Public Cloud and Disaster Recovery: A Perfect Match

Imagine you're speed dating for your next disaster recovery solution. You sit down with a drink in hand and prepare for the "interesting prospects" you're about to encounter. When you signed up, the matchmakers told you the attractive public cloud would be in attendance, but first, you just have to weed through the undesirables.

Okay, take a deep breath because the first round is about to start…

Date 1: The Build-It-On-Your-Own DR

Right from the start, this one seems like high maintenance. Sure, you'll have full control over available assets while adhering to security requirements, but is the tradeoff worth it? You'll certainly have the flexibility of the cloud, but at the cost of maintaining all that equipment. After a few years, your hardware will be old and you'll either have to keep using it or spend a fortune on upgrades. Not a wise match.

Date 2: The System Integrator

Oh no. This is just getting worse…How did you let your CTO talk you into this?

This solution is going to cost not only in OpEx, but in CapEx too. Between the facility costs, cooling and heating, and hardware it just seems like a bad fit. While the system integrators could come in and plan everything for you now, down the road if your needs change, you'll either be supporting a partially unused data center or needing more servers than you have.

Then there are duplication needs in an area far enough away that if a natural disaster hits, your data center will be okay. It also must be close enough that your team can get to it in case of an emergency. On top of everything, the staff will need to be highly trained, which is just another added cost.

Date 3: DRaaS

Well, this is getting a little better, but it's not yet a perfect match. Unlike the last date, this match is more affordable since you wouldn't have to manage your own off-site DR system.

You will feel some flutters in your stomach, but that's just nerves about DRaaS' security. Your data, whether in rest or in motion, will need to be encrypted. So although it's a step up from building your own DR and system integration, you still would really need to have a trusting relationship for DRaaS to work.

Date 4: Public Cloud

Finally! It's "the one." There's so much to love about public cloud:

- *Affordable – Check!* With pay-as-you go models, you will simply use your OpEx for resources without any waste**.** No need to invest in multiple data centers or hardware that will quickly be outdated.

- *Flexible – Check!* The public cloud offers greater elasticity. No matter what demands you have, they will never max out the capacity of the cloud. The public cloud has greater economy of scale than any enterprise could ever have, which allows you to use the exact amount of resources you need for any given task.
- *Secure – Check!* The public cloud is no stranger to security threats. With hackers constantly pounding providers like AWS they have developed top-notch security practices. Plus, they retain the best security professionals in the business.
- *Ease of Deployment – Check!* You won't have a lengthy planning process here since all of the resources are at hand. Public cloud is available within minutes.

Whether you are dealing with a man-made or natural disaster, the public cloud offers unique solutions for every business. Now that the DR Dating Game is over, let's review more specifically the advantages of public cloud:

Replication of Entire Application Stack

Just backing up "data" to the cloud is not enough for a DR plan. Entire systems and applications must be included in order to successfully be back online after a disaster. Databases, load balancers, and other systems need to be fully operable upon failover. Public cloud can support all of these necessities.

Failover Prioritization

With just one click (or zero), you can be up and running after a failure. By prioritizing which applications need to come up first, you can ensure that a failover scenario goes as planned. Different applications and their data will have different Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). For example, a customer-facing portal for accessing medical records might be able to wait a couple of hours to back up, but cannot have any data loss. In contrast, an internal HR system for processing leave requests may be able to roll back any "recent" point in time, but needs to be up within 15 minutes.

It's extremely important to define these service levels when building a DR plan. When it comes to using a public cloud-based DR, there are restraints and limitations for recovery that must be contemplated. Elasticity and the ability to spin up as many instances as necessary come with a high cost. It will be more financially viable to prioritize certain applications and services in a cloud DR plan than to bring every single system back online simultaneously.

Continuous Replication

Rather than backing up at distinct and sparse intervals, Continuous Data Protection (CDP) to a cloud service allows for real time updates no matter the environmental complexity. If your RPO is two hours for business critical applications, CDP is a must.

Replication To, Across, and Between Multiple Cloud Locations and Providers

Is your CIO paranoid about downtime and data loss? By including multiple cloud providers in your DR plan, you can affirm that this will never be a possibility. This may seem like overkill for some applications, but for business critical systems like payment processing, having more than one vendor housing your data allows for peace of mind (and iron clad guarantees of SLAs). From Amazon's Elastic Cloud Compute (EC2) to VMware's vCloud Air, there are vendors at all price points. The flexibility here allows your DR administrators to choose a platform they are more comfortable with.

Even if you choose a single provider, being able to enact a DR plan from different geographical locations is still a good idea.

Non-disruptive testing for cutover / failover

In a disaster with a cloud-based DR setup, you are guaranteed that your RTO and RPO will be met. Like all systems in IT, constant testing and quality assurance are important. They should be part of your business continuity plan for DR. Is there a hurricane coming? No need to worry, you can migrate your entire DR system to a geographically separated datacenter with a few clicks and zero downtime.

Disaster Recovery Options at a Glance

	Private Cloud	**System Integrator**	**DRaaS**	**Public Cloud**
Affordability	Requires CapEx & OpEx	Very expensive - Must pay for all the set up and the consulting	Affordable but may only be simple backup and restore	Affordable pay-as-you-go model with no waste
Flexibility	Limited to available assets	Limited to available assets	Must trust that the provider can implement recovery plan in the time of the disaster	Elastic & greater economy of scale
Security	Lacks security specialist and/or requires the cost of training employees	Lacks security specialist and/or requires the cost of training employees	Need for encryption	Best in business security prompted by unrivaled experience with hacking
Deployment	Long lead time to build datacenter and plan DR	Long lead time to build datacenter and plan DR	Easily deployed after agreeing on an SLA	Ready in minutes

Tired of bad matchmaking? There’s no need to keep playing the DR Dating Game. At CloudEndure, we can connect you with the DR solution of your dreams. Learn more