HYCU

Multi-cloud backup as a service:

9 Ways to Get BaaS Right

Have data and applications distributed across multiple clouds? A multi-cloud strategy requires you to rethink your approach to data protection.

Read on to explore nine key success factors to optimize your multi-cloud Backup as a Service.

Choosing the Right Class of Solution

1

When deploying backup and recovery to the cloud, you have a few choices.

You can write your own scripts. But that can be risky.

You could deploy an image of your on-premises backup solution to the public cloud. But that's still infrastructure you run yourself, with all the associated maintenance hassles and risk.

Or, you could use a cloud-native backup as a service (BaaS).

It's easy to turn on and off as your needs change. And it offers the flexibility to adapt to the different capabilities—and shortcomings—of each cloud you're using.

BaaS offers simplicity and agility.
Isn't that why you moved to the cloud in the first place?

Upkeep and Maintenance for the Cloud Operations Model

2

How will you adapt your data protection infrastructure as your needs evolve?

You could have your in-house team continually updating your backup infrastructure. But that's an investment in time and talent that doesn't generate additional value.

Or, you could use backup as a service (BaaS). This offloads the updating task to someone else, ensuring you always have the latest updates, with no effort on your part.

When it comes to resizing, BaaS will size to fit changing needs seamlessly. You'll have the data protection capacity you need on every cloud, without complicated sizing exercises.

Automating Protection

3

When setting up your backups, you have some options.

One approach is to set up agents/connectors, set up the backup configuration, backup jobs, and backup targets. But that's a time-consuming manual task.

Remember, you moved to the cloud to reduce the burden on your IT team, right?

Here's a better option: Automated, policy-based backups using backup as a service (BaaS).

Ideally, BaaS should provide 1-click backups based on flexible policies —**"set and forget."**

Leave No Application Behind

4

Protecting applications in a dynamic, multi-cloud environment is very different than in a static, on-premises environment.

Manually configuring backups just doesn't work. You need a data protection solution that automatically discovers new applications—while providing application consistency.

Manually assigning backup policies negates the speed advantage of the cloud. So your backup solution should assign backup policies automatically.

But what if a developer forgets assign a policy tag? You need to ensure default policy assignment is in place to provide a critical "safety net."

Bottom line

Make sure your backup solution provides both automated and default assignment.

Recoverability

5

How can you ensure business continuity and resiliency?

You could perform a VM-level backup and manually recover it. But that requires time and effort, creating delays and disruption.

Or, you could use a backup as a service (BaaS) solution with automated recovery. When people are demanding that you restore their data NOW, having a simple, automated recovery solution speeds your restore process and reduces the pressure level.

Your BaaS solution should also provide the granularity to recover whatever people need—applications, databases, folders, or files.

Ideally, end-users should be able to recover files and applications themselves, speeding recovery and taking pressure off busy system admins.

Cloning

6

If you run multiple infrastructures—for development, testing, analytics, forensics, etc.—you'll want an efficient way to create cloned copies.

A good backup as a service (BaaS) solution can automate the process of creating application-consistent copies of your production environment.

It should provide the flexibility to clone applications, VMs, Kubernetes clusters, or containers, depending on the level of granularity needed. This functionality is a huge time saver, delivering real value.

Data Migration and Disaster Recovery

7

A key benefit of a multi-cloud infrastructure is the ability to move workloads around to meet changing needs. You can move from one on-prem infrastructure to another, from on-prem to public cloud, or from one public cloud to another.

Ideally, cross-cloud migration should be a simple “one-click” process. If moving a workload requires a big service engagement, you’ve lost the speed and agility advantages of the cloud.

You also want to think about disaster recovery (DR). Do you have DR functionality for all of your workloads or just for mission-critical tier one workloads, due to cost constraints?

Cost-efficient DR is possible when you do it intelligently.

Traditional DR software is designed to replicate a full production environment on the DR site. But a smart solution will store your backed-up copy but only use compute resources in the public cloud when you are in a DR situation.

Make sure you backup as a service (BaaS) solution provides this intelligent functionality.

Organizational Scaling

8

To control costs, you need the ability to scale to meet growing organizational needs without expanding your IT team.

Look for a backup and recovery solution that supports self-service, enabling business users to restore their own files without having to rely on IT. Think about how ATMs transformed financial services, increasing customer convenience while reducing overhead for banks. Your backup solution should deliver that same advantage.

Another important factor is **multi-tenancy.**

Most companies are divided into internal organizations or groups. In some cases, IT services may be charged back to these departments or groups.

Having a BaaS solution that supports multi-tenancy out of the box helps support organizational scaling.

Cost Efficiency

9

Assessing the cost efficiency of data protection is critical in multi-cloud environments.

When evaluating a backup as a service (BaaS) solution, make sure pricing scales with usage, so you only pay for what you actually need.

Also, a BaaS solution should be “smart” enough to recognize the varying topologies and characteristics of each cloud. This enables you to optimize your backup strategy while minimizing costs.

You also want the ability to leverage available cloud storage economics. Cloud vendors offer a range of storage options to meet a variety of needs. Your BaaS solution should be smart enough to use the right kind of storage in the right way.

Key Takeaways

Managing data protection in a multi-cloud environment is distinctly different than in a traditional, on-prem data center model. Hopefully, we've helped illuminate some best practices that can help ensure the most effective data protection, with the least risk of surprises.

When evaluating a backup as a service (BaaS) solution make sure it:

- Supports all elements within your infrastructure, both on-prem "clouds" and public clouds.
- Offers elastic scaling to keep pace with growth.
- Simplifies data migration, disaster recovery, cloning, and other advanced capabilities.
- Knows how to use the cloud cost-effectively.

Need more information on managing multi-cloud data protection?

Go to www.hycu.com.