GETTING SMART WITH MULTI-CLOUD DATA MANAGEMENT

Today, many enterprises are adopting a multi-cloud model as part of their digital transformation strategy. The multi-cloud approach makes sense for many reasons, but there are also many challenges to consider as organizations deploy multi-cloud strategy. Your enterprise will gain maximum value from the multi-cloud model as long as you properly manage, secure and protect your data.

In this tech brief, we will outline how companies should manage and protect data in a multi-cloud environment. We will also address the challenges of managing data in a multi-cloud environment, the benefits of cross-cloud data protection and components to look for in a solution.

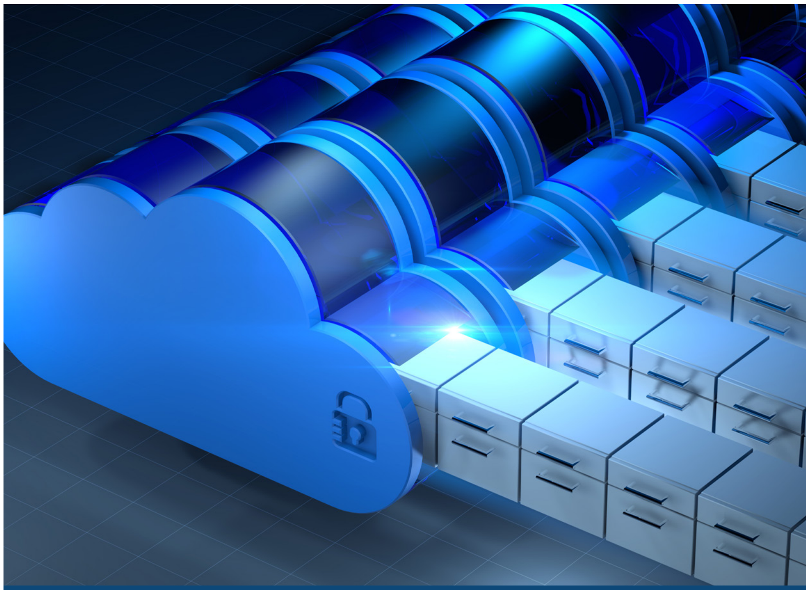
WHAT IS A MULTI-CLOUD MODEL?

For many reasons, including improved ROI, agility, autonomy and improved disaster protection, we have seen a shift away from in-house servers towards cloud computing. The multi-cloud model uses more than one cloud computing and storage service in a single architecture. Going forward, multi-cloud infrastructure is a trend that will only continue to grow in adoption. According to Cloudify's 2017: State of Enterprise Multi-Cloud report, 50 percent of organizations are managing more than one cloud. Nine percent are managing more than five clouds.[1]

There are many reasons an increasing number of organizations may opt for a multi-cloud infrastructure. With the multi-cloud model, you achieve greater reliability, more options to match workloads to the cloud service that is the right fit for the business need, greater flexibility, data sovereignty, competitive pricing—and enterprises are less susceptible to vendor lock-in.[2] Although there are many benefits to the multi-cloud model, it is not without its challenges.

CHALLENGES OF THE MULTI-CLOUD MODEL [AND HOW TO ADDRESS THEM]

With the ever-growing number of enterprises relying on multi-cloud solutions, protecting and managing data across all cloud types is key. In many cases, protecting digital assets will require a new mindset. Identity and access management, encryption, data migration, key management, security monitoring, risk analytics, backup and recovery are some of the top data management challenges enterprises face in multi-cloud environments.



Your enterprise can gain maximum value from the multi-cloud model as long as you properly manage, secure and protect your data.

There are factors companies need to consider and actions to take, in order to implement the optimal multi-cloud solution. Companies:

- ▪Should make sure data is managed through a single interface;
- ▪Must be able to implement a seamlessly integrated data management strategy;
- ▪Must know where the organization's data is held;
- ▪Need to be able to overcome next-generation backup and recovery requirements; and
- ▪Need to be able to augment the native capabilities with their own data protection systems.

This can be difficult. While challenging to manage multi-cloud environments, IT leaders need to strive for the optimal management. After all, leaving any business at risk for data loss, downtime and lost productivity is unacceptable.

Organizations working within a multi-cloud system need to understand that security is a shared responsibility. While enterprises need to communicate with the cloud provider when it comes to data security and backup recovery processes and policies, IT leaders cannot assume that the cloud provider will handle everything because they have outsourced the infrastructure. The company needs to have an efficient and effective method of protecting data while keeping it scalable for future growth. For maximum multi-cloud security, it is not enough to rely on someone else—*you need to be in control.*

If you are looking for a good place to start when it comes to managing multi-clouds, here are five questions to answer before moving forward:

1. What does it mean to have data spread across multiple cloud platforms?
2. Do you know where all of the data resides?
3. Can you retain control of data across multiple clouds?
4. Who owns data security and compliance in the cloud?
5. Who is liable if a data breach occurs in the cloud?

Better yet, ask each cloud provider the same questions, you may be surprised by their response. Having confidence with the answers to the above questions gets the enterprise moving in the right direction toward a well-protected and well-managed multi-cloud environment.

BENEFITS OF CROSS-CLOUD DATA PROTECTION

Effective multi-cloud data management requires a comprehensive, yet simple, automated and cost-effective approach. IT leaders will need to create a data protection plan to serve needs that is different from a traditional model, often referred to as a cross-cloud data protection plan.

This solution is a software platform that allows companies to back up, replicate and restore cloud-based apps within and across clouds.[3] Despite the built-in redundancy within cloud environments, organizations must implement a flexible backup technology with granular recovery tools.

So what does a solid cross-cloud data protection solution provide?

- **Data replication:** As companies transition to multi-cloud solutions, they demand a way to synchronize data seamlessly across multiple providers—cross-cloud replication makes this possible. Data replication allows entreprises to copy data from one location to another so that they won't lose data in the event of a disaster.
- **Application availability:** This allows companies to configure backup and recovery across cloud centers as needed.
- **Archival storage:** A high-performing cross-cloud data protection plan will make sure that active storage is

archived in a cloud data center that is different from the storage that hosts applications.

- **Data sovereignty:** Data sovereignty allows you to ensure compliance with all data sovereignty laws as well as industry and government-mandated regulations.

The right cross-cloud data protection plan will not just provide the security your company needs, but it will help with the smooth flow of business and guard against financial losses the company may otherwise encounter.

With these plans, the company's IT department will be able to realize increased uptime, fewer migration challenges, assured compliance, fewer required resources and a reduction in management costs.

Protecting data clouds will also help the organization maximize ROI. The business value of a cross-cloud data protection plan includes:

- ▪Higher productivity with less unplanned downtime;
- ▪Strong data protection to keep all data safe;
- ▪Increased customer satisfaction;
- ▪Increased agility;
- ▪Access to next-generation functionality;
- ▪Cost-efficiency; and
- ▪Protection against accidental deletions, outages, malicious attacks or any other type of data loss that organizations want to avoid.

Another option for enterprise storage functionality is software-defined storage (SDS). SDS decouples storage from a specific hardware platform and is managed through an intelligence layer of software.[4] With SDS you can consolidate multiple infrastructure elements into a single pool and then make changes as needed. This provides greater agility and flexibility, while also reducing cost.

To be safe, IT leaders should regularly test data recovery across clouds. Implement cross-platform single point-of-control tools that enable management across different cloud environments, both public and private.

WHAT TO LOOK FOR IN A SOLUTION

Include multiple key components within your cross-cloud data protection plan.[5]

The cross-cloud data protection plan should have the following protections, such as:

- ▪Support for all major clouds, both current and future
- ▪Support for private cloud integration
- ▪Support for all data applications, both current and future
- ▪Deployable in your data center
- ▪Simple user interface

And here are three pillars of best practices for a multi-cloud protection plan:

- ▪Encryption of data-at-rest in multi-cloud environments is essential to address categories of threats such as insider vulnerabilities or cyber-attacks.
- ▪Organizations must manage keys throughout the key lifecycle including the ability to generate, store, rotate, distribute and revoke keys as needed. It is more complex to manage across multiple clouds.
- ▪Organizations should make sure that cloud providers never hold or control the keys that encrypted the data.

A data protection plan should also include parameters for Recovery Time Objective and Recovery Point Objective. Recovery Time Objective (RTO) is the duration of time within which a business process must be restored to avoid unacceptable consequences. This is the time it will take to recover from a disruption. Recovery Point Objective (RPO) is the maximum time that the enterprise can have a disruption in service. Of course, these numbers are different for each business, but it is essential to clearly define RTO and RPO numbers.

Companies should also have a point-in-time recovery (PITR). This is a process that allows the organization to restore or recover a set of data from a time in the past if you have a PITR capable database.

SO WHAT DOES THIS MEAN?

It makes sense that a growing number of enterprises are adopting multi-cloud models today, but a multi-cloud environment does not have to be any less secure than single-cloud or on-premises infrastructure. Data needs to be managed, secured and backed up with an effective recovery process in place.

Given the complexity of managing a multi-cloud model, and the speed at which cloud technologies and services are growing, the other best practice is to talk with an IT solutions provider with cloud management and cloud security experience. A strategic IT partner can help the organization better navigate the challenges discussed in this paper, and can also help you right size cloud workloads for each cloud service so that you are only paying for what you use. Costs can quickly escalate when working with public cloud providers, so as the conversation should start with security and backup, talk through different scenarios and be sure to understand the associated cost implications. By taking the appropriate measures that are reviewed regularly and adjusted as needed, you will be able to protect your business, minimize risks and maximize performance.

TALK TO WEI TODAY

Ask the cloud experts at WEI to review your cloud and backup strategies to ensure your data is protected and ask how you can shave costs.

Sources:

[1] 2017: State of Enterprise Multi-Cloud Report
[2] The Benefits of Multi-Cloud Computing
[3] Multi-Cloud Complexity Calls For A Simple Cross-Cloud Data Protection Solution
[4] Architecting the Future Data Center with Multi Cloud Data Management
[5] Multi-Cloud Complexity Calls For A Simple Cross-Cloud Data Protection Solution

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

WEI
Dedication
meets
innovation.

info@wei.com
www.wei.com

43 Northwestern Drive | Salem, NH 03079
800.296.7837