

gamechanger

Game changing technology for guarding data in the cloud

How to Protect Data in a Multi-Cloud World

By Brien M. Posey

Are data protection needs lagging behind in your cloud strategy?



In enterprise class organizations, the question of whether or not to use the cloud has long been answered. Today, it is not a question of whether to use the cloud, but rather of how to realize the greatest benefit from the organization's multi-cloud strategy. Even so, adopting data protection strategies have sometimes lagged behind in the race to multi-cloud. Having data within multiple clouds does not diminish the need for data protection planning. As such, the enterprise needs to take a step back and objectively assess the degree to which its cloud resources are protected.

THE AVAILABILITY GAP

Some of the most significant data protection challenges commonly encountered by the enterprise in multi-cloud environments are Availability and protection gaps. These

are the gaps that exist between what the organization requires with regard to being able to protect its data, and what it can realistically deliver. For example, there is often a gap between the RPO and RTO that the organization needs, and the RPO and RTO that can be achieved for workloads running on a public cloud.

This gap not only prevents organizations from achieving the desired level of data protection, it can also lead to significant financial costs. According to one report (<https://go.veeam.com/2017-availability-report>), the average financial cost of Availability and protection gaps within the enterprise is a staggering \$21.8 million.

MULTI-CLOUD DATA PROTECTION

One of the most pervasive trends in enterprise IT over the past few years has been the adoption of a multi-

cloud strategy. According to a 2017 ESG study on public cloud computing trends, 81 percent of enterprises have a multi-cloud strategy. Now that multi-cloud deployments have become the norm however, organizations must seriously consider their Availability and data protection requirements.

The first step in this process is to consider what it means to adequately protect their data. Cloud data protection means more than just backing up on-premises resources up to the cloud. Organizations must also consider how to protect their resources residing in the cloud. This can mean backing IaaS resources up to a different Availability zone, or even to another cloud. Similarly, organizations must also develop a strategy for protecting Software as a Service (SaaS) data.

Cloud data protection means more than just backing up to the cloud. Organizations must also protect resources residing in the cloud.

CLOUD BACKUP AND DRaaS

Cloud backup and DRaaS has become extremely popular over the last several years, because such services provide a comparatively inexpensive way of ensuring the continuity of business. Even so, the DRaaS market is still maturing, and many vendors focus on a specific aspect of DRaaS rather than providing a comprehensive, multi-cloud solution.

Some of the available solutions for example, are public cloud centric, and are based around a specific public cloud such as Azure or AWS, rather than being cloud agnostic. Other solutions tend to be more flexible, but may lack application level support for services such as SQL Server or Exchange. A good DRaaS solution must be a true multi-cloud solution, and should work with all of an organization's VMs, regardless of the virtualization platform, guest OS, or applications that are being used.

SAAS AND IAAS BACKUPS

Perhaps the most overlooked aspect of cloud backups is that of protecting SaaS data. In some cases, this may be attributed to an assumption that the SaaS provider

is backing up their subscriber's data. In other cases, it is possible that admins do not realize that it is possible to backup SaaS cloud data. Whatever the reason SaaS data needs to be protected, just like any other data.

Every SaaS provider has its own way of doing things, but most will not perform restorations on behalf of their subscribers. If an organization needs to revert its SaaS data to an earlier point in time, then using an independently created option may be the only option for doing so. It is also important to consider that relying on the SaaS provider to back up your data leaves you at the provider's mercy. If the provider suffers a data loss event, and you do not have your own backup, then you may be left with no recourse.

When IaaS clouds first began to see mainstream adoption, organizations sought to back them up in any way possible. This almost always meant however, that an organization used one backup solution to protect its on-premises resources, and another to protect IaaS cloud resources. Organizations that were early adopters of multi-cloud architectures often had to use a separate backup solution for each cloud.

CROSS CLOUD DATA PROTECTION (WITHIN THE CLOUD)

One of the primary data protection goals for today's enterprises should be the consolidation of data protection resources. By using a single, extensible data protection platform to protect on-premises, multi-cloud IaaS, and SaaS resources, an organization can simplify its data protection architecture. This approach also allows backup admins to use a cohesive interface that spans all resources, which can help an organization to reduce costs, while also making it easier to spot protection gaps.

Perhaps even more importantly, standardizing around a single data protection solution allows for uniform data recovery capabilities. Organizations that utilize a multi-vendor approach to data protection may find that some of the data protection applications that they use provide better RPO and RTO capabilities than others.

CONCLUSION

Today, it is more important than ever for organizations to take an objective look at their data protection efforts. Data protection and Availability need to be front of mind because 66 percent of enterprises admit their digital transformation initiatives are being held back by unplanned downtime, and over half of the US businesses that suffer a cyberattack lose data.

VEEAM'S GAME CHANGING SOLUTIONS FOR MULTI-CLOUD DATA PROTECTION

Veeam is the number one Availability provider for any app, any data, across any cloud. Veeam was recognized as a leader in Gartner's Magic Quadrant for 2017, and named to Forbes 2017 list of the 100 best cloud companies for the second time. Additionally, the company reports a customer satisfaction rate of 91 percent, which is about two and a half times higher than the industry average.

HOW VEEAM ADDRESSES MULTI-CLOUD DATA PROTECTION

The cloud is not one-size-fits-all, and providers have worked to create different cloud environments and architectures to meet the needs of the multi-cloud enterprise. A data protection strategy that leverages existing cloud investments affords organizations of all sizes the opportunity to protect workloads running within the cloud of origin, and even across clouds. For example, AWS users can get the most of out their AWS EC2 investments by backing up data locally, or by leveraging AWS Glacier Cloud Storage or AWS S3. With Veeam, you get seamless Availability solutions that allow you to leverage the right cloud for your data protection business needs.

VEEAM IAAS AND SAAS DATA PROTECTION

What is your Availability strategy for your applications running in the cloud? Many enterprises that run cloud-based applications assume those workloads are protected on their behalf, but the reality is you are responsible for complete data protection.

Public clouds are responsible for the underlying infrastructure that your workloads run on, but they are not intended as a backup solution. Human error, retention policy misunderstandings, as well as internal and external security threats still exist in the cloud and require a strategic backup and recovery plan. The Veeam Agents ensure the Availability of Windows and Linux workloads running on any public cloud, including Azure Virtual Machines and Amazon EC2 instances. You can also backup and recover workloads running in the IBM Cloud.

Microsoft Office 365, one of the most popular SaaS clouds, includes built-in georedundancy to ensure your

users remain connected, but they are not responsible for your data — you are. Office 365 backup is a necessity in today's digital transformation where it is all too common to see accidental deletion scenarios, retention policy gaps and internal or external security threats.

VEEAM CROSS-CLOUD DATA PROTECTION

It is widely accepted that cloud computing delivers numerous benefits for today's enterprise. Although cloud providers leverage fully redundant architectures, a comprehensive backup application with granular recovery tools is still a must. The need for such tools becomes even more pressing as enterprises move to a multi-cloud strategy, because of the need to protect data within any cloud, and across availability zones. Veeam ensures that applications and data remain

Although cloud providers leverage fully redundant architectures, a comprehensive backup application with granular recovery tools is still a must.

protected and always-on, regardless of their location.

VEEAM PARTNER SOLUTIONS

Veeam has partnered with a number of cloud providers including Microsoft, AWS, and IBM Cloud, to offer the best in class protection for enterprise data in multi-cloud environments and an ecosystem of over 16,000 cloud service providers to meet your local needs. Veeam is the definitive solution for organizations that are serious about achieving comprehensive data protection for their multi-cloud environments.

Find out more:

<https://www.veeam.com/multi-cloud-enterprise.html>

