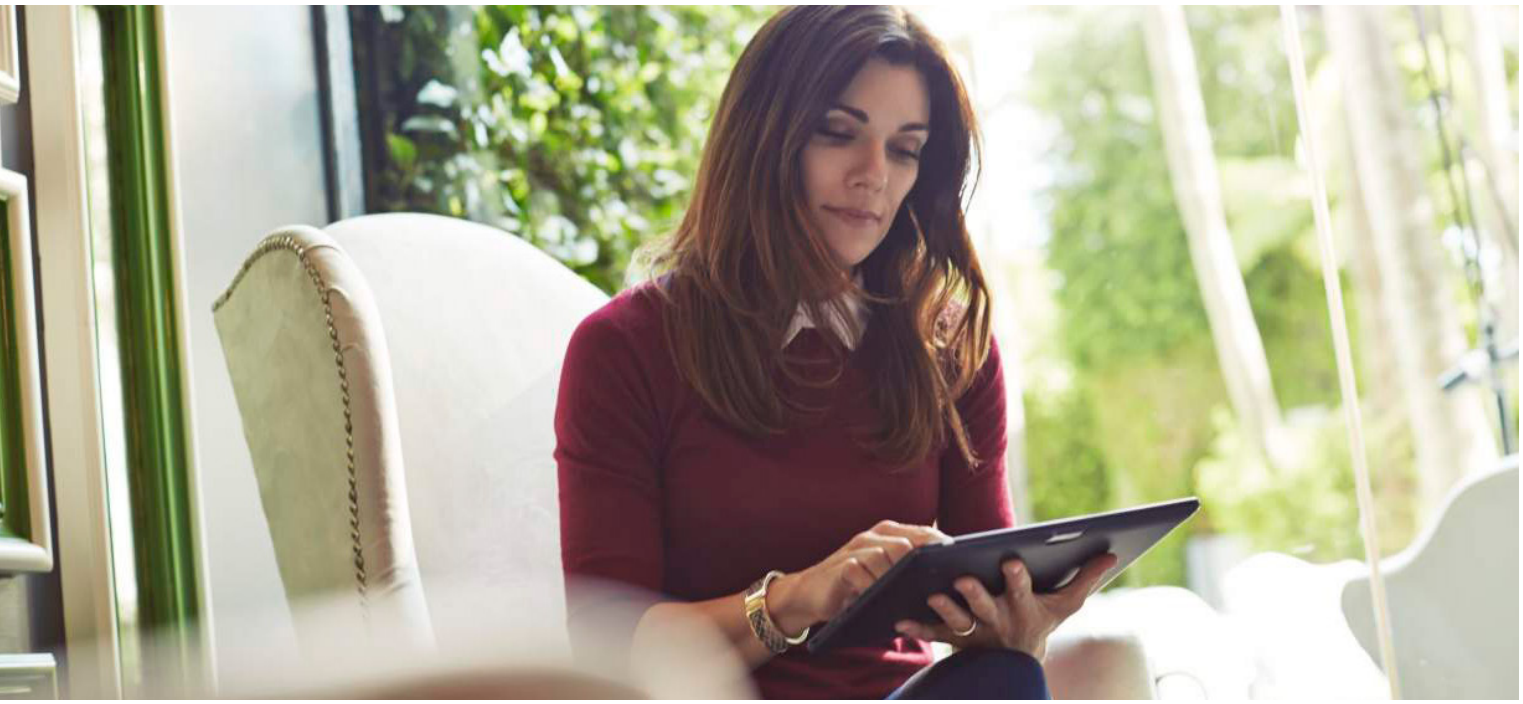
Software

Choosing the Right Public Cloud for Better Data Protection



Introduction

Let's face it, cloud is everywhere and it's transforming IT. With five minutes and a credit card, nearly anyone can spin up public cloud capacity for testing, development, quality control, and production. Beyond this ease of access, other benefits emerge: reliability, efficiency, and cost transparency, to name a few. That's why more and more organizations are turning to public cloud for any new requirements. New workloads go on new cloud capacity. That makes sense.

But what happens to existing IT – the already functioning workloads and processes? Well, existing workloads *could* migrate to public cloud but often that's not a priority – if the workloads are stable, why move them? If the hardware is still being depreciated, why decommission it? So workload migration isn't often a priority.

But there's another opportunity to use public cloud to make existing IT better. It's leverging public cloud, or infrastructure-as-a-service (IaaS), for backup and recovery enabled data protection.

Using public cloud for data protection

Imagine a workload that's running locally but that generates huge amounts of data. That data is important. It needs to be protected. Now, traditionally, you'd protect that data with local disk or tape, and that's okay. But what's stopping you from leveraging public cloud to protect that data? Seems like an easy fix, doesn't it?

For that matter, you have dozens or hundreds of workloads. Where will you put the data? Does it make sense to use IaaS to protect those workloads?

And perhaps you have a combination of cloud-based and non-cloud based workloads. Could you use public cloud to protect everything?

And you need to archive? Can the cloud do that too?

Yes, you can use public cloud to protect anything you want – but only if you choose the right approach, with the right tool, in the right cloud.

Traditionally, organizations used object storage to keep archives. This isn't a bad approach, but it can be more cost effective to choose a public cloud that's optimized for archive.

Making those choices isn't necessarily easy. Let's explore four scenarios and talk, in some detail, about ways to use IaaS and innovative data protection software as an innovative attack on the complexity and cost of protecting data, no matter where the data lives.

Scenario 1: Archive

What is archive? Simply put, it's the process of moving infrequently accessed data to inexpensive storage. Usually this data is kept because of regulations or simply because it's important, but infrequently accessed.

Traditionally, organizations used local Tier 3 or object storage to keep archives. This isn't a bad approach, but often it can be more cost effective to choose a public cloud that's optimized for archive. The right approach combines an archive optimized public cloud along with archive software, delivering these characteristics:

- Since archived data isn't mission-critical or even important for day-to-day functioning, the right public cloud offers redundancy, but usually not 99.999% availability
- The ability to manage huge amounts of data – hundreds of terabytes up to dozens of petabytes.
- Performance isn't a key measure – massive bandwidth isn't needed.
- A way to minimize utilized capacity — for example, strong dedupe and compression.
- Business stability – you can't pick a cloud provider that might go out of business next year.
- The ability, in software, to mount the cloud archive directly, enabling file and/or folder level recovery from local devices.

If organizations choose a cloud with these characteristics, they'll be in a strong position to strike the right balance of recovery time, cost, and risk for their archives.

Scenario 2: Backup and restore

Here, organizations use public cloud as backup servers and backup targets. This is an especially good approach for workloads already in public cloud, but public cloud is also often used as a good way to augment to extend existing backup infrastructure. It can be faster and as cost-effective as tape.

Organizations who want to use IaaS for backup and restore need to understand the parameters, which include:

- A good level of availability. Perhaps 99.999% isn't needed, but redundancy is.
- The ability to cope with large amounts of data.
- The need for regular dataset transfers. Many organizations use snapshots to make backups more granular and reduce the need for full restores.
- A reasonable amount of bandwidth for good RTO.
- Granular restore to reduce complexity and RTO – everything from file level to full system recovery.
- Cost that's comparable to tape.

Scenario 3: Workload protection

In this scenario, we're exploring the possibility of utilizing data protection software to create a workload specific DR site in a public cloud. Perhaps it's for an order processing app or email services.

What kind of infrastructure-as-a-service and data protection software features are needed?

- This is a higher risk scenario since, if the cloud isn't available, failover isn't possible, so 99.999% is required.
- This involves smaller amounts of data so cost/GB isn't so much of a concern.
- You'll need data protection software that provides frequent snapshots/replication as well as tight integration with the application and the hypervisor.

- The software needs to handle physical to virtual migration, virtual to virtual migration, and even virtual to physical migration that encompasses the entire working environment (hypervisor, operating system, application).
- Cloud to cloud replication – in case your cloud-based workload needs to be protected in another cloud, which is good operating procedure for safety's sake.
- The public cloud will have to offer good compute performance, good storage performance, and good bandwidth for this to work.

Scenario 4: Environment protection

In this scenario, organizations use public cloud to create a disaster recovery site for their entire environment. This is a challenging undertaking because it puts the highest demands on a public cloud and the data protection software.

It's characterized by:

- The highest level of risk so a need for the highest level of availability.
- Very large amounts of data capacity because odds are good the DR site will also be backed up into the cloud.
- The need for constant snapshots/ replication across many workloads.
- Built-in deduplication and compression to reduce bandwidth and storage costs.
- The ability to keep DR site virtual machines in sync, and in standby, so failover takes minutes instead of hours.
- Cloud to cloud replication and protection.
- Data protection software that has wide-ranging application and hypervisor awareness.
- Quick restores, all the way up to bare metal recovery.
- Scale that matches the production environment, including compute, storage, and networking.

Making the right choice

Looking over the landscape, it's not hard to find cloud providers who offer general purpose capabilities like compute and storage. Digging deeper, there are opportunities to find cloud providers who optimize their offerings for specific requirements. For example, there are public clouds that are ideal for archive. They describe the use cases to include media asset archiving, healthcare information archiving, compliance archiving, scientific data storage, digital preservation, and local Tier 3 disk replacement. To put price into context, one of these starts at $0.007 per gigabyte per month.[1]

Beyond choosing a public cloud, it's also essential to choose a data protection software that's a good fit for leveraging public cloud. At a minimum, the software needs to offer:

- A good range of cloud connectors to fit many clouds, including Azure, Openstack, and Amazon.
- Strong application and hypervisor awareness.
- Built-in deduplication and compression to speed up snapshots, reduce data transfer times, and minimize the cost of cloud storage.
- Global encryption for data-in-motion and data at rest.

Many familiar data protection packages weren't designed to take full advantage of infrastructure-as-a-service capabilities. By carefully evaluating public cloud capabilities and data protection software capabilities, organizations can make the right choices for any scenario.

By carefully evaluating public cloud capabilities and data protection software capabilities, organizations can make the right choices for any scenario.

[1] https://aws.amazon.com/glacier/.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
4 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com

Refer to our Web site for regional and international office information.