user. CloudVelox Pilot Light DR for AWS eliminates this barrier with unprecedented automation. The cloning and replication processes configure the necessary AWS resources (compute, storage, and network) automatically. Simple configuration parameters can be altered, such as compute, but again no specialized knowledge of AWS is required.

**Conclusion**

Cloud-based disaster recovery drastically changes the economics of disaster recovery and enables disaster protection for a far greater number of organizations. Cloud DR’s significant cost savings enables recovery methods that were previously only possible for larger organizations. By leveraging cloud-based virtualization, Cloud DR offers increased agility and flexibility as compared to traditional DR. With Cloud DR you can allocate capacity and performance on demand and only pay for the services you use. Cloud service providers take care of the hardware and infrastructure maintenance, leaving you in charge of your applications. Cloud DR does not change DR fundamentals, including a solid disaster

recovery plan, periodic testing, and having trained and prepared staff. Cloud DR is economically priced while meeting mission-critical availability, performance, and protection requirements. Cloud DR is a game changer for disaster recovery. Now is the time to lower data protection costs and ensure data is protected.

These vendors can be companies' way to make sure all of their bases are covered regarding how they back up data, how they educate employees regarding recovery strategies and how critical applications are restored following floods, fires, hurricanes, earthquakes, power outages and disruptions caused by human error.

**FOR SECURITY**

**V. SOLUTION APPROACHES**

First approach should be that cloud user and cloud provider must make sure whatever request/response they have got is from

trusted source by estimating the correctness of data that they have received. This can be done by implementing trust based protocol

between user and cloud provider. That will ensure cloud provider as well as user about data consistency and data security of user

data.

***Cloud Trust Protocol (CTP):***

The Cloud Trust Protocol is a mechanism that help cloud user to request and retrieve standardized inquiries about cloud provider

transparency. CTP is a procedure for establishing digital trust between cloud user and cloud service provider. With the CTP cloud

user are provided a way to find important information about security, privacy that is being performed in the cloud. The CTP

empower the cloud consumer with right information to make right choices about data what to put in the cloud or leave the cloud

and to decide which cloud is best suited for his data.

**4 standard Approaches of Backup and Disaster Recovery using Amazon Cloud:**

 1. Backup and Recovery: To recover your data in the event of any disaster, you must first have your data periodically backed up from your system to AWS. Backing up of data can be done through various mechanisms and your choice will be based on the RPO (Recovery Point Objective- So if your disaster struck at 2 pm and your RPO is 1 hr, your Backup & DR will restore all data till 1 pm.) that will suit your business needs. AWS offers AWS Direct connect and Import Export services that allow for faster backup. For example, if you have a frequently changing database like say a stock market, then you will need a very high RPO. However if your data is mostly static with a low frequency of changes, you can opt for periodic incremental backup. Once your backup mechanisms are activated you can pre-configure[AMIs](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html)(operating systems & application software). Now when a disaster strikes,[EC2](http://aws.amazon.com/ec2/faqs/) (Elastic Compute Capacity)  instances in the Cloud using [EBS](http://aws.amazon.com/ebs/) (Elastic Block Store) coupled with AMIs can access your data from the [S3](http://aws.amazon.com/s3/) (Simple Storage Service) buckets to revive your system and keep it going.

2. Pilot Light Approach: The name pilot light comes from the gas heater analogy. Just as in a heater you have a small flame that is always on, and can quickly ignite the entire furnace; a similar approach can bethought of about your data system. In the preparatory phase your on premise database server mirrors data to data volumes on AWS. The database server on cloud is always activated for frequent or continuous incremental backup. This core area is the pilot from our gas heater analogy. The application and caching server replica environments are created on cloud and kept in standby mode as very few changes take place over time. These AMIs can be updated periodically. This is the entire furnace from our example. If the on premise system fails, then the application and caching servers get activated; further users are rerouted using [elastic IP](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)addresses to the ad hoc environment on cloud. Your Recovery takes just a few minutes.

3. Warm Standby Approach: This Technique is the next level of the pilot light, reducing recovery time to almost zero. Your application and caching servers are set up and always activated based on your business critical activities but only a minimum sized fleet of EC2 instances are dedicated. The backup system is not capable of handling production load, but can be used for testing, quality assurance and other internal uses. In the event of a disaster, when your on premise data center fails, two things happen. Firstly multiple EC2 instances are dedicated (vertical and horizontal scaling) to bring your application and caching environment up to production load. [ELB](http://aws.amazon.com/elasticloadbalancing/) and Auto Scaling (for distributing traffic) are used to ease scaling up. Secondly using [Amazon Route 53](http://aws.amazon.com/route53/) user traffic is rerouted instantly using elastic IP addresses and there is instant recovery of your system with almost zero down time.

4. Multi-Site Approach:  Well this is the optimum technique in backup and DR and is the next step after warm standby. All activities in the preparatory stage are similar to a warm standby; except that AWS backup on Cloud is also used to handle some portions of the user traffic using Route 53. When a disaster strikes, the rest of the traffic that was pointing to the on premise servers are rerouted to AWS and using auto scaling techniques multiple EC2 instances are deployed to handle full production capacity. You can further increase the availability of your multi-site solution by designing [Multi-AZ architectures.](http://d36cz9buwru1tt.cloudfront.net/AWS_Building_Fault_Tolerant_Applications.pdf)

Natural disasters are common in certain geographies. For example, the U.S. reports more than 1,200 tornadoes every year. Earthquakes and tsunamis, floods, forest fires, hurricanes, mudslides, and avalanches can destroy a data center, sometimes without warning.

Many natural disasters can affect an entire area, which is why you must store one backup copy a reasonable distance from the original location. Being prepared is the key to ensuring that your organization’s operations continue.

War, terrorism, and sabotage are all man-made disasters. In many cases, man-made disasters are not intentional. Regardless, a fire caused by negligence or human error can destroy an entire data center. While some man-made disasters can be prevented, no organization is 100 percent protected.

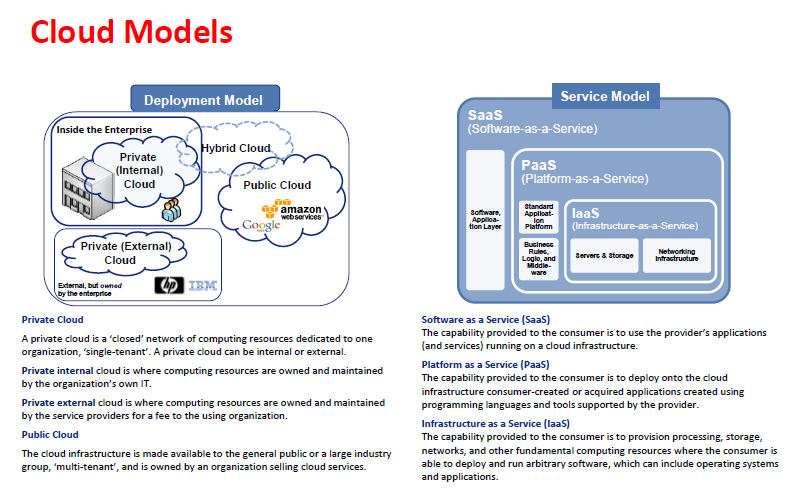
The DR plan must cover any incident that causes company operations to cease or data to be lost. The company creates a high-level DR plan, and the IT team develops a plan for the data center. The IT team plans, documents, and tests every step of the DR process.

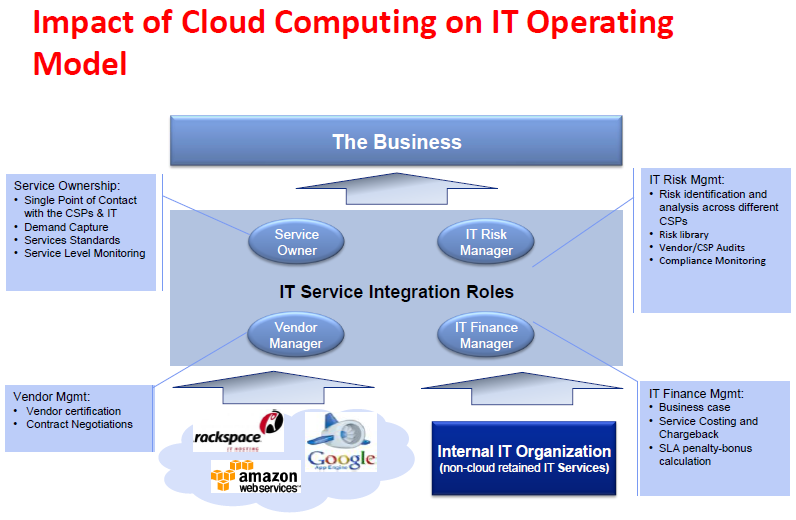
IT does not need to create DR plans for each server or VM. Acronis Backup Advanced automatically generates the individual plans, providing detailed customized steps for recovery that includes machine names, setups, system configuration, backup archive naming, and so on. During a disaster, the high-level plan is activated with instructions already prepared for single machines. The IT team exercises their DR plan on a regular basis so that every engineer understands their objectives and tasks. All engineers are required to attend Acronis’ training courses to receive Acronis Certified Engineer certifications

A disaster destroys the company’s data center but the company is prepared. The IT team developed a disaster recovery plan that included the Recovery Point Objective, Recovery Time Objective, backup source systems, backup storage policy, backup schedule, and backup duration. The management team approved the disaster recovery plan. IT exercises the plan on a regular basis using different scenarios.

The timeline of actions clearly lays out the steps the IT engineers took to recover the data center and restore operations. Using Acronis Backup Advanced suite of products, the IT team achieved all of the business objectives set forth in the DR plan and restored all data center operations in 28 hours, well below the RTO of 72 hours.

The IT team used the following Acronis Backup Advanced products to support the backup and recovery of their data center:

****

****

Cloud environment comprising of a large quantity of shared servers distributed all over the world. These servers provide the infrastructure, platform, devices, software and other resources. The basic theme of Cloud computing is to “pas as you use it basis”. What a system is composed of, is not the concern of the cloud user so Cloud computing is an abstract model of distributed computing. For a cloud user the cloud computing is simply as a black box of software and hardware [1].

**Internationally**, Introduction of Amazon’s Elastic Computing Cloud (EC2) in 2006 becomes the first appearance of Cloud computing to the world. In 2007 [2], IBM introduced Blue Cloud at the same time Dell also introduced its version of Cloud computing. After it Microsoft’s Windows Azure and Google’s Map reduce suits are released in the market [3].

Internationally Disaster Trends ,according to Disaster Recovery Survey 2016 by Cloud Endure.

This survey is based on responses from 141 IT professionals from around the world, collected through an online survey conducted in January 2016.

Some of the key findings of the survey include:

* + - * The #1 risk to system availability remains human errors, followed by networks failures and application bugs.
* Cloud provider downtime has moved down from being risk #3 in 2015 to #6 in 2016.
* While the majority of organizations surveyed (77%) have a service availability goal of 99.9% or better (“three nines” or less than 9 hours of downtime a year), more than half of the companies (57%) had at least one outage in the past 3 months, and almost a third (31%) had an outage in the past week or month.
* The cost of downtime for over a third (36%) of the organization surveyed is a $100,000 per day or higher.
* When it comes to service availability, there is a clear gap between how organizations perceive their track records and the reality of their capabilities. While 90% of respondents claim they meet their availability goals consistently (38%) or most of the time (52%), 22% of the organizations surveyed don’t measure service availability at all. It is hard to tell how these organizations claim to meet their goals when they are not able to measure them.
* The top challenges in meeting availability goals are insufficient IT resources, budget limitations and lack of in-house expertise.
* There is a strong correlation between the cost of downtime and the average hours per week invested in backup/disaster recovery.

**Locally in Pakistan** Disaster profile of Pakistan

Clearly indicates that Pakistan has a multiple disaster statistics as it is a disaster--‐prone country

Of South Asia in which huge loss of property, flora and faunas generally occurs every year in the

country. Frequent occurrence of flood causes severe disaster in Pakistan, followed by tropical

cyclone, infrequent strong earthquakes and landslide in the country. Government of Pakistan

involves various stake holders of country and overseas to deal with disasters on massive scale

to mitigate hazards caused due to various types of natural calamities During the last 50 years

about 162 Natural disasters have killed 106,036 people ,while affected 88,140,223 and people

respectively. This is a very large number and has major implications on growth and development

of the country .

The IT industry has undergone a revolution, cloud computing has not yet established its firm roots in Pakistan. The Asia Cloud Computing Association’s Cloud Readiness Index 2014 indicates that Pakistan is not among the top 15 countries in Asia where cloud services are being used optimally (Asia Cloud Computing Association, 2014).

In Pakistan, Different cloud firms in the country are providing cloud services of various types and models to the private sector.

* **GOVERNMENT CLOUD PROVIDERS**

1. **PTCL is the pioneer in providing telephonic and internet services around the country**. PTCL maintains a mesh of optical fiber around all the major metropolitan cities of the country and is providing download / upload speeds from 1Mbps up to 50 Mbps. PTCL is also offering cloud services to its customers. **Since PTCL is a government-owned corporation, all infrastructure / setup and data warehouses are located inside Pakistan.** PTCL offers a public as well as a private model of cloud with servers starting from basic to enterprise. PTCL’s standard server cloud package with standard disaster recovery support costs around US$10,500 per year.

The Telecommunication Industry Association (TIA) and the American National Standards Institute (ANSI) have defined four levels of data centers. PTCL maintains a Tier III certified data center. PTCL provides the flexibility to its customers to utilize cloud services and pay for services only used by the firm. This gives the customer much flexibility in using cloud services and results in significant financial savings. PTCL cloud uses state-of-the-art hardware and provides disaster recovery for the protection of live workloads from a single point of failure.

The disaster recovery facility gives assurance to cloud users for availability of enterprise data in case of loss or damage to primary data storage. The PTCL cloud is supported by team of experts with 24/7/365 availability. .The PTCL data center with its large redundancies can be considered as the best among various competitors in the country. Since PTCL is a government-owned organization, it can be considered as a more reliable and trustworthy institution,

* PTCL offer cloud computing solutions from its information center features situated in Islamabad, Lahore and Karachi. So far PTCL has two major clients Government of Pakistan and AIOU but still it is looking to extend its services to small and medium sized businesses.

1. **Punjab Information Technology Board PITB’s** established First Cloud Computing Data Centre in Karachi Launched in 2013. The data center plays a pivotal role in an organization delivering cloud services Punjab Information Technology Board (PITB) had launched its Data Centre and Cloud Computing Services for both public and private sector in Karachi. This is the first public cloud service by the government of Pakistan under the PITB. The PITB will be offering all required services of a Tier-III with an international standard compliant Data Centre and Cloud Computing that will host applications and services of both public and private sector at the Arfa Software Technology Park Data Centre. The cloud computing services project has been named Cloud for Everyone.

**B. COMMERCIAL CLOUD PROVIDERS**

There are many private firms in the country that are providing cloud services in the commercial sector. Among these cloud providers, Cube XS Weatherly cloud services and Rapid Compute are among the best commercial cloud providers in the country. Details about these two firms are provided in the following paragraphs.

**1. Cube XS Weatherly Cloud Services**

In 2006, Cube XS Weatherly Cloud Services (CWCS), a privately owned firm, established the first Tier IV compliant data center in Karachi Pakistan. A Tier IV data center, in addition to meeting the Tier III data center requirements, CWCS provides flexibility to its customers through pay-as-you-go cloud services and an optimized backup and disaster recovery strategy. CWCS maintains a highly competent workforce and support team that is available 24/7/365. CWCS offers IaaS and SaaS to its public cloud users, whereas it also offers private cloud to its customers. CWCS charges around US$1,400 per month for an enterprise level private cloud facility for an unlimited number of users (CWCS, n.d.).

CWCS is maintaining a superior Tier IV data center in comparison to the PTCL Tier III data center. However, besides its data center, CWCS is using similar IT infrastructure and storage devices as PTCL. Moreover, CWCS in comparison to PTCL charges more money for utilizing similar package of cloud services. Nevertheless, CWCS is a highly reliable and well reputed cloud firm that can be considered as a potential cloud provider for

**2. Rapid Compute**

Rapid Compute is another cloud service provider owned by a private firm, Cybernet, which was established in 1997 in Pakistan. The firm has a widespread network of its own fiber, making it one of the biggest ISPs in the country. Besides providing internet services, the company provides various IT solutions including cloud services to a large number of its customers. May 2012 Cybernet, an enterprise network and data service provider, has launched Pakistan’s first commercial cloud infrastructure Rapid Compute is providing private and public cloud services with internet speeds in excess of 200 Mbps to its customers.

Further, a highly protected Rapid Compute data center is located inside Pakistan, which further enhances the confidence of its customers. Scalable, flexibility of paying as you go, disaster recovery infrastructure, and use of enterprise-class hardware makes Rapid Compute a strong competitor in the market. Accelerating data using SAN devices results in delivering high performance for input/output operations. Rapid Compute owns a high performance and robust fault tolerant data center, which can allow its customers to access its data via either virtual local area network (VLAN) or virtual private network (VPN) secure connection. Higher data rates offered by Rapid Compute enhances a user’s ability to upload and download data files in a secure VPN tunnel (Rapid Compute, 2014)

Rapid Compute is now spreading its wings, and has established a strong foothold in the Lahore region, where it has opened its third Data Center. Prior to this recent expansion, the highly evolved enterprise already had two Data Centers operating in Karachi. it will not only come a step closer to the local companies based in Lahore; but can also offer city-wise redundancy for its Disaster Recovery service.

**BACKGROUND**

Disasters, either man-made or natural, can lead to expensive service disruption. As a famous proverb says: "Don't put all your eggs in one basket" using one cloud site is not a right approach to the cloud systems. In fact, any single platform may lead to interruption for whole system. One of the goals of disaster recovery planning is to omit as many of single point of failure as possible. So, each cloud needs to have an extra location for risk avoidance which is geographically separated from the original site.

In 2015, a study done by the University of Texas found that 43 percent of companies that experience a catastrophic data loss will never reopen its doors. Another 51 percent will close within two years of that catastrophic event. Only six percent of companies that experience a catastrophic data loss will recover and survive. So if you are not willing to put a data recovery management plan in place, then you are taking a huge risk. If you are reading this and these percentages, do not alarm you, then you probably either have a very strong constitution or, hopefully, you already have implemented an effective data recovery plan there.

**Internationally following big disaster faced in Data Centers**

• Disasters cause expensive application downtime

• Truck crash shuts down Amazon EC2 site (May 2010)

• Lightning strikes EC2 data center (May 2009)

• Comcast Down: Hunter shoots cable (2008)

• Squirrels bring down NASDAQ exchange (1987 and 1994)

**Meanwhile in Pakistan also disaster effect communication instead service of cloud is started very late in country.**

Cyber attacks, Terrorism, flood, earthquake, and power loss and network connectivity are most Common Disasters faced in a last five year period.

1. **Cyber Attacks**

Cyber-crime rises rapidly in Pakistan. There are about 30 million internet users with 15 million mobile subscribers in Pakistan. According to Cyber Crime Unit (CCU), a branch of Federal Investigation Agency, only 62 cases were reported to the unit in 2007, 287 cases in 2008, ratio dropped in 2009 but in 2010, more than 312 cases were registered. But unreported incidents of cyber-crime are huge in numbers

Indian hackers often hacked and penetrated the government websites of Pakistan and left derogatory messages. In “Operation Hangover” against Pakistan, cyber analysts in Norway claimed that hackers based in India have been targeting government and military agencies in Pakistan since 2010 and extracting information of national security interest to India.

“Black Dragon Indian Hackers Online Squad” defaced official websites of Pakistan People’s Party (PPP), apparently annoyed by PPP Chairman Bilawal Bhutto-Zardari’s remarks about Kashmir, Pakistan Railways, National University of Modern languages (NUML), Quaid-e-Azam Public College, Gujranwala, Pakistan Electric Power Company (Private) Limited, and National Manpower Bureau.

1. For example, an Indian hacker group called ‘Black Hats’ confessed that it was responsible for the 7 January 2016 cyber-attack in Pakistan. The latest cyber-attack had some Indian hackers retaliating after a deadly cyber-attack on the Indian Air Force base on 2 January 2016.

* Cyber attack on the bank. Earlier, some hackers allegedly from Indian origin had attacked the bank in September 2015 which caused some losses to the bank customers and the bank blocked the cards of the users. Before that, HBL changed their website portal address after facing problems and cyber attack threats in early 2015.
* 24 January 2016 Hackers, while committing cyber-crime, hacked the website of federal health ministry and left message regarding Charsadda massacre. The hackers showed solidarity with the bereaved families of Bacha Khan University attack’s martyrs and victims and reminded the incumbent government to take stern action against the terrorists. They wrote that if the government failed to punish the militants than they would take revenge by themselves. “Wake up Pakistan, its war on hearts,” the hackers wrote. On the other hand, the intelligence agencies are investigating the whole case and vowed to take the action according to the law.

1. The main objectives of modern cyber crime include destructive purposes, intelligence collection, and economic espionage. There are following main types of cyber-crime:

* E-Mail Bombing: Email bombing refers to sending a large amount of e-mails resulting in interruption in the victims’ e-mail account or mail servers.
* Data Diddling: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.
* Salami Attacks: These attacks are used for the commission of financial crimes. A bank employee inserts a program into bank’s servers, which deducts a small amount from the account of every customer.
* Denial of Service:  This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

Furthermore Since the beginning of 2014, a large number of well-recognized companies have fallen victim to cyber crime which include:

eBay,Target,Google,Apple,Yahoo! Mail,IRS ,MLB ,AT&T ,Neiman Marcus, Michaels Home Depot (retail). P. Morgan Chase

Each year the Ponemon Institute, a conductor of independent research on privacy, data protection and information security policy, releases a report on cyber attacks. This year’s report polled more than 250 companies, over 2,000 company personnel, in seven different countries, researching over 1,700 attacks that took place during 2014.

What they found:

In the U.S., the average cost per cyber attack was $12.7 million in 2014, up from $11.56 million in 2013.

In Germany companies reported the average losses of $8.13 million, up from $7.6 million in 2013.

In Japan the average was $6.9 million in 2014, compared to $6.7 in 2013

The UK companies averaged $5.93 million compared to $5.19 million

Australian companies reported an average loss of $3.9 million in 2014 compared to $3.7 million in 2013.

Based on the findings, the United States companies had the highest and costliest incidence of cyber attacks. Regardless of location however, cyber attacks are increasing and are costing more each year. Overall, there was a 10.4% net increase in attack costs from fiscal year 2013 to 2014.

1. **Terrorism**

* In year 2012, a planted bomb in Kohat damaged the structures of Ufone tower and a PTCL telephone exchange.
* In year 2009, A Pakistan Telecommunication Company Limited (PTCL) exchange was damaged when it was hit by a bomb in Wana, South Waziristan.

1. **Network connectivity issues**

* Fault in submarine cable impacts internet services in Pakistan June 2015.

Internet speeds across Pakistan plummeted after a technical fault hit the main underwater fibre-optic cable system in the Arabian Sea connecting the country to the internet.

* Internet service disrupts after a fault in submarine cable 2013

One of the international submarine cable’s (SMW4) has experienced fault in sea waters near Alexandria, Egypt which has impacted internet services in the Far East, Middle East, Pakistan, India and North Africa. The total length of the SEA-ME-WE 4 (SMW4) submarine cable system is approximately 20,000 km which consists of the main backbone across the Eastern and Western worlds and links 14 countries with 16 landing stations across Europe, Middle East and Asia plus the extension links in various countries. The international consortium of operators in the region that manages the submarine cable system is proceeding to deploy repair services to restore services at the earliest, said a press release issued here by PTCL.

1. **Fire incidents**

* February 2015, a portion of the Edgerton Road Lahore exchange of Pakistan Telecommunication Company Limited (PTCL) which was caught fire. the blaze had damaged PTCL equipment and machinery, disrupting telephone and internet services in Lahore, Faisalabad and Multan for several days. Fire in PTCL Exchange Disrupts Landline and Broadband Services in Lahore
* September 2014, a PTCL exchange on Mall Road Lahore – which is said to be the backbone of company’s DSL services in the city – caught fire, the massive fire erupted again at or around fourth floor of PTCL exchange that engulfed the entire building and surroundings. According to “The News” as many as 45,000 telephone lines and almost 25,000 internet connections were disconnected due to the fire.

1. **Flood**

# August 2010, PTCL Suffers Rs 2.5 Billion Loss Due to Floods.

Pakistan Telecommunication Company Limited (PTCL) suffered a loss of Rs 2.5 billion due to floods in different parts of the country as over 150 exchanges and 150,000 connections were damaged.

* **September 2014**

Floods have affected a large part of the PTCL network in the flood affected areas. Flood waters have not only flowed into the exchanges, but cable system has also been damaged by the gushing water, resulting in temporary disruption of services to the customers

1. **Earthquake**

# *In 2005 Earthquake , PTCL network in NWFP suffered Rs112m loss’*

The government was taking various steps for restoration and rehabilitation of the telecommunication network in the province Pakistan Telecommunication Company (PTCL) is the main service provider in the earthquake affected areas of the NWFP. According to its survey, sixteen exchanges of PTCL were completely destroyed, 37 exchanges were partially damaged and boundary walls worth of Rs. 15.48 Million was destroy/damaged due to the earthquake. The total loss calculated by the PTCL is around Rs. 45.30 Million. Being a profit oriented entity; it is going to rehabilitate its services from its own resources.

**DATA ANALYSIS / METHOD**

**Research Methodology**

To frame the main research design the following research questions aim to be answered:

• Should be possible to integrate organization legacy systems into a common infrastructure that will be

able to work as one in case of failure?

• What shall be the requirements, the problems to tackle, critical business processes, licenses needed

and system maintenance?

• How to support business continuity in case of failure?

• How to maintain the system running in order to support decision-making and reporting?

The research methodology used was action-research and it involves the process of actively participating in an organization change situation whilst conducting research. This was done by the researcher while be a member of team as part of a community of practice, as it is the whole organization. Action research can also be undertaken by larger organizations or institutions, assisted or guided by researchers, with the aim of improving their strategies, practices and knowledge of the environments within which they practice. This was also done, when dealing with technological issues in order to design and discuss an implementation solution.

In this section, research methodology used to answer formulated research questions will be discussed giving a clear picture of experimental setup.

The purpose of research methodology is to provide scientific way to solve research questions. It includes pertinent research methods and approaches in finding solutions for research problems .

This master thesis has been supported by investigative approach to solve research questions and objectives. Investigative study is an important means in looking for new understanding, figuring out patterns and clearing up research problems [26]. The different research methods used are literature review, survey and case study. In the elementary stage literature review was conducted to gain knowledge of existing backup and recovery strategies and their challenges in enterprises. An online survey was conducted with professionals in the field of Backup and DR to find challenges faced by them. A questionnaire has been prepared based on literature study for an online survey. To gain better understanding of the research a case study was conducted.



Figure 6, Research Methodology overview

**1 Literature review**

Literature review is an elementary and crucial step for research. By literature review, we can analyze, and assess problems pertinent to research area. Literature review can be based on scrutinizing scientific articles, books and other sources.[27], [28]. According to Kitchenham[28] literature review can be endeavored not only for identification of 16 research gap but also to epitomize existing technologies in an intensive and impartial way. By using literature review, Backup and DR technologies are analyzed and a questionnaire was prepared.

For relevant scientific articles and books various databases were referred to, which include BTH Archive Ex, ACM digital libraries, IEEE Xplore, Inspec/ Compendex, were used. The search strategy described by Kitchenham [28] was pursued. The search without any limitations included different whitepapers released by companies, scientific journals and online reports found on Internet.

The objective of this thesis is to find an optimal Backup and DR system for a large FMCG Company by understanding current trends followed by different enterprises. The current trends will be understood by analyzing various white papers released by enterprises. These white papers are authentic documents released by the enterprises, as current trends are scarcely present in scientific journals.

**2 Survey**

In investigative research, for accumulation of data the most common way used is survey. Information gathered from survey is valuable in creating relationship of research variables and conceivable purposes behind specific trend.[26].

The questionnaire for online survey was prepared based on literature study. It was aimed to extract different challenges faced by enterprises using their existing technologies. The interested colleagues made changes in questionnaire according to various informal discussions before conducting it online.

**3 Participants of survey**

For handling of survey, web based survey tool Google forms was used. It is a user-friendly survey tool. Microsoft excel and Google spreadsheets are used for the analysis of results. Answers for questions are availed in pie chart in appendix A. The participants of this survey were Backup and DR experts, working in different enterprises.

For choosing participants in the survey, we have attended several seminars conducted by Backup and DR providers.

**4 Research Questions**

1. What are the challenges faced by enterprises using different Backup and DR systems?

2. What is the time taken for backup and recovery operations in a disk-based Backup and DR system and how can they differ from a cloud-based Backup and DR system?

3. How can we assess the performance of existing Backup and DR systems in terms of performance metrics such as RPO, RTO and Total Cost of Ownership?

Furthermore, Pakistan Telecommunication (PTCL) to conduct my case studies because they were using Cloud Computing in their company. Research did not select more enterprises for the case study because of the lack of resources. Another motive to choose PTCL enterprise was, because it was easier to get contract for case study and information from people. No doubt, conducting interview in PTCL was same as of some other enterprise.

This research have chosen a qualitative method and researcher aim was to get both the overall understanding of the information system of enterprise and Cloud Computing along with the perceived benefits and drawbacks related to them, hence, the most suitable method was to conduct semi-structured interview.

The first interview, this research took in PTCL focused about on the Cloud Computing and the cost effects on enterprises.

Research formulated an interview guide which can be found on Appendix A, Appendix B and Appendix C.

1. Interview started with introduction questions followed by general view of Cloud Computing.

After the general questions I developed particular and direct question about the cost effect on enterprises related with my theory part i.e. cost model, enterprise size, elasticity and administration cost etc.

1. The second interview with the same employee of PTCL focused on security problems of Cloud Computing for enterprises. This interview began with the general questions about security and following with the specific questions like completion of security, data connection encryption, TLS, security for different models of Cloud Computing, and governance issues. In interview also designed the questions around the advantages offered to enterprise by Cloud Computing including centralized data, audit and effective, suitable information.
2. Third interview was conducted in the Cyber net cloud ISP, has focused on the point of view of the Cloud Computing provider. The interview was more a general interview for both compression and security in the actual cost of the current market.

The next step was to arrange an interview to convert speech to text. It was an important issue to take care of the reliability and validity of the transfer.

Physical Separation

Based on your risk assessment of the potential disasters what is the minimum level of physical

separation you require between your live and DR systems? Options to consider include:

• Different building

• Different campus

• Different town/city

• Different area of the country

• Different country

• Different continent

Acceptable Downtime

The initial reaction from many IT managers and business managers is that no downtime is acceptable.

However, if the building containing your primary data centre and finance department burns to the

ground it will take time for the finance team to be relocated to different premises, it will take time to

find computers for them to use etc… therefore how quickly do you really need to restore access to your

finance system?

Acceptable Data Loss Window

Whilst zero data loss is certainly desirable as the level of synchronicity between live and DR systems

increases so do the costs, either in terms of the technology required or bandwidth utilised to maintain

synchronicity.

Databases which handle real time transactions, such as on-line or face-to-face enrolments, normally

require a small data loss window, ideally the window should be no more than a handful of transactions.

If you lose a day of transactions can you recreate that data? Does the person who enrolled via your

website know you have lost their data? Do you even know who they are?

For other systems a high window may be more acceptable, what would be the impact of losing the last

3-4 hours of data from your file servers? Is this any different from someone forgetting to press save and

losing a file?

Capacity/Performance

What sort of capacity and performance is acceptable for your DR services? Thought needs to be given as

to whether your DR services need to give your users the same level of performance as your live systems.

Your DR system may introduce new bottlenecks to the mix such as available WAN/internet bandwidth

between DR facilities and users. The amount of expansion capacity and historical capacity also needs to

be considered.

Acceptable Restoration Time

If you have had to activate your DR services at some point you’ll want to switch back to your live

services. How will you do this? Will the failback result in any downtime?

The answers to many of the questions you will need to ask yourself will vary from system to system.

The Cloud Options

Maintaining DR facilities can be expensive, both in terms of investment in hardware, hardware which

you hope you will never need to use, and time to maintain and administer the DR hardware. Use of the

cloud to host your DR facilities can eliminate or reduce a number of these costs.

Most major Cloud providers have globally dispersed redundant data centres which that will generally

be hundreds of miles away from your facilities.

• **Infrastructure as a Service (IaaS)**

Selection of an IaaS option will remove the need to invest in hardware and construct a secondary

server room/data centre. An IaaS DR solution involves renting sufficient computing resources from

a cloud provider to allow you to create a “virtual data centre” in the cloud. You are then responsible

for creating and maintaining the virtual machines which provide your DR facilities.

• **Platform as a Service (PaaS)**

With PaaS the cloud provider is responsible for the hardware, operating systems and services.

This removes the need for you to maintain and patch virtual machines. An example of PaaS is

the Microsoft Azure SQL Database service, Microsoft are responsible for the hardware, operating

systems and SQL Server installation, you only need be concerned about your database.

In some cases you may be forced down an IaaS route due to the need to install 3rd party software on a

server, in other cases PaaS may be appropriate. For example, you may need to use IaaS for your finance

system DR as you need to install a 3rd party finance server product but you can use PaaS to provide DR

for your website.

**Alternatives to Disaster Recovery - Software as a Service (SaaS)**

When looking at the services for which you need to provide DR facilities it is worth asking the question

of whether there is a better way to deliver those services. By moving services such as e-mail from

traditional on-premises hosted solutions to cloud hosting you obviate the need to invest time and money

in providing DR facilities for those services, the availability and accessibility of those services becomes

the cloud providers concern.

Selecting a Cloud Provider

Platform

The cloud is a growth area within the IT sector that is rapidly expanding, both in terms of services

offered and companies providing those services. Some providers have invested in the development of

proprietary platforms, such as Amazon E2C or Windows Azure, whilst other providers have developed

services based on “off the shelf” products, such as VMWare.

Compatibility

Compatibility between your cloud provider’s platform and your on-premises virtualisation platform can

affect the options available for your data replication strategy. If the two platforms are compatible or can

be managed by the same virtualisation management platform, such as Microsoft System Centre Virtual

Machine Manager, you may be able to move, or replicate, data and virtual machines between your onpremises

solution and your cloud solution.

Compliance

The requirements of the Data Protection Act (1998) are often cited as being a barrier to the use of the

cloud, in particular the need to obtain subject consent prior to transferring data outside of the EU. You

should not assume that because a cloud provider is based in the UK, or Europe, that your data will be

stored within the EU.

Most major cloud providers have data centres located within the EU and some allow you to select the

“region” or even individual data centre that will be used to store your data.

Security

Physical

Reputable cloud service providers should be able to provide information on the levels of security

accreditation to which their services and data centres comply. Many providers will be delivering services

to customers in the financial, health care, defence sectors as well as local and national governments and

as such will already comply with extremely stringent security requirements.

Connectivity

For your data to reach the data centres of your chosen cloud provider it will probably need to travel

across the public internet. It is important to ensure that the data is protected in transit.

Most SaaS and PaaS solutions have been developed from the ground up as internet services and will

make use of SSL & HTTPS to provide secure connectivity. For example HTTPS to connect to a web based

SaaS e-mail solution or SFTP to transfer files to a PaaS hosted website.

IaaS services typically require Virtual Private Networks (VPN) to connect the hosted virtual machines to

your on-premises LAN. Site-to-site VPN’s require a device at both sites to “terminate” the connection,

therefore it is important to confirm that you have a suitable end point device capable of handling your

end of the connection and that the device will work with your cloud providers VPN implementation.

Pricing Model & Contract Offerings

Is it necessary for all of your DR assets to be operational 24x7? or do you simply need them ready and

waiting to be fired up?

Most cloud providers pricing is based on the size, allocated storage and hours of usage of a virtual

machine. Applications which are built around an n-tier model will have application servers that host

websites or application software. You may only need to fire up the virtual machines hosting these

application server roles for a few hours a month for testing and patching. Does your cloud providers

pricing structure reflect this usage model?



Understanding Risk

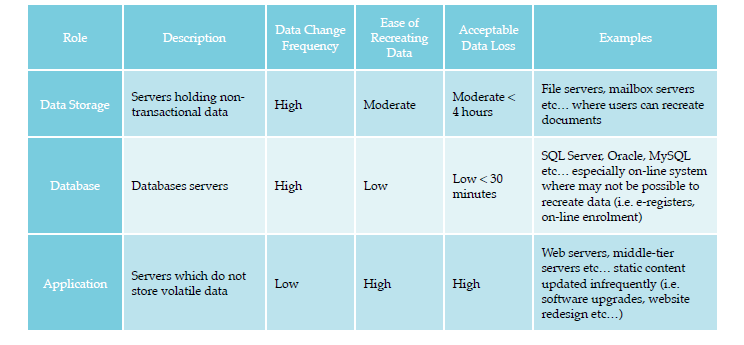
An analysis of the roles and workloads of your systems will help you to identify the level of risk that the

loss of a system poses and therefore the level of DR protection and effort that it warrants.

Systems are often comprised of multiple servers each fulfilling distinct roles. The impact of loss, and ease

of restoration, will vary depending upon the role of the server.

Suggested role are listed below:



Data Replication Strategy

Obviously it is necessary for the data in each of your DR systems to be updated regularly and to be no

older then the acceptable data loss window you have identify for that system. It is important to select a

replication method that is appropriate for the level of risk and acceptable data loss window.

Approaches

**Application Replication**

Many enterprise class applications incorporate their own replication technologies, for example,

Microsoft Exchange Database Availability Groups, Oracle Data Guard, MySQL master/slave replication

etc… Where application replication technologies are available they should be considered as the preferred

option as they are designed to replicate data in a manner that makes sense to the application.

**File System Level**

In some cases simply copying files from the live systems to the DR systems will suffice to replicate

the data.

Tools such as “robocopy” and “rsync” are able to intelligently determine what differences exist between

source and destination locations and only copy new or changed files to the DR location as well as

removing redundant files from the DR site. Services such as the “Distributed File System” (DFS) built

into Windows server can be used to automate and manage file replication.

It is important to check that a file system copy is appropriate for the type of data being replicated.

Using file system replication to copy the data files of your SQL Server whilst it is running could result

in data corruption.

**Virtual Machine Replication**

Replication or cloning of entire virtual machines is also a strategy that should be considered. This is

especially useful for cases where all the components of a single system are located on a distinct virtual

machine. This approach should also be consider for application/middle-tier servers where significant

time and effort has been expended customising or configuring the middle-tier components.

Best Approach

Complex systems often consist of multiple servers each of which has a distinct role within that system.

Consider a student records system, this will probably consist of a database server, two identical

application servers and a client application. Your database will be experiencing constant changes

and you need to ensure that in the event of a disaster you don’t lose any records, on the other hand

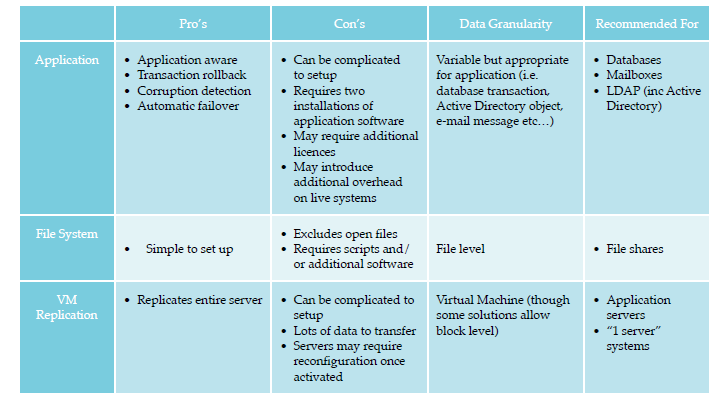
the software on the application servers is updated via a controlled process every 6 months when the

software vendor releases an update. In this scenario it would be appropriate to make use of the database

systems inbuilt replication technology to protect your database and to use virtual machine replication to

replicate one of the application servers, you might only replicate the virtual machine once a month as it

has a low degree of data volatility.



Considering Failover

If you have to activate your DR facilities how will your users and client devices know where to find the

systems they need to connect to?

Most modern networks make use of DNS to locate servers and services, in some cases you may be using

IP addresses to locate services. It is probably that your DR facilities will be on a different IP subnet from

your live systems, your clients need to be informed of this to allow them to connect to your DR facilities.

**Active Directory & DNS**

Assuming that you are utilising Microsoft Active Directory (AD) the servers on your DR site will need

access to the AD and associated DNS in order to operate. Therefore it is recommended that you maintain

at least one operational Domain Controller in your DR facilities. This will also provide inherent DR for

your AD and DNS infrastructures without any further work on your part.

**IP Address Allocation**

If you have chosen to replicate virtual machines to your DR site do these virtual machines have static IP

addresses assigned? If so you will need to login to each VM as you bring it online and assign a new IP

address. Consider whether you can use DHCP to assign IP addresses to your servers.

**Application Aware Failover**

If an application has some form of application level replication it may also have application level

failover. Microsoft Exchange Database Availably Groups (DAG) are such an example, with DAG’s the

Exchange client access servers automatically connect to the mailbox server which is hosting the active

database.

**Distribute File System (DFS)**

Switching to an alternate file server normally involves finding all references to the UNC path of the

failed file server and replacing them with references to the new file server.

DFS allows the creation of a fault tolerant file share containing folders that refer to one or more real file

shares. By configuring an active and inactive referral for each file share, one referencing your live system

and the other your DR system, all you need do to failover is change the referrals appropriately.

12 Utilising the Cloud for Disaster Recovery

**DNS for Failover**

It is assumed that you have created a Domain Controller in your DR site that is also a DNS server, thus

providing resilience for your DNS. Most of your clients will be using DNS to locate the servers and

services to which they connect, in many cases switching to your DR facilities may involve no more than

changing DNS entries so they point at the DR system.

Consideration needs to be given to the TTL value of the DNS entries as these determine the length of

time your clients will cache the returned DNS data. If your records have a TTL of an hour it could take

that long before some of your clients can access your DR services. You should ensure that the TTL values

for the critical DNS records are set to values that are consistent with your failover objectives.

When planning for DR it is recommend to review the way your clients currently locate their servers,

where possible try to avoid the use of IP addresses or server names and use DNS aliases (CNAME)

records. For example, instead of using http://servername.college.ac.uk/ebs create a DNS CNAME for

ebs-live.college.ac.uk which refers to servername.college.ac.uk that way if you have to switch to your DR

system all you need do is update the CNAME record.

**Replicated Virtual Machines**

In most cases failover of replicated VM’s will be as simple as powering on the VM, checking it has an

appropriate IP address and ensuring that DNS reflects the current IP address.

Where the VM is a part of a multi-tier application and you have also failed over database tier

components you may need to update the application with the new address of the database server. This

process can be simplified through the use of DNS aliases and application specific redirects, for example,

you might create an DNS alias for “studentrecords-live.college.ac.uk” which points at your live database

server, you then use this address when installing/configuration application-tier components, in the

event of failure all you need to do is change where the DNS alias points.

**Network Load Balancers**

Network load balancers (NLB) provide an option for failover of some services, good quality load

balancers will be able to detect server and application failure automatically and redirect traffic. However,

you also need to consider DR for your NLB, if you position an NLB on your live site which is configured

to redirect traffic to your DR site what will you do if your NLB is out of action?

Planning

Once you’ve carried out your risk assessment you will have a better idea of the disasters that you may

encounter and the how what the probability of each disaster is. As you have hopefully realised you are

probably more likely to encounter situations where one, or a small number, of related systems have

failed, probably as a result of hardware failure or software problem. The level of detail involved in your

DR plan should reflect how critical the system is and how quickly it needs to be recovered.

You may have generic processes that apply across multiple systems, for example, if you have multiple

database servers with identical DR processes a single process is probably sufficient.

Whilst it is possible to create detailed scripts and automated procedures that can be sued to activate DR

facilities every disaster tends to be different and needs to be assessed individually. The process to fix a

disaster of type A may in fact make a disaster of type B worse.

Utilising the Cloud for Disaster Recovery 13

The best approach is to take a scenario based approach, start with the highest probability & highest

impact risks and work down to those with the lowest probability and impact.

An important consideration in your planning is who has the authority to declare a “disaster” and invoke

the DR plan? In some cases invoking the DR plan may result in more overall disruption then it would to

leave a particular service offline for an hour while you fix it.

Testing

It is essential to test your DR processes regularly. The scope of testing needs to be considered on a system

by system basis, also consider if you need to test every system? again if you have 20 servers with an

identical process do you need to test them all regularly?

For systems with transparent application level replication and failover testing should be straight forward

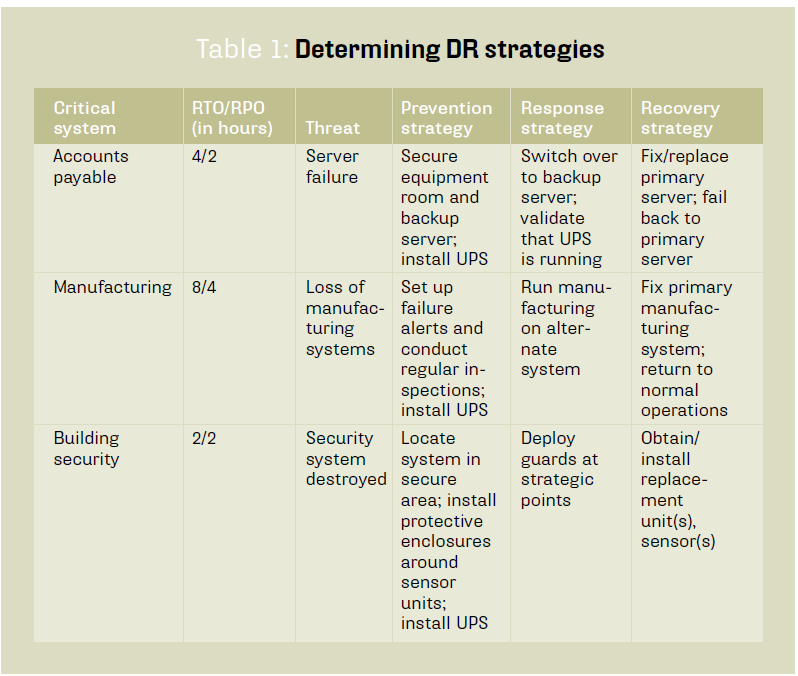
and can be done regularly. In cases where a failover would be disruptive is simulating failover sufficient

for the system in question?

**DEVELOPING DISASTER RECOVERY STRATEGIES**

Regarding disaster recovery strategies, ISO/IEC 27031, the global standard for IT disaster recovery, states, “Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place.”

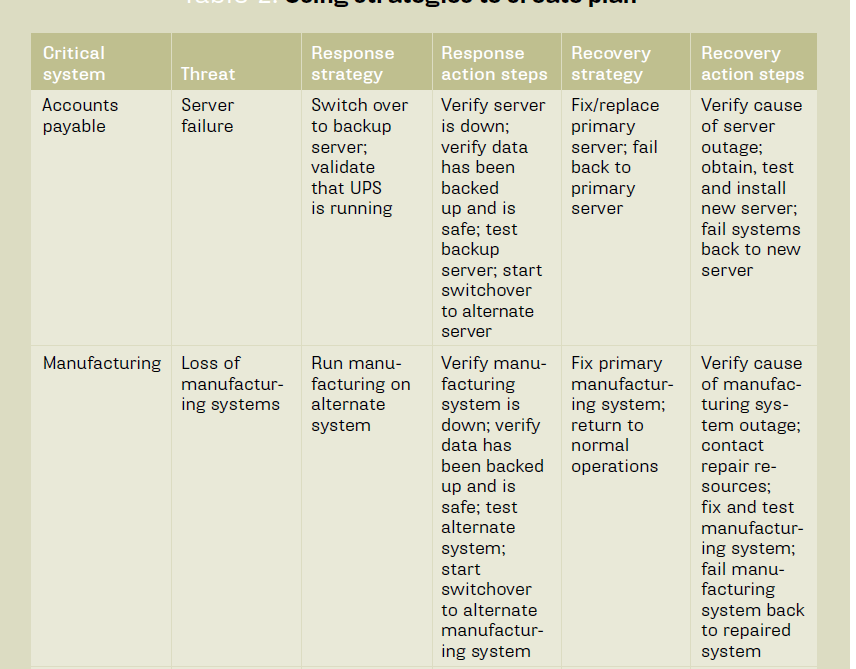
Strategies define what you plan to do when responding to an incident, while plans describe how you will do it. Once you have identified your critical systems, RTOs, RPOs, etc, create a table, as shown below, to help you formulate the disaster recovery strategies you will use to protect them. You’ll want to consider issues such as budgets, management’s position with regard to risks, the availability of re-



Sources, costs versus benefits, human constraints, technological constraints and regulatory obligations.

**TRANSLATING DISASTER RECOVERY STRATEGIES INTO DR PLANS**

Once your disaster recovery strategies have been developed, you’re ready to translate them into disaster recovery plans. Let’s take Table 1 and recast it into Table 2, on p. 9. Here we can see the critical system and associated threat, the response strategy and (new) response action steps, as well as the recovery strategy and (new) recovery action steps. This approach can help you quickly drill down and define high-level action steps.



From Table 2 you can expand the high-level steps into more detailed step-by-step procedures, as you deem necessary. Be sure they are linked in the proper sequence.

**DEVELOPING DISASTER RECOVERY PLANS**

DR plans provide a step-by-step process for responding to a disruptive event. Procedures should ensure an easy-to-use and repeatable process for recovering damaged IT assets and returning them to normal operation as quickly as possible. If staff relocation to a third-party hot site or other alternate

space is necessary, procedures must be developed for those activities.

When developing your IT DR plans, be sure to review the global standards ISO/IEC 24762 for disaster recovery and ISO/IEC 27035 (formerly ISO 18044) for incident response activities.

**INCIDENT RESPONSE**

In addition to using the strategies previously developed, IT disaster recovery plans should form part of an incident response process that addresses the initial stages of the incident and the steps to be taken. This process can be seen as a timeline, such as in “Disaster timeline” (below), in which incident response actions precede disaster recovery actions.

**THE DISASTER RECOVERY PLAN STRUCTURE**

The following section details the elements in a DR plan in the sequence defined by ISO 27031 and ISO 24762.



*Important: Best-in-class DR plans should begin with a few pages that summaries key action steps (such as where to assemble employees if forced to evacuate the building) and lists of key contacts and their contact information for ease of authorizing and launching the plan.*

**1. Introduction.** Following the initial emergency pages, DR plans have an introduction that includes the purpose and scope of the plan. This section should specify who has approved the plan, who is authorized to activate it and a list of linkages to other relevant plans and documents.

**2. Roles and responsibilities.** The next section should define roles and responsibilities of DR recovery team members, their contact details, spending limits (for example, if equipment has to be purchased) and the limits of their authority in a disaster situation.

**3. Incident response.** During the incident response process,we typically become aware of an out-of-normal situation(such as being alerted by various system-level alarms), quickly assess the situation (and any damage) to make an early determination of its severity, attempt to contain the incident and bring it under control, and notify management and other key stakeholders.

**4. Plan activation.** Based on the findings from incident response activities, the next step is to determine if disaster recovery plans should be launched, and which ones in particular should be invoked. If DR plans are to be invoked, incident response activities can be scaled back or terminated, depending

on the incident, allowing for launch of the DR plans. This section defines the criteria for launching the plan, what data is needed and who makes the determination. Included within this part of the plan should be assembly areas for staff (primary and alternates), procedures for notifying and activating DR team members, and procedures for standing down the plan if management determines the DR plan response

is not needed.

**5. Document history.** A section on plan document dates and revisions is essential and should include dates of revisions, what was revised and who approved the revisions. This can be located at the front of the plan document.

**6. Procedures.** Once the plan has been launched, DR teams take the materials assigned to them and proceed with response and recovery activities as specified in the plans. The more detailed the plan is, the more likely the affected IT asset will be recovered and returned to normal operation. Technology

DR plans can be enhanced with relevant recovery information and procedures obtained from system vendors. Check with your vendors while developing your DR plans to see what they have in terms of emergency recovery documentation.

**7. Appendixes.** Located at the end of the plan, these can include systems inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data, and any additional documentation that will facilitate recovery.

**DISASTER RECOVERY OF CLOUD STORAGE**

While applications and data services are transparent, malicious attacks must be avoided. It is important and difficult to ensure data security in cloud storage system. It is necessary to establish fault tolerant function in less cost for cloud storage. The fault tolerant function can overcome single point failure and avoid data loss. At the same time, there must be fault-tolerant backup system, which can ensure that data have a reliable backup if they are lost due to force majeure.

In order to satisfied the continuity of application and the security of data, the structure of disaster recovery system is "distributed computing, centralized storage".

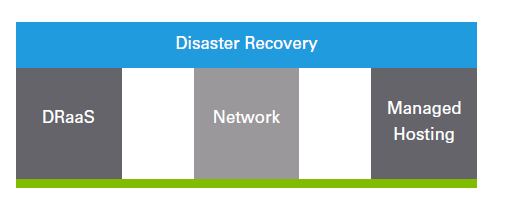
According to different requirements, disaster recovery has three levels.

They are data-level disaster recovery, system-level disaster recovery, and application-level disaster recovery.

1. Data-level Disaster Recovery
2. System-level Disaster Recovery
3. Application Level Disaster Recovery

* **Three pillars of effective disaster** recovery

The technology industry overuses architectural metaphors such as “framework,” “foundation” and “platform.” This white paper adds “pillar” to the list but appropriately so as modern Disaster Recovery does in fact have essential components upon which it must stand.



1. The first pillar is Disaster Recovery-as-a-Service (“DRaaS”). DRaaS a cloud-based service with computing and storage resources to back-up data, run applications, test/simulate disaster events and manage the migration of services.
2. The second pillar is Networking. Since DRaaS is a cloud-based service network connectivity is a must-have. In fact, in the context of DRaaS there are two networking choices: robust network connectivity and failure.
3. The third pillar is Managed Hosting the server, networking and other infrastructure that is owned and operated by a third party provider in their data center specifically to support your applications and related services. Many organizations used Managed Hosting to reduce CapEx, outsource system management and take advantage of contractual Service Level Agreements. Managed Hosting is a pillar of the Disaster Recovery puzzle because in the event of a catastrophe business continuity may require you to run applications out of an offsite data center in conjunction with replicated data, also stored offsite

**FURTHER ACTIVITIES**

Once your DR plans have been completed, they are ready to be exercised. This process will determine whether they will recover and restore IT assets as planned. In parallel to these activities are three additional ones: creating employee awareness, training and records management.

These are essential in that they ensure employees are fully aware of DR plans and their responsibilities in a disaster, and DR team members have been trained in their roles and responsibilities as defined in the plans. And since DR planning generates a significant amount of documentation, records

management (and change management) activities should also be initiated. If your organization already has records management and change management programmes, use them in your DR planning.

Offerings in the DR space fall into one of three categories:

do it yourself (DIY), DR as a Service (DRaaS) or cloud-to-cloud disaster recovery (C2C DR).

**1. Do it yourself (DIY):** DIY providers offer managed hosting, cloud, colocation and other data center services. Many don’t have a DR-in-the-cloud offering, but their services can be leveraged for companies to build their own recovery cloud. Since most companies lack the internal expertise to architect and manage an effective DR solution or add DR responsibilities to internal teams that are already struggling to maintain existing IT responsibilities, DIY may not be the best or most cost-effective solution.

**2. DR as a Service (DRaaS):** DRaaS providers can provision, configure and test an effective DR plan. DRaaS vendors provide a standard DR failover to a cloud environment. Businesses can buy on a pay-per-use basis with varying rates based on recovery time and applications being spun up during a disaster. DRaaS providers replicate data and applications or use image-based backups to send data to the cloud.

During a disaster or for testing, businesses’ production environments can be run out of the cloud because the DRaaS vendor is less likely than the business to suffer the effects of a disaster.

**3. Cloud-to-cloud disaster recovery (C2C DR):** These providers offer the ability to failover infrastructure from one cloud data center to another, either within a single vendor’s environment or across multiple vendors.

**TRENDS OR EXISTING APPROACHES OF BACKUP OR DISASTER RECOVERY**

**There are different types of backup techniques, Full back up, Incremental backup, differential backup, and the combination of these backup techniques.**

**1.1 Full backup**

Creating a copy of an entire file system to another set of media is said to be full backup. In this type of backup, each and every folders and files are backed up on selection.

It is the easiest way of generating a backup. In Figure 1, all files are present in local drive and backed up to other set of media. In this type of backup, all the files backed up will be present in one place. The major advantage of this backup type is restoration of data takes lower amounts of time than other backup techniques, and it has good storage management, as backup files are stored in a single file. This being the reason, a full backup requires longer time and larger storage space. The full backup is used by companies which have less data growth from day to day[14].

**2.2 Incremental backup**

In this backup, the files that have been newly created or modified since previous backups are copied. It tracks and records the previous backup time, and checks time stamp while backing up and only backs up data that has been changed since the previous backup[15].

It is the fastest backup technique and requires less space as it backups only the newly created or modified data. But when it comes to recovery it requires more time and to restore individual file, initially one has to search for the file.

**2.3 Full + Incremental backup**

This type of backup is combination of full back up and incremental backup. First day full backup is conducted and from the next day incremental backup are performed.

In this backup technique, initially a full backup is done, where each and every file is backed up. In the above figure, A, B, C, D, E, and F are different files present on a disk. During a full backup, all these files are backed up to backup media. On day 2, G 11 and H are added to the disk. In the incremental backup it backs up only the newly added data or modified data. Only G and H are backed up to the media. On day 3, I, J and K are added and D file is modified to the day 2 data, by doing the incremental backup D, I, J and K are added to the backup media. In this type of backup, it requires less data space in backup media and requires less time to backup. But when it comes to recovering day 3 data, all backup media from day 1 are required. Without the previous backup media, day 3 data can’t be restored making recovery process complex. This type of data can be used when there is small backup window, as it takes less time to backup.

**2.4 Differential Backup**

A differential backup, backs up only data that has changed or newly created since previous backup. Differential backups are cumulative, which aggregates all changes from previous backup. The data size on backup media after a differential backup grows day by day. In case of restoration, incremental backup requires each and every backup media conversely differential backup requires only the latest differential backup media for a full restoration[16].

**2.5 Full + differential Backup**

This type of backup is a combination of full back up and differential backup. Combinational backups reduce the space occupied on backup media and time taken for backup is diminished.

Figure 3, Full and Differential backup[13]

In full + differential backup, on day 1 full backup is performed, where each and every file of the file system is backed up. In above figure, A, B, C, D, E, and F are different files present on a disk. During a full backup, all these files are backed up to the 12 backup media. On day 2, G and H are added to disk. In differential backup it backs up only newly added data or modified data. So, only G and H files are backed up to the media. On day 3, I, J and K are added and D file is modified to day 2 data. In case of incremental backup, only D, I, J and K are backed up but in case of differential backup, newly created or modified data from last full backup is backed up, it means D, G, H, I, J and K are backed up to the media. It requires moderate data space in backup media less than full backup, slightly more than incremental backup. But when it comes to recovery, the day 3 data can be restored from backup media of day 1 and day 3. This type of backup can be used when there is less rate of change of data.

**2.6 Synthetic backup**

The standard backup, which is the very first copy of a full backup and the subsequent incremental or differential backups create synthetic backup. The synthetic backup is nothing but a consolidated form of existing full backup copy and consecutive incremental/ differential backups[17].

**2.7 File Level Storage**

NAS users generally use file level storage. The file level storage is a centralized network to store all files, folders with easy access and high availability. It is comparatively inexpensive and is a storage system that enterprises look for without any complexity in management [18].

If high performance is a requirement of enterprise, then the block level storage will be more effective in comparison to file level storage.

If there is a requirement for both levels of storage then a hybrid model with both file and block level storages can be used.

**2.8 Block Level Storage**

Block level storage is generally used by Storage area network, SAN users. Block level storage can be compared to a hard drive connected remotely and makes use of Fiber Channel and iSCSI connectivity mechanisms of industry standards.

It is known for its pliability and adaptability as the blocks of storage volumes are created and these are individually accessed.

Block level storage has a complex manageability. It is difficult to directly access the small blocks containing files and folders [19].

**2.9 VM Level Backup**

In VM level backup, the complete Virtual machine is backed up. Every time there is a change, it is required to back up the whole VM and restoration from this is tedious as each file is read in the entire backup copy.

**2.10 JBOD**

JBOD stands for just a bunch of disks. It is a collections of disks kept at a backplane. It doesn’t have any front-end logic to manage distribution of data among disks; it represents each disk as a separate resource. JBOD can be used as direct attached storage to the host server or it can be used as storage array as in Network attached storage or with fiber channel interface can be used in storage area networks[20][21].

Depending upon the type of JBOD system using there are different types to connect disks in JBOD. Based on that there are SCSI and Fiber channel. The SATA/ SAS is 13 Serial attached SCSI, has a point-to-point connection with SATA/SAS port expander, which can remove the fan out problem by allowing one host controller to connect to different disks. In this thesis we have used SCSI disks.

Figure 4, SATA/SAS JBOD[21]

**2.11 AWS direct connect**

AWS direct connect provides a devoted connection between enterprise data center and AWS cloud. It is different from the VPN as, VPN utilizes WAN while in AWS direct connect, a private connection is established from the on premise data center to AWS. By using this, network costs will be reduced and bandwidth throughput will be increased [22].

**2.12 Performance metrics**

The performance metrics we considered here are RTO, RPO, Total cost of ownership, time taken to backup and time taken to recover.

RPO and RTO are the most important recovery objectives for any enterprise prior to planning a Backup and DR solution for the company.

Total Cost of Ownership is the expenditure spent by enterprise, it plays a vital role in deciding what requirements are to be fulfilled on a undoubtedly and which may need not be of high priority

Time take to Backup and Time take to recover are compared with the same underlying infrastructure but different Backup and DR to understand which solution performed better.

**2.12.1 RTO and RPO**

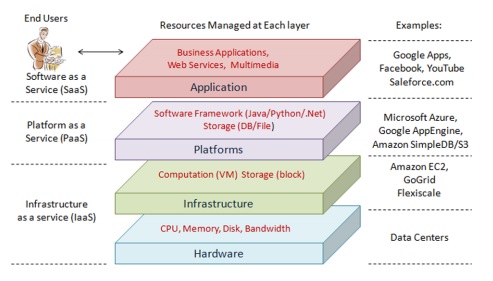
RTO stands for recovery time objective and RPO stands for recovery point objective. 14 Figure 5, RPO and RTO[23] RTO and RPO are important terms related to recovery operation. RPO is the time between two backup operations. In other terms it is the maximum allowable data loss. By analyzing the RPO values we can get to know the frequency at which backup operation is performed. In asynchronous replication, data is backed up to backup media whenever there is a modification or newly creation. In this case RPO value is zero[2]. RTO is maximum permissible time for an application or data to not be available. It is the maximum time that is required for an application or a file to be available again after occurrence of a disaster[24].

**Need plans and systems in place to recover from disasters**

A key concept in a DRP is the physical separation of the primary and backup sites. A significant fraction of disasters including those caused by outages are geographical as shown in the below.

**Problem Statement and Model:**

Based upon the type of resources assigned to the cloud user’s by the cloud service provider are classified into three service models. They are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) [4]. Other services offer by Cloud computing are; Data as a Service (DaaS), Identity and Policy Management as a Service (IPMaaS), Network as a Service (NaaS). Figure 1, depicts the three most commonly used cloud services, the resources managed at each layer and examples from real life.



**Figure 1: Cloud computing service model [5]**

According to latest trend or common disaster in country shows that a disaster is any unlooked-for incident threatening the personnel, buildings, or normal operational structure of an organization which is beyond the immediate ability of the organization’s staff and normal management structure to control.

The biggest threats to most organizations are from fire, robbery or damage. Serious storms, floods or water escape from other sources can also have a major impact, especially if premises are in low-lying land near a river and important equipment, machinery or computers are sited on the lower floors. Some businesses are at risk from terrorists because of their links with certain overseas countries. And all premises and employees are at risk, from falling aircraft, chemical or nuclear pollution, disease or personal attack [6].

Disaster Recovery has always been about dealing with a single disaster or potentially disastrous situation. Every organization must have a disaster recovery plan (DRP) which is testable, executable, maintainable and scalable. Such a plan must satisfy cost constraints while achieving the target recovery objectives; that is recovery time objective (RTO) and recovery point objective (RPO) [7]. The organizations involved must identify likely events that can cause disasters and evaluate their impact. They need to set the objectives clearly, and evaluate feasible disaster recovery plans to choose the optimal disaster recovery plan. Because **Cloud-based disaster recovery** can help you

bridge, as business becomes more dependent on IT, and downtime and data loss are less acceptable

Following are the main key points   
Cloud Based Disaster Recovery is best instead of Traditional Disaster Recovery

(All data according to US Industries)

* Time

|  |  |
| --- | --- |
| 24 – 72 Hours  Are required for traditional  recovery from a tape backup | ≤ 1.3 Hours  Is the recovery time objective  of best-in-class companies |

* Money

|  |  |
| --- | --- |
| **Do you know the financial impact of an IT**  **outage to your business?**  **Fact:** The cost of downtime per hour across US industries:  **Brokerage service: $6.48M**  **Energy: $2.8M**  **Telecom: $2M**  **Manufacturing: $1.6M**  **Retail: $1.1M**  **Healthcare: $636K**  **Media: $90K** | **Overall cost savings**  Enhanced reliability  Eliminates secondary or tertiary data center investments and  ongoing maintenance  Government agencies reduced DR spend by 50% after switching to cloud backup |

* Data

|  |  |
| --- | --- |
| ¾ of companies worldwide are in danger of  failing to recover from a disaster/outage  **1 in 10 organizations** indicated damage  to business reputation after data loss  **70% of SMBs** go out of business  within a year of data loss | **Enhanced Reliability**  Custom recovery point objectives from 15  minutes to 24 hours  72% of enterprise companies  and 93% of mid-market  businesses will pursue a cloud strategy by 2015 |

* Disaster Recovery Coverage

|  |  |
| --- | --- |
| 47 % rank or tier the recovery priority of business  services, leaving some applications at risk | **Elastic cloud compute and storage**  Easily scalable to accommodate growth, pay for what you need now and expand as needed |

**DISASTER RECOVERY PREPAREDNESS**

|  |  |  |
| --- | --- | --- |
| 21% of business lack the skills | 36% of businesses  lack the time | Easier DR Readiness Built-in automated  workflows for failover  testing, planned  migrations and  recovery |
| **to adequately plan for and test DR** | | 43% are getting  started with cloud  to improve their  DR capabilities |
| **1 in 4** never test their DR plans | |

* Organizations with high cloud adoption are reporting nearly:

|  |  |
| --- | --- |
| 2 X the revenue growth | 2.5 X higher gross profit growth than peer  companies that are more cautious  about cloud computing |

There are three main cloud Dister Recovery models:

1. **DATA ONLY:**

The DR process focuses on ensuring a backup copy of data is available on the cloud platform and represents the lowest level of recovery. This means protecting data such as that sitting on file servers, including home directories and shared folders. In the event of a disaster, the data can be accessed from the DR location in the cloud. Depending on the amount of data that must be restored, downtime can be significant and even require physically shipping data back to the primary site on an appliance to restore.

1. **APPLICATION-BASED.**

The DR process focuses on replicating application data into the cloud to a secondary deployment of the application. Data is moved using native application capabilities or a third-party product. Failover consists of re pointing access to the application running in the cloud (typically through DNS changes).The secondary application instance is running permanently in the cloud, receiving data on a periodic basis.

1. **VIRTUAL MACHINE IMAGE.**

The DR process replicates an entire VM image, including data, to the cloud. The VM image itself is dormant (not running) until required, at which point it can be powered up and accessed, typically through DNS changes. VM image backup can also be used as a method of protecting physical (bare metal) application deployments through P2V replication.

**CLOUD Disaster Recovery Issues**

Of course, moving to a cloud-based disaster recovery service has issues. Many of the following examples could be experienced when deploying any DR system; however, some are more particular to cloud deployments.

1. **Network bandwidth.** Bandwidth is an issue from a number of angles. First, you must have enough throughput capability between the primary site and the cloud to ensure data can be replicated in a timely fashion without too much lag in concurrency (which affects RPO). Second, you need enough bandwidth available to recover changed data back to the primary site once the DR issue is over. Third, you must be able to access services from the cloud, either from the internal business network or from the Internet with client-facing applications.
2. **Network security.** Data moving to the cloud will be outside of the protection of the private network in the data center, so it must be encrypted in flight at a minimum. Compliance or other regulatory restrictions may require data to be encrypted at rest when off-site. This can have implications on how applications are implemented on-site, to ensure that the encryption process does not interfere with normal operations.
3. **Network addressing.** As application workloads are moved to the cloud, IP addresses will change. When primary and secondary application servers are kept on-site, IP addressing can be managed relatively easily, either through implementing a level 3 network between sites or by using routing. Moving an application to the cloud will require changes to DNS (to point to the new server/data location) and modification to the application itself in some cases.
4. **Network latency.** Running applications from the cloud rather than on-site may cause performance problems due to increased latency. This can occur if only part of a service is migrated into DR with issues experienced in intercommunication between on- and off-site services.
5. **Licensing.** DR instances of applications require purchasing licenses, depending on the terms of the application vendor. These license options may be different for cloud implementations or, in the worst case, not supported.
6. **Cost.** The cost of implementing DR will include providing the cloud services, additional network capacity, licensing dedicated backup software and extra application licenses. All of these may vary depending on the way in which cloud DR is delivered.

**COMPARING CLOUD DISASTER RECOVERY SERVICES**

What should buyers look for when reviewing a cloud-based disaster recovery service?

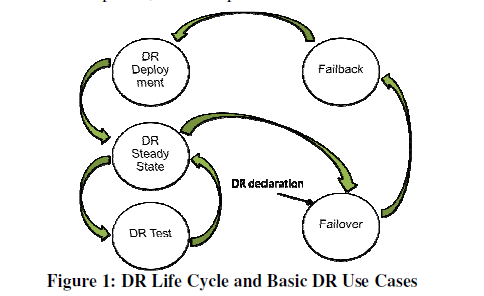
Here are a few additional pointers:

* **Cost basis.** How is the service charged; per TB of storage or per VM? Are there additional charges for running in DR mode?
* **Time limitations.** How long can I run the service in DR mode? Are there any restrictions on how many systems I can fail over?
* **How does failback work?** Can I incrementally fail back to production (take back only the changes) or do I need to restore all my data?
* **Does the service offer extended protection?** If I am in DR mode, can I also replicate my data

to a third copy until I return to production? A cloud-based disaster recovery service offers flexibility for providing data protection to on-premises environments. As applications evolve, we will perhaps see the distinction between DR and dispersed applications start to blur, with DR providing both application protection and scalability. Whatever happens, the need to provide application resiliency and data protection will always remain.

***Disaster Recovery Life Cycle***

Figure 1 illustrates the typical DR life cycle consisting of a number of phases, which map to basic DR use cases.

****

**Figure 1: DR Life Cycle and Basic DR Use Cases**

1. **Disaster Recovery Deployment** is the start phase of the DR life cycle. In this phase, the primary cloud site and the secondary site(s) are set up for supporting DR, and clients and their workloads are enrolled for DR protection. If a cloud system has distributed sites and built-in DR capabilities (which may be exposed through APIs), development of client workloads using such capabilities would also fall in this phase.
2. **DR Steady State** is the normal mode of operations, characterized by continuous data replication from the primary cloud site to the secondary site. DR-enabled machines may be modified or reconfigured in this phase, e.g. by adding new disks or installing new applications. Continual monitoring of replication and DR readiness is required in DR Steady State.
3. **DR Test** is the phase in which a client conducts tests of the recovery procedures by emulating a disaster occurrence and verifying that the procedures indeed recover workloads per SLAs. Cloud clients may demand DR testing annually, multiple times per year, or even on-demand. DR Testing is typically designed to be non-disruptive to production workloads and steady-state operations at the primary site, including data replication. Even if an actual disaster occurs during the DR test, recovery must happen correctly.
4. **Failover** refers to recovery of the primary cloud site at the DR site after a disaster has been *declared*. *DR declaration* is usually an executive-level decision, and may happen upon actual occurrence of a disaster, or even pre-emotively (e.g., a hurricane forecast). Upon DR declaration, failover procedure .Start to execute as a complete automatic process. This phase is marked by workload downtime and is bounded by RTO guarantees. After failover, clients’ workloads run on the DR site.

**Furthermore Cloud Computing Associated Risks are also needed to focus during Disaster Recovery Cycle.**

There are numerous concerns and risks associated with cloud computing. The most important risks are the three fundamental tenets of information security (i.e., the confidentiality, integrity and availability [CIA] triad). Confidentiality is the protection of data from unauthorized disclosure. This disclosure can either be accidental or intentional. Integrity is the assurance that a message or data received is in its original form, has not been modified, and is coming from a legitimate sender. Availability is the guaranteed access to data at all times without any delay, disruption or denial. Based on the CIA triad, the risks associated with cloud computing are expanded upon in the ensuing paragraphs.

1. ***Data Confidentiality and Security***

All data rests with the cloud provider in unencrypted/readable form to facilitate data processing. Hence there are chances that data may be compromised and provided to an adversary against personal interests. Since the Internet is used to access data from cloud storage, it is more prone to attacks. Incidents like the Edward Snowden leaks in 2013 have also adversely affected the cloud industry. Unauthorized use of data in the cloud by any government or other intelligence agencies has raised serious concerns among cloud consumers.

1. ***Availability of Data***

To ensure uninterrupted access to data, the cloud provider must guard against denial of service (DoS) attacks. Attacking a computer network with enormous floods of traffic and emails containing large attachment files can exhaust all resources and make it impossible for legitimate traffic to get through (Krutz & Vines, 2010). Since cloud consumers are relying on their CSP for data availability, cloud vendors must utilize highly resilient hardware and software techniques to ensure uninterrupted data availability.

1. ***Database Integrity***

Database integrity is a very important aspect of cloud computing, as the prime mover for cloud computing is management of data and associated resources. If the database is not reliable or can be modified by an unauthorized user, results will never be fruitful and will eventually lead an organization toward failure. Session hijack attacks, man in the middle attacks, replay attacks, and others can also account toward an unreliable database.

1. ***TCP Hijacking and Social Engineering***

While legitimate users are maintaining a connection with their cloud server, an attacker can hijack the TCP session and access the database. Similarly, various social engineering techniques can be employed by the attacker to capture the password or personal identification number (PIN) of the user for future use in manipulation of or access to the database.

1. ***Alignment and Integration***

Enterprise architecture requires modification to meet the CSP model for optimum utilization, thus causing an organization to modify its enterprise architecture to meet the data formats, hardware interfaces, and so on.

1. ***Control of Data***

Cloud computing is dynamic, with ubiquitous access to vast resources (Antonopoulos & Gillam, 2010). However, if the CSP faces a financial crisis, there are fair chances that hard drives from its data center will be sold on some online store like eBay or Amazon, thus causing consumers to lose control over their data.

1. ***Data Location***

If the cloud provider stores data outside the territories identified in the service level agreement (SLA), serious concerns about the privacy and security of data may arise (Antonopoulos & Gillam, 2010). Additionally, if the data center is located at a place which experiences a natural disaster, complete loss of data and infrastructure may occur.

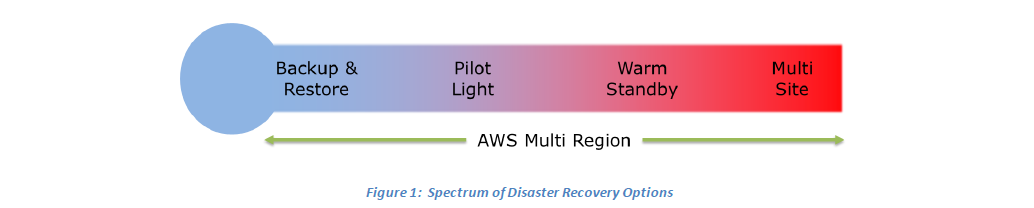
1. ***Trojan Horses and Malware***

Emails containing Trojan horses and other malware from attackers can infect user machines. These Trojans or malwares can be programmed to silently transmit all data to the attacker when the user initiates connection with the cloud server.

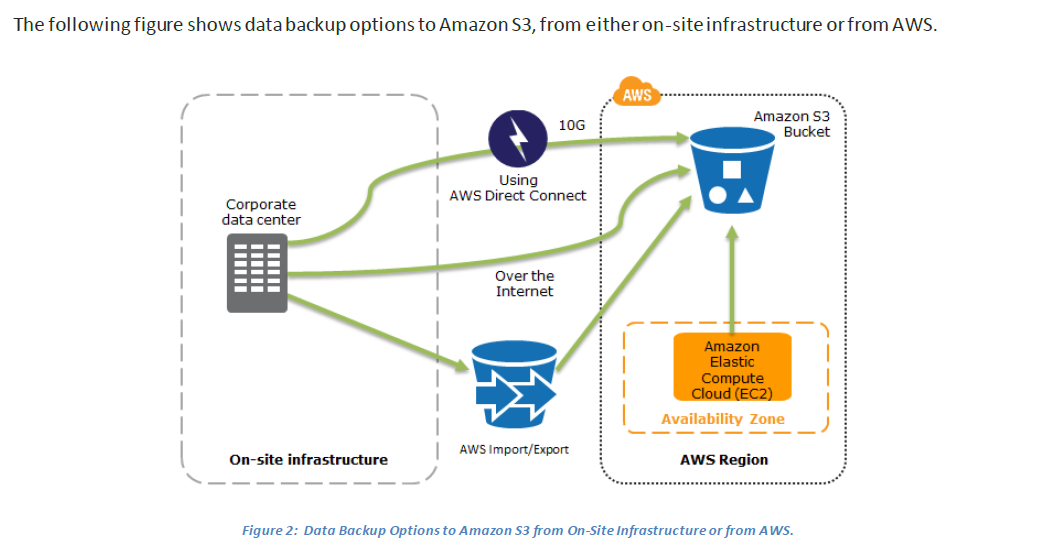
* According to AWS, “Disaster recovery is a continual process of analysis and improvement, as business and systems evolve. For each business service, customers need to establish an acceptable recovery point and time, and then build an appropriate DR solution.”
* Amazon Web Services are available in multiple regions around the globe, so you can choose the most appropriate location for your DR site, in addition to the site where your system is fully deployed. AWS has multiple general purpose regions in the Americas, EMEA, and Asia Pacific that anyone with an AWS account can access. Special-use regions are also available for government agencies and for China.

**Example Disaster Recovery Scenarios with AWS**

This section outlines four DR scenarios that highlight the use of AWS and compare AWS with traditional DR methods. The following figure shows a spectrum for the four scenarios, arranged by how quickly a system can be available to users after a DR event.

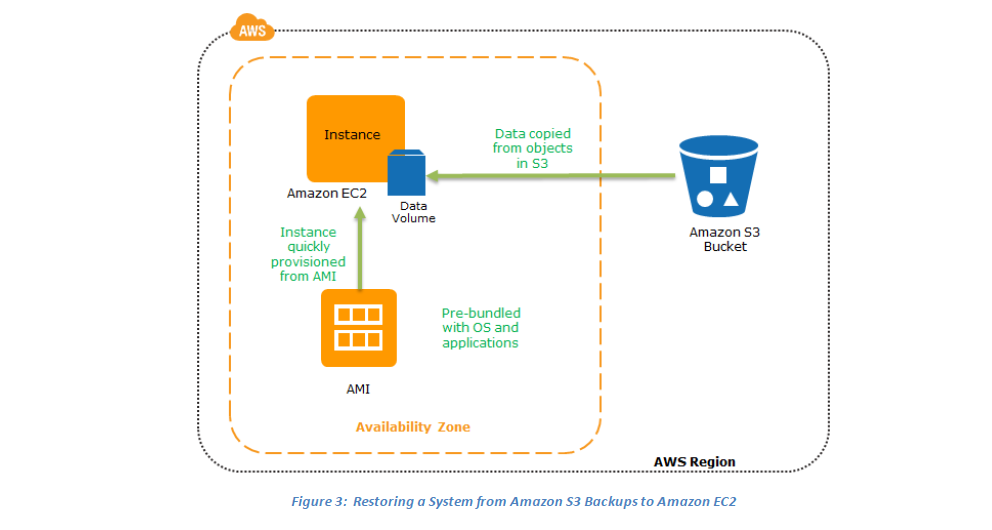


AWS enables you to cost-effectively operate each of these DR strategies. It’s important to note that these are just examples of possible approaches, and variations and combinations of these are possible. If your application is already running on AWS, then multiple regions can be employed and the same DR strategies will still apply.

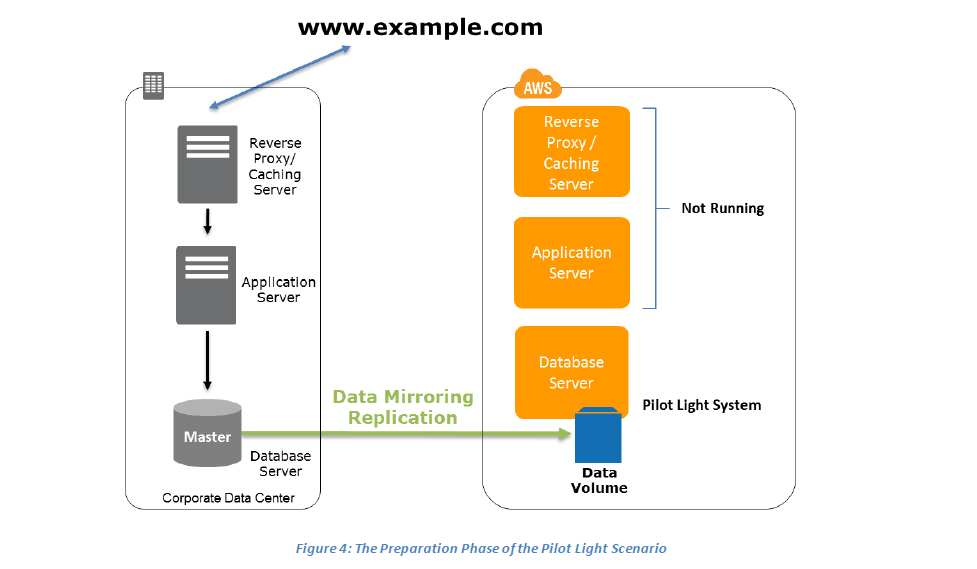


Of course, the backup of your data is only half of the story. If disaster strikes, you’ll need to recover your data quickly and reliably. You should ensure that your systems are configured to retain and secure your data, and you should test your data recovery processes.

The following diagram shows how you can quickly restore a system from Amazon S3 backups to Amazon EC2.



The following figure shows the preparation phase, in which you need to have your regularly changing data replicated to the pilot light, the small core around which the full environment will be started in the recovery phase. Your less frequently updated data, such as operating systems and applications, can be periodically updated and stored as AMIs.



Key steps for preparation:

1. Set up Amazon EC2 instances to replicate or mirror data.

2. Ensure that you have all supporting custom software packages available in AWS.

3. Create and maintain AMIs of key servers where fast recovery is required.

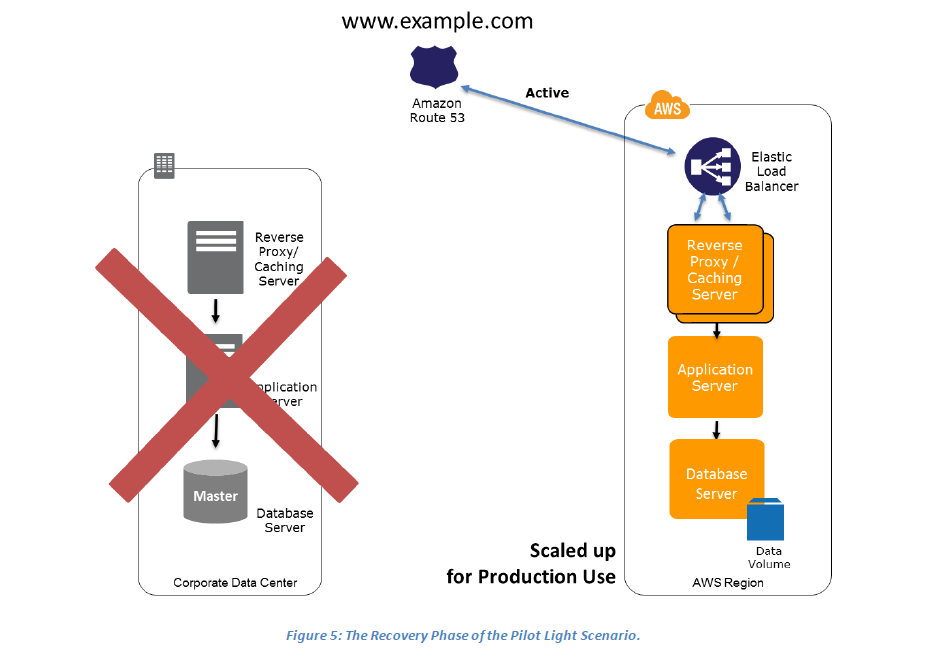
4. Regularly run these servers, test them, and apply any software updates and configuration changes.

5. Consider automating the provisioning of AWS resources.

To recover the remainder of the environment around the pilot light, you can start your systems from the AMIs within minutes on the appropriate instance types. For your dynamic data servers, you can resize them to handle production volumes as needed or add capacity accordingly. Horizontal scaling often is the most cost-effective and scalable approach to add capacity to a system. For example, you can add more web servers at peak times. However, you can also choose larger Amazon EC2 instance types, and thus scale vertically for applications such as relational databases. From a networking perspective, any required DNS updates can be done in parallel.

After recovery, you should ensure that redundancy is restored as quickly as possible. A failure of your DR environment shortly after your production environment fails is unlikely, but you should be aware of this risk. Continue to take regular backups of your system, and consider additional redundancy at the data layer.

The following figure shows the recovery phase of the pilot light scenario.



Key steps for recovery:

1. Start your application Amazon EC2 instances from your custom AMIs.

2. Resize existing database/data store instances to process the increased traffic.

3. Add additional database/data store instances to give the DR site resilience in the data tier; if you are using Amazon RDS, turn on Multi-AZ to improve resilience.

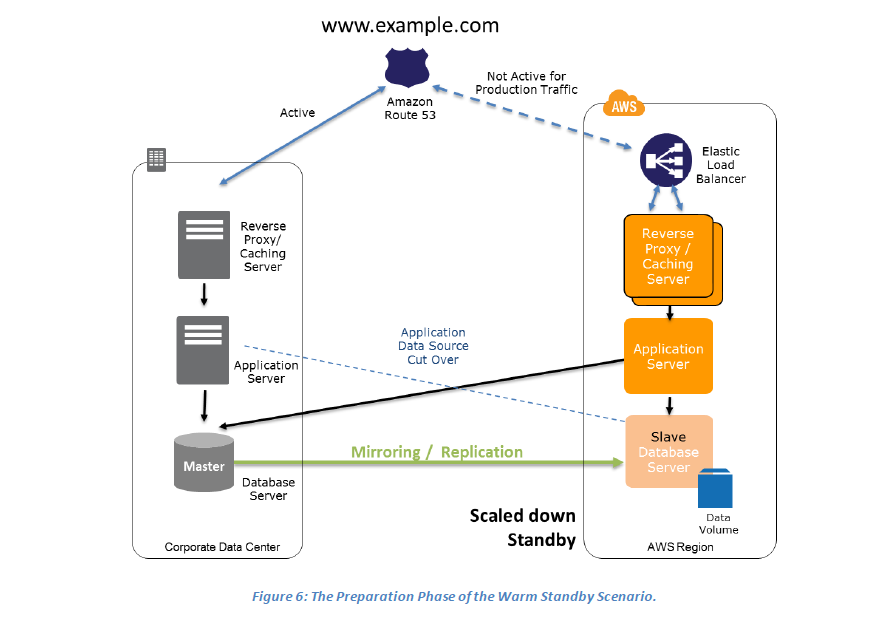
4. Change DNS to point at the Amazon EC2 servers.

5. Install and configure any non-AMI based systems, ideally in an automated way.

In a disaster, the system is scaled up quickly to handle the production load. In AWS, this can be done by adding more instances to the load balancer and by resizing the small capacity servers to run on larger Amazon EC2 instance types. As stated in the preceding section, horizontal scaling is preferred over vertical scaling.

**Preparation phase**

The following figure shows the preparation phase for a warm standby solution, in which an on-site solution and an AWS solution run side-by-side.



Key steps for preparation:

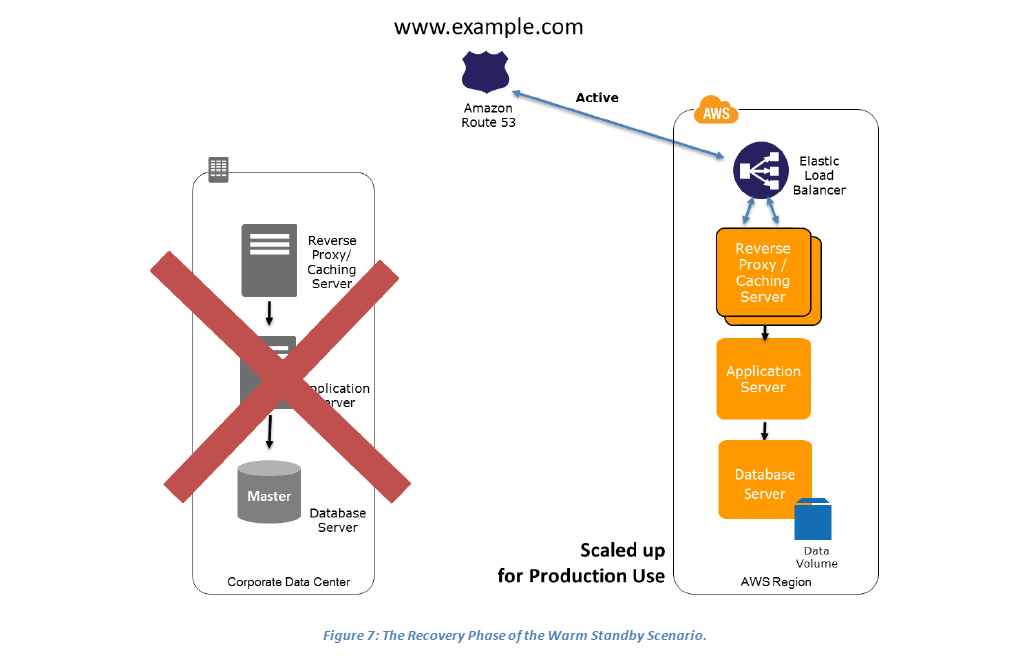
1. Set up Amazon EC2 instances to replicate or mirror data.

2. Create and maintain AMIs.

3. Run your application using a minimal footprint of Amazon EC2 instances or AWS infrastructure.

4. Patch and update software and configuration files in line with your live environment.

In the case of failure of the production system, the standby environment will be scaled up for production load, and DNS records will be changed to route all traffic to AWS.



Key steps for recovery:

1. Increase the size of the Amazon EC2 fleets in service with the load balancer (horizontal scaling).

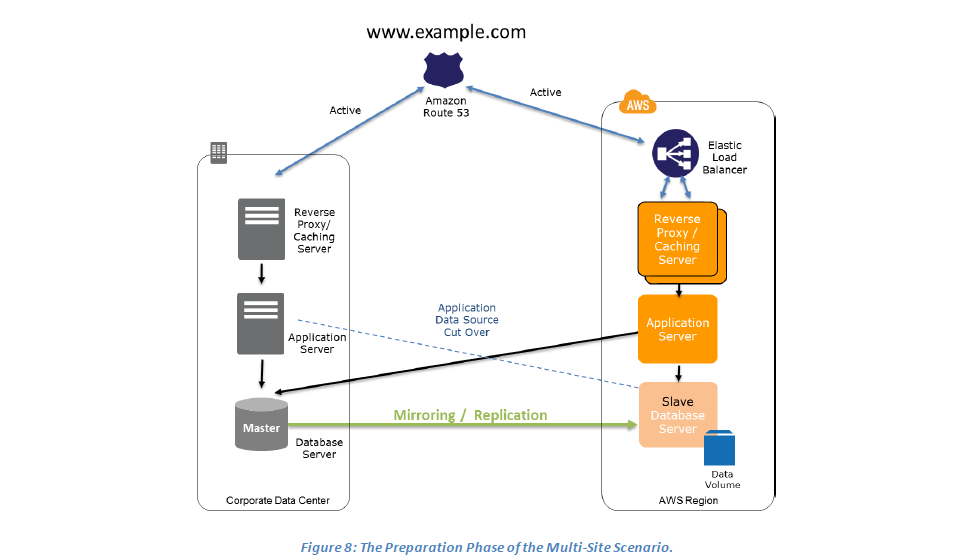
2. Start applications on larger Amazon EC2 instance types as needed (vertical scaling).

3. Either manually change the DNS records, or use Amazon Route 53 automated health checks so that all traffic is routed to the AWS environment.

4. Consider using Auto Scaling to right-size the fleet or accommodate the increased load.

5. Add resilience or scale up your database.

The following figure shows how you can use the weighted routing policy of the Amazon Route 53 DNS to route a portion of your traffic to the AWS site. The application on AWS might access data sources in the on-site production system. Data is replicated or mirrored to the AWS infrastructure.

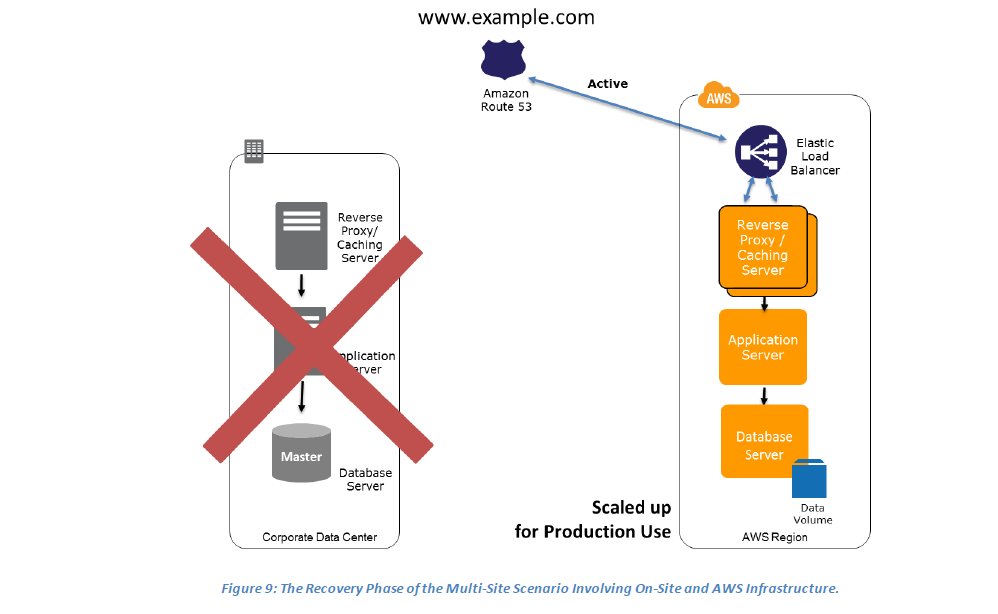


Key steps for preparation:

1. Set up your AWS environment to duplicate your production environment.

2. Set up DNS weighting, or similar traffic routing technology, to distribute incoming requests to both sites. Configure automated failover to re-route traffic away from the affected site.

The following figure shows the change in traffic routing in the event of an on-site disaster. Traffic is cut over to the AWS infrastructure by updating DNS, and all traffic and supporting data queries are supported by the AWS infrastructure.



Key steps for recovery:

1. Either manually or by using DNS failover, change the DNS weighting so that all requests are sent to the AWS site.

2. Have application logic for failover to use the local AWS database servers for all queries.

3. Consider using Auto Scaling to automatically right-size the AWS fleet.

**Replication of Data**

When you replicate data to a remote location, you should consider these factors:

 **Distance between the sites** — Larger distances typically are subject to more latency or jitter.

 **Available bandwidth** — The breadth and variability of the interconnections.

 **Data rate required by your application** — The data rate should be lower than the available bandwidth.

 **Replication technology** — The replication technology should be parallel (so that it can use the network effectively).

There are two main approaches for replicating data: synchronous and asynchronous.

**Synchronous replication**

Data is atomically updated in multiple locations. This puts a dependency on network performance and availability. In AWS, Availability Zones within a region are well connected, but physically separated. For example, when deployed in Multi-AZ mode, Amazon RDS uses synchronous replication to duplicate data in a second Availability Zone. This ensures that data is not lost if the primary Availability Zone becomes unavailable.

**Asynchronous replication**

Data is not atomically updated in multiple locations. It is transferred as network performance and availability allows, and the application continues to write data that might not be fully replicated yet.

Many database systems support asynchronous data replication. The database replica can be located remotely, and the replica does not have to be completely synchronized with the primary database server. This is acceptable in many scenarios, for example, as a backup source or reporting/read-only use cases. In addition to database systems, you can also extend it to network file systems and data volumes.

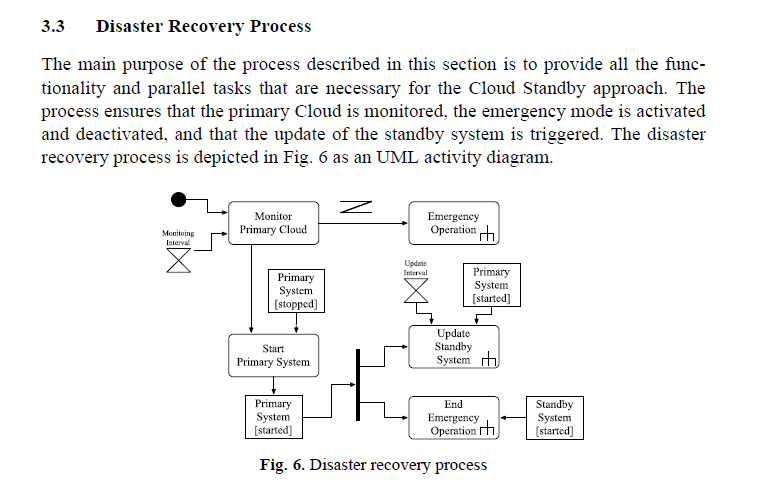
We recommend that you understand the replication technology used in your software solution. A detailed analysis of replication technology is beyond the scope of this paper.

AWS regions are completely independent of each other, but there are no differences in the way you access them and use them. This enables you to create DR processes that span continental distances, without the challenges or costs that this would normally incur. You can back up data and systems to two or more AWS regions, allowing service restoration even in the face of extremely large-scale disasters. You can use AWS regions to serve your users around the globe with relatively low complexity to your operational processes.

Differences between DRaaS and Traditional DR:

|  |  |
| --- | --- |
| Traditional Disaster Recovery | Disaster recovery as a service |
| A secondary physical DR site means investment  in additional data centre space, connectivity and  servers. It also leads to additional operational  costs-power and cooling, site maintenance and  manpower requirements | A cloud based disaster recovery service provides virtual machine snapshots of physical or  virtual servers at the primary data centre. The organization pays for storing the snapshots,  application data in a suspended state, and replication of data from primary to secondary site  for data synchronization. It pays for the infrastructure as a service feature only in case of a  disaster, wherein virtual machines need to be brought online as a substitute for the primary  site. |
| A physical dr site operates only during the  actual disaster. the time taken to make a dr site  live be more than a cloud dr resulting in huge  data loss | With cloud disaster recovery services the DR site can be brought online within minutes. A  cloud DR site that boosts up within a few seconds translates to data loss of just that timeframe |
| In case connectivity is unavailable then manual  connection is needed to start the sites operations | A cloud based disaster recovery is triggered from anywhere using internet |

**Disaster Recovery Process**

****

**1**

**Proposed Solution:**

To develop more efficient and more reliable Disaster Recovery Process (DRP) and Business Resumption Service (BRS). In this work, we are planning to use the cloud technology for the disaster recovery service which is well suited as it uses pay-per-use concept and dynamic provisioning of resources. A scientific methodology is adopted to prove this research work. Literature review and background study becomes the base of this research work. To make a strong base of this research work, many different published International Journal papers, conference paper, books, websites, communities and blogs are consulted. The literature review provides a comprehensive picture to disaster recovery related issues and their solutions along with reasoning. After the detailed comparative analysis of existing solutions, a new hybrid solution is presented based upon some standard parameters. The presented approach provides better features in the form of recovery time objective, recovery point objective, cost and security and availability.

Furthermore as our focus on disaster recovery structure and mechanism for cloud computing networks are the key factors that determine the disaster recovery ability and efficiency of networks. Through studies on technologies, including intelligent monitoring, load scheduling, hybrid gateways, clustering and data mirroring, we construct a multi-level disaster recovery network framework. The structure also increases the disaster recovery ability and the security level of cloud computing networks.

Approaches & Existing Models / Proposed Solutions.

|  |  |
| --- | --- |
| **Intelligent disaster recovery framework and realization mechanism** | A Model-Driven Deployment Method for Disaster Recovery in the Cloud |
| Enriched Multi Objective Optimization Model |  |
|  | Priority with Adoptive Data Migration in Case of  Disaster using Cloud Computing use style |
| Enriched multi objective optimization model based cloud  disaster recovery | Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review |
| Disaster Recovery – a project planning case study in Portugal |  |
| Disaster Recovery Approaches | **Experiences with Building Disaster Recovery for Enterprise-Class Clouds** |
| Load Balancing with Disaster Recovery using Multi Cloud |  |
|  |  |

**CASE STUDY**

Pakistan Petroleum Protects IT Systems from Disaster by Using Microsoft Private Cloud

Pakistan Petroleum Limited (PPL) needed to ensure greater continuity of IT systems that the business depends on to manage well production and provide communication among geographically dispersed employees and company partners. PPL used the Windows Server 2012 Datacenter operating system and Microsoft System Center 2012 with Service Pack 1 to build a private cloud environment that provides rapid disaster recovery and IT service delivery. Starting business systems in a disaster recovery location now takes just nine minutes versus the nine hours previously required. Configuring new servers takes 10 to 15 minutes rather than three to seven days. Because it can now automate many IT processes, the IT staff has reduced its maintenance and an operation work by 70 percent and has more time to focus on new projects that make the business more competitive.

Situation A petroleum engineer sits in the air-conditioned office of the Sui gas field, hunched over his computer. He glances at his watch; he has 20 minutes left to complete the daily production report and submit it to his boss in Karachi, 1,400 kilometers away. He types the final numbers into the company’s production planning system and is about to shut down for the day when his screen freezes. The machine has failed. Again. Who knows when it will be restored? The deadline missed, he stares out the window at the heat rising off the 102-degree desert sand stretching in every direction. Keep Servers Safe “Many of our employees are working in remote locations, and their only connection to the rest of the business is their computer,” says Mirza Anwar Hussain, General Manager of IT, Pakistan Petroleum Limited. “When our computer systems fail, our employees are frustrated and unproductive.” With our Microsoft private cloud, we can reinstate business systems in nine minutes versus the nine hours previously required. This is critical, considering the part of the world in which we operate.

So to overcome from plain data backup and recovery problem, it requires more safe and effective system such as

* RAID (Redundant Array Independent Disk)
* HSDRT [1]
* PCS [2]
* ERGOT [3]
* Linux Box [5]
* Cold and Hot back-up technique [6]
* SBBR [7]
* REN [8] etc.

Disaster Recovery Simulator Tools

1. Progressive recovery is tested using custom-developed models in the *OPNET ModelerTM* simulation tool
2. Matlab
3. NS2

Sandboxing and orchestration come into play when testing disaster recovery in the cloud.

“Rule No. 1 of a DR solution is you have to be able to test it. If you want to test a backup solution, you take a couple of files,” Buffing­ton said. “If you want to test a DR solution, you have to power up the VMs. The problem is, the live VMs are still doing their thing. If the live VMs are working, and I power up the test VMs, you could have an outage. So you need sandboxing, the ability to isolate what is in your DR environment so you can bring it up without impacting the production environ­ment. Sandboxing allows you to power up in a vacuum without impacting the validity of any­thing else.

“Orchestration has two roles. You orchestrate dependencies between VMs. The file server might seem like a simple thing, but if you don’t have a logon [on] the server, you need to bring up the Active Directory and another server. Sometimes there are up to three tiers of VMs. You have to bring them up in the right order or nothing works.”

For example, you may need to bring up the most important VMs in two hours. Maybe you can wait 24 hours to bring up the next round of VMs, 36 hours for the third round and so on.

“There has to be intelligence and intent,” Buffington said. “The worst thing to have is whoever screams the loudest gets their server first. You need a policy to define that.”

—Ed Hannan

Existing Tools for recovery of data when a system encounter an attack in cloud environment [11]:

1. VMWares: For virtualization and use of Hypervisor for data control
2. EnCase: Acquisition and analysis (while maintaining state), Data recovery.
3. LinkAlyzer: analyzing link files.
4. PmExplorer: GSM Key decoder.

Read

A. AppSim: is an Internet level application simulator which is used for Software-as-a Service. This tool supports Multitenant applications and can be efficiently used for calculating multitenant non functional requirements. It has two mechanisms that are Load Generator and Virtual Distributors13.

B. Google App Engine: Google App Engine is a Java and Python based platform that affords web application, resource storage and application hosting, data storage, and high-speed networking by Google’s huge infrastructure. It is easy to scale, build and maintain resources. It provides a high level access to hardware such that it does not support access to kernel level services.

Hence, need for the existence of virtual machine is not required14.

C. Nimbus: This Nimbus tool is built on public cloud and it provides the IaaS platform for its clients. Nimbus supports Xen and recently added KVM hypervisors. Platforms for this tool are Java and Python. The structure of Nimbus contain Light weight components15.

D. Open Nebula: Open Nebula is an open-source toolkit to effortlessly fabricate private, public and hybrid clouds. Open Nebula has been intended to be incorporated with any networking and storage solution and also fits into any obtainable data center. This tool converts data center into agile and flexible virtual infrastructure. C, C++, Ruby, Java, Shell script are the languages that are required to support this tool. The hypervisors which supports this are Xen, VMWare, and KVM. The advantage of

this tool is that it supports VM migration16.

E. Green Cloud: The motivation of Green Cloud is to support the researcher to develop, observe, cooperate and determine cloud performance. The Green Cloud is implemented using C++ (85 %) and (15%) of Tool Command Language scripts (TCL)

S). The hypervisors which supports this tool are Xen, KVM, and VLAN17.

F. Amazon web services: This tool is based on heuristic algorithm to arrange applications such as computation cost and data transmission cost. The implementation can be in C++ and hypervisor support is Xen. The tool is flexible, cost-effective, scalable, elastic and secure18.

G. CloudSim: This is a toolkit developed by the Grids laboratory of university of Melbourne. This is used in cloud computing environments to enable modeling and simulations, it also supports creation of virtual machines of a data centers and migration of virtual machines for reliability and automatic scaling. It is an independent platform for modeling datacenters, service brokers, scheduling and allocation policies. Cloud sim supports modeling and simulation of virtualized cloud based data center

for virtual machines, memory storage and bandwidth19.

H. Cloud analyst: It is developed on the Java platform, it has the features of CloudSim and SimJava.This simulation tool contains very high configurable and flexible features. Cloud Analyst is competent produces graphical output results of simulation in the form charts and tables. The advantage of this tool is that it supports Virtualization (Xen)19.

I. Eucalyptus: Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems) is one of the major open source cloud computing tool. It supports private cloud and hybrid cloud and works under IaaS Cloud Services. The languages support for Eucalyptus are Java/ C++, Python, Perl, Shell scripts and also hypervisors are VMware, Xen, KVM20.International Journal of Interdisciplinary and Multidisciplinary Studies (IJIMS), 2014, Vol 1, No.4, 82- 86. 85

J. Virtual Cloud: In the cloud computing components Virtual Cloud has sub-blocks as a replacement for isolated layers. Some of the resource utilized by virtual clouds is CPU, RAM, Disk I/O and it supports virtual migration. It is implemented in Xml format, Xen. KVM hypervisors supports this tool19.

K. Open stack: This is suitable for Public and Hybrid cloud. The tool is progressing with improvements to support wide spectrum of requests from the growing user community. It is a single code-base simulator and supports migration. Additionally, this tool supports Data Protection and Data Recovery for VM data. Intel, Cisco, Dell, AMD, IBM, Canonical, HP, SUSE Linux, Red Hat uses Open stack project21.

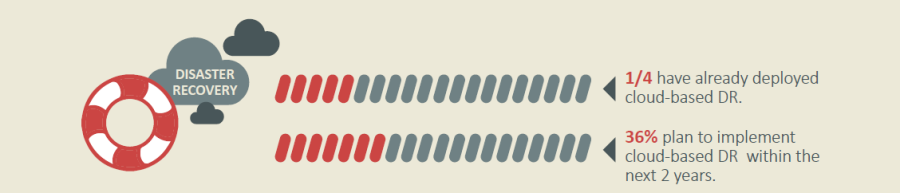
Using this all data imposed on Punjab Emergency Service Rescue 1122

After All Analysis ,Case Study & Implementation in Rescue 1122 Department.

Arbisoft-SME Case Study from Pakistan

Forward-looking software house in Lahore established in 2007

* Develop Smartphone apps, interactive enterprise apps, and search analysis
* 100+staff with Multi million dollar revenue
* One of the Fastest growing software house in Pakistan
* Entire development activity on Amazon cloud (PaaS)
* All IT enterprise services (email, collaboration,calendars) are on GoogleApps cloud (SaaS)
* Using other cloud services (SaaS) such as drop box



These results came from an IDG survey which polled 400 global IT executives in the early 2015.

**Thesis Outline:**

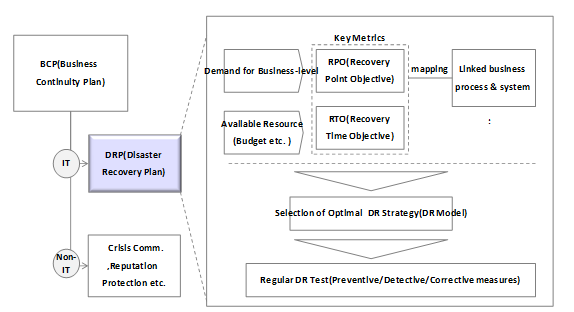
**Chapter 1**

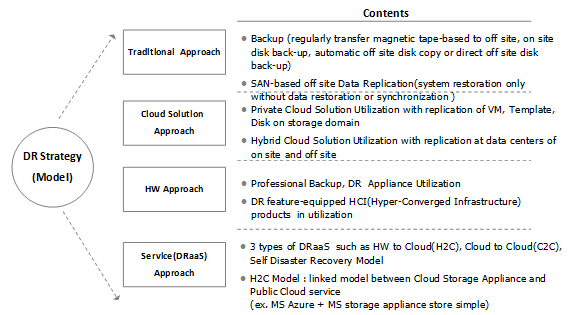
Introduction (Chapter 1) gives a complete overview of the thesis. This chapter is organized such as thesis introduction, problem statement, research objective, proposed solution and methodology to authenticate the problem statement.

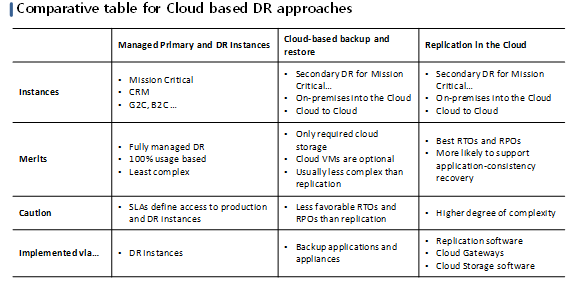
**Chapter 2**

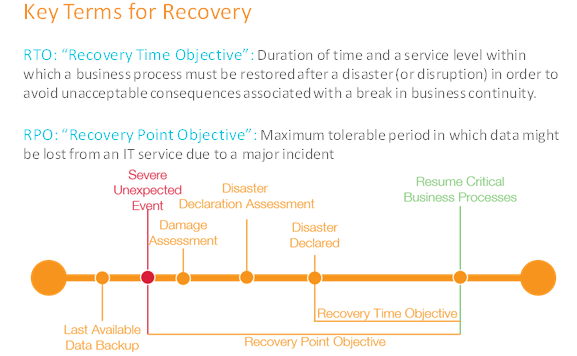
Background and Literature Review (Chapter 2) gives a brief overview of the research area. This chapter is organized such as background of Cloud computing, Cloud computing service models, types of Cloud computing architecture, types of disasters in Pakistan and disaster recovery plans.

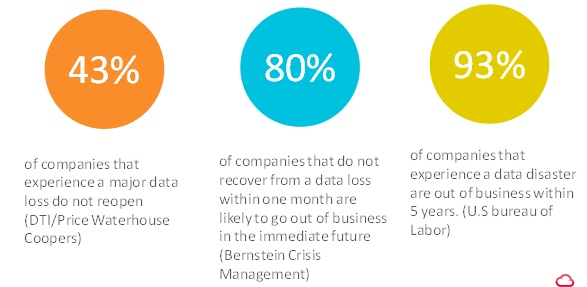
Disaster Recovery Planning

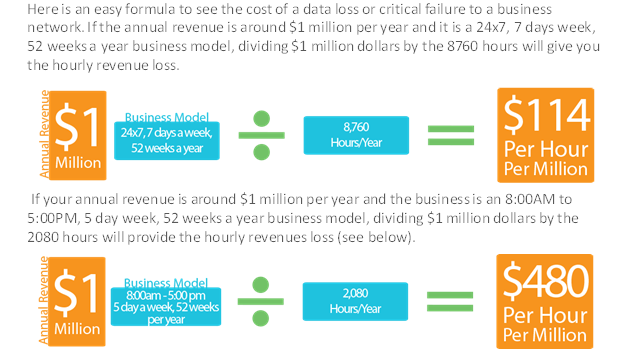












**Chapter 3**

Problem Statement and Proposed Approach (Chapter 3) presents the research problem statement under consideration and the proposed approach to provide a solution of problem statement.

**Chapter 4**

Research Methodology (Chapter 4) discusses the scope, objectives and the approach used to solve problem under study. A scientific approach is used to propose a solution of research problem.

Cloud-based disaster recovery tends to be automated and non-intrusive to ongoing operations. Some providers will even run virtual tests in separate network environments. Planning, implementing, and testing disaster recovery is complicated and there are a number of pitfalls along the way that even time-tested IT staffers can miss when focused on their primary jobs. If your organization pushes disaster recovery to the back burner or tries to patch it together with inadequate resources, you’re gambling with the business. You also miss out on the cost savings that come with DRaaS. You will only need to tap greater compute resources at the time of an outage or testing, and you won’t need to overinvest in infrastructure that you may never need. No one ever wants to go through a disaster. They are stressful situations that can threaten an organization. Why not lean on the experts who can put you on the road to disaster recovery nirvana?

**Chapter 5**

Implementation (Chapter 5) presents the implementation details of the proposed solution and analyzes different disaster recovery plans as an example of the problem under study.

In chapter 5 implementation, implementation examples, of proposed solution as well as study and analysis of different problem under this scope are discussed.

**Chapter 6**

Conclusion (Chapter 6) discusses the objective of the thesis and how well the thesis achieves its objective by providing proposed solution and the benefits obtained.

**References:**

[1] Mr. A. Srinivas, Y. Seetha Ramayya, B. Venkatesh, “A Study on Cloud Computing Disaster Recovery” IJIRCCE Vol. 1, Issue 6, August 2013

[2] Omar H. Alhazmi, Yashwant K. Malaiya, “Assessing Disaster Recovery Alternatives: On-site, Colocation or Cloud” ISSRE Workshops, page 19-20. IEEE, 2012

[3] Suma. V , Chintureena Thingom “Effective Disaster Management to Enhance the Cloud Performance” Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 *Vol. 2*, Advances in Intelligent Systems and Computing 328, page153 -162

[4] Chintureena Thingom “Cloud Disaster Management with Scheduling Strategy”, International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 3, Issue 5, May 2014page 305-310

[5] Muppalla Prudhvi, “Disaster Recovery on Double Duty Using Cloud”, International Journal of Computer Science & Communication Networks, Vol 3(2)

[6] Shalini Wunnava, Dr. Selwyn Ellis, “Disaster Recovery Planning: A Pmt-Based Conceptual Model”, Proceedings of the Southern Association for Information Systems Conference, Richmond, VA, USA March 13th-15th, 2008

[7] Omar H. Alhazmi, “Evaluating Disaster Recovery Plans Using the Cloud” IEEE 2013

[8] Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, “Performance Evaluation of a Disaster Recovery System and Practical Network Applications in Cloud Computing Environments” International Journal on Advances in Networks and Servics,2011, page 130-137.