Public Cloud and DRaaS

What You Should Know

Is the public cloud a suitable solution for Disaster Recovery? This whitepaper will explore the ramifications of public cloud as a DR solution including: monitoring, builds, service, running from the cloud, networking, SLAs, security and other issues you will face with any disaster recovery solution.

The public cloud and DRaaS

Disaster Recovery as a Service (DRaaS) continues to grow rapidly. While implementation can be complex, the concept is simple: backup and/or replicate your servers to a secure remote facility where they can be brought live or used to restore lost data in the event of an outage or data loss at the primary site.

VMware and Hyper-V are the primary hypervisor platforms for virtual servers currently and these tools make it possible to support moving servers among different hardware infrastructures in different geographies. Private Cloud solutions use software tools to manage backup, replication and retention. As a service provider, we're often asked what we think about using the public cloud as a remote repository for these servers.

Based on our experience in this space, here are eleven things we believe are critical to DRaaS and whether they are included in a public cloud implementation versus the services available from some private cloud providers.

1. MONITORING – There are many technical components required to implement DRaaS, including primary hardware, local software, firewalls, connectivity, and remote infrastructure. The smallest change to any of the components can affect the completeness of the recovery, from a small data loss to a total data loss.

Public cloud	No monitoring is provided.	🔴
Private cloud	Monitoring varies among service providers. Most private cloud providers offer some level of monitoring.	🟡
Fully managed	The best service providers offer full monitoring and help with managing changes that impact the quality of the solution.	🟢

2. TEST BUILDS – Bringing a server live at a remote site is certainly possible, but it's not a trivial task. A time-honored tenet of IT is that remote DR servers should be tested regularly.

Public cloud	Test builds are not provided.	🔴
Private cloud	Most private cloud providers offer a test build capability. In some cases, it's included in the basic service offering and in some cases additional fees apply for a testing environment. In either case, it's an essential component.	🟡
Fully managed	Fully managed solutions include test builds.	🟢

3. SERVICE RELATIONSHIP – In a complex implementation where a high quality result can be so important, having a warm contact matters – whether it's a technical issue or service delivery, it's always beneficial to have someone to call.

Public cloud	When you need help with the public cloud, "you may have to stand in line, if you can even find a line to stand in" – from Veeam's DRaaS for Dummies.	🔴
Private cloud	Most private cloud providers offer a free or paid support arrangements.	🟡
Fully managed	Fully managed service providers know and expect their customers to call, email or even text about questions, concerns and the general matters required to support the solution.	🟢

4. SERVER SPINUP – A proper DR environment needs more than just storage. Proper DR needs CPU and memory resources to allow booting and running that or those servers during an outage.

Public cloud	Available but requires extra cost and effort to provision.	🔴
Private cloud	Available but generally requires extra cost and effort to provision.	🟡
Fully managed	Fully managed service providers understand and deliver on the customer's need to actually spin up and run from the cloud environment.	🟢

5. NETWORKING – Servers that are replicated to cloud infrastructure will not network with each other unless the network configuration for each server is properly adjusted for the remote environment.

Public cloud	Available in most cases but requires additional effort to provision.	🔴
Private cloud	Available but requires extra effort to provision.	🟡
Fully managed	Fully managed service providers may offer to automatically perform the network configuration to support running form the cloud environment.	🟢

6. RESTORING DATA – What happens when you need to recover data?

Public cloud	Requires significant additional costs in some cases.	🔴
Private cloud	Usually included.	🟡
Fully managed	Always included at no additional cost.	🟢

7. SERVICE LEVEL AGREEMENT (SLA) – What guarantees does the provider offer in terms of how quickly you can recover (Restore Time Objective or "RTO") and how recent is the data you will get back (Restore Point Objective or "RPO")?

Public cloud	The only SLA you get from public cloud is related to their infrastructure working – not whether your servers stored there are available and working. See this article in Information Week explaining the weaknesses of public cloud SLAs http://ubm.io/1XRkSrF	🔴
Private cloud	SLA's vary widely among private cloud providers.	🟡
Fully managed	The SLA should pertain to your ability to recover and it should be measured in hours or minutes of RPO and RTO..	🟢

8. PUBLIC IPs – You will need public IP addresses for mail and web servers in your DR environment.

Public cloud	Requires additional costs in most cases.	🔴
Private cloud	Requires additional costs in most cases.	🔴
Fully managed	Generally included at no additional cost.	🟢

9. SECURITY – A new category of products are designed to provide additional security for users of public cloud. In their words, "keeping the bad guys out of clouds." Why would there even be a market for these if public cloud was secure enough in the first place?

Public cloud	We're only just learning publicly what some cloud providers will disclose. Google searches and indexes offer little data, and Microsoft does not disclose what data is provided to the government in regards to security of the public cloud.	🔴
Private cloud	Provides a higher level of security and provides visibility and disclosure about security.	🟡
Fully managed	Similar to private cloud and can also offer full end-to-end encryption.	🟢

10. CONTROL OVER STORAGE LOCATION OF DATA – Tax laws, security regulations, national protectionism, and other factors can all place limits on where data can move and be stored. For example, some provinces in Canada prohibit healthcare data from being stored in the United States.

Public cloud	Little to no control is provided.	🔴
Private cloud	Provide a higher level of control.	🟡
Fully managed	You know exactly where your all of your data is located.	🟢

11. ULTIMATE RESPONSIBILITY – What is the real level of responsibility taken by each type of provider?

Public cloud	Public cloud providers stand up the platform and that's where their responsibility ends. Everything else is up to you. That includes setting it up, making it work, keeping it working, and, most importantly performing restores and recoveries during outages and disasters. And keep in mind, during a disaster you may have other concerns.	🔴
Private cloud	Assumes a higher level of responsibility.	🟡
Fully managed	Fully managed solution providers manage, monitor, test and assist with restores and recoveries. They don't see how it makes sense to offer anything less.	🟢

So why use public cloud for Disaster Recovery? Initially, it may look like a low cost option, but after properly configuration with the additional CPU and RAM needed for recoveries, plus all the extras thrown in, the actual cost adds up. Even then, it's still a "Do It Yourself" solution.

While it might appear that it is a bit costlier, Private Cloud solutions offer a higher level of service as outlined in the many areas detailed above.

Fully managed solutions from providers like Global Data Vault are price competitive with a properly configured public cloud solution, all while providing a much higher level of service.

Request Information

To learn more about Global Data Vault's data protection solutions, contact GDV at:

Department	Email	Phone
Sales	sales@globaldatavault.com	214-363-1900 x 1
Support	support@globaldatavault.com	214-363-1900 x 2
Customer Service	billing@globaldatavault.com	214-363-1900 x 3