the Availability Digest

www.availabilitydigest.com
@availabilitydig

Cloud-to-Cloud Backup

February 2018

There is an increasing trend for companies to run their applications in the cloud. Whether a public cloud or a private cloud, cloud computing has the advantage of eliminating the need for dedicated servers for application processing. Furthermore, the cloud provides the scalability necessary to support an application. If the application load should suddenly increase, the cloud can provide additional processing resources. When the increased load diminishes, the cloud can recover those resources and use them for other purposes.

However, though clouds have proven to be highly available, they do occasionally fail. All application data stored in the cloud can potentially be lost. It is therefore important to back up that data so that it can be recovered in the event of a cloud failure. Though cloud data can be backed up by on-site backup hardware, it makes more sense to back up the data in another cloud. Cloud-to-cloud backup is the practice of copying data that is stored on one cloud to another cloud.

Why Are We Seeing the Emergence of Cloud-to-Cloud Backup?

Moving applications and workload to the cloud poses risks. The control of storing and protecting the company's data is being handed over to a third party. Therefore, it is imperative that this data be recoverable. For full protection of data generated by cloud-based applications, cloud-to-cloud backup is the answer.

The third party to which the data is being handed is typically a Software-as-a Service (SaaS) provider. SaaS has become a common delivery model for many business applications. SaaS is a software licensing and delivery paradigm in which software is licensed on a subscription basis. It is centrally hosted and is accessed by users using a thin client via a web browser.

Software-as-a-Service suppliers typically take responsibility for infrastructure availability, but data loss is the sole responsibility of the client. It is interesting to note that human error is the most common cause of data loss. Though companies invest the resources to provide redundant servers, storage arrays, and networks to protect their data, they rarely invest in redundancy for humans. For any critical action that could cause data loss, there should be two people involved – one to enter the command and the other to check it before it is executed.

Cloud-to-cloud backup provides several advantages over local backups:

- Lower infrastructure costs – there is no need for redundant servers, storage arrays, and networks.

- Faster backup and recovery – data is immediately available from the cloud without the need to reconfigure local hardware to recover data.

- Greater flexibility – data can be accessed from anywhere and can be stored and retrieved in any format.

Cloud-to-cloud backup has gained popularity because it eliminates the management and maintenance of storage hardware and software. It takes the management and maintenance of hardware out of the equation for the customer.

In the Forrester report "Back Up Your Critical Cloud Data Before It's Too Late," a Forrester senior analyst urges users not to ignore cloud-to-cloud backup. "Many SaaS providers will not restore lost data for users or will only do so for an exorbitant fee," the report notes.

The report lists risks to information stored in a cloud application. These risks include data that is lost during data migration to the cloud or from one cloud vendor to another, accidental deletion of information by the users, malicious insiders, departing employees, cyber criminals and rogue applications.

"For years, it has been standard practice to back up your critical data. … Yet, every day, enterprises send critical data to SaaS providers without any plan for how they will back up the data and restore it," the Forrester report states. "Only when an enterprise experiences data loss does it ask the question, 'Who is responsible for backing up my data?'"

Other Advantages of Cloud-to-Cloud Backups

Storing data in the cloud via cloud-to-cloud backups has several other advantages besides protecting the data:

- Cloud backups are accessible from anywhere.

- Organizations can use the backed up data for data mining and analytics without putting the original data at risk and without impacting data access to the primary copy of the data (performance offloading).

- Backup services will allow customers to make backup copies of any data that is stored in one cloud to another cloud backup, like Amazon Web Services. These copies typically include metadata and audit logs that can be searched for quick and granular restores.

Multiple locations are advised for backups to provide added data security. Cloud-to-cloud backup offers users a convenient way to have data stored in many locations. However, this puts the data at an increased risk of breaking and being stolen. Hence, data must be encrypted.

What to Look For in a Cloud Service

CIOs should understand how their cloud data is backed up. A cloud service that will be used to store primary or backup data should have multiple data centers and redundant data stores to ensure business continuity and the ability to recover data in the event of any failure in the infrastructure. IT teams should be able to restore their data to any provider that supports the application, to a VM running in the cloud, or to a local data center.

Cloud services are highly reliable, but they do fail. Therefore, it is important to check the cloud service SLA. Typically, the SLA is unlikely to guarantee that data can be recovered or what the recovery times will be. The SLA will offer only a 'best efforts' commitment.

Backupify and Spanning seem to be the most popular cloud-to-cloud backup service providers, mainly because they attract bigger companies that are taking steps to protect their cloud data. Backupify claims to have 1.7 petabytes under management from over 7,000 business customers, some with tens of thousands of employees. Spanning claims more than 3,000 customers including Netflix.

Where Is This Technology Headed?

The cloud-to-cloud backup market is moving to a managed pay-as-you-go model. The cloud-to-cloud backup providers will manage the storage and retrieval of an organization's data and will charge the customer only for the storage used.

The main backup suppliers are planning to add support for cloud copies of entire virtual machines (VMs) including the VMs' host operating systems.

A present-day concern is that many cloud-to-cloud backup providers typically will protect only a few applications. However, on a good note, these providers are adding more applications and abilities all the time.

Summary

Cloud-to-cloud backup provides an economic and flexible way to protect data stored in a cloud. It requires no on-site hardware that imposes management and maintenance costs. The storage of data can be geographically dispersed to protect it from local disasters. The data can be backed up and recovered quickly, and it is available from anywhere.

Look for cloud-to-cloud backup to become an ever more popular method for protecting data stored in a cloud.

Acknowledgements

Information for this article was taken from the following sources:

Cloud-to-cloud backup: What it is and why you need it, *Computer Weekly*; undated.
What Is Cloud-to-Cloud Backup and Why Is It Necessary, *Local Web*; undated.
Cloud-to-Cloud Backup, *Tech Target*; undated.
WhatIs