Cloud Storage: How to Pick a Provider

Crystal Bedell
Network Computing (www.networkcomputing.com)
08/26/2014

When it comes to enterprise cloud storage, there's no shortage of providers. Here's what you need to consider in order to make the right choice.

Enterprise cloud storage offers a number of benefits -- scalability, reduced infrastructure and predictable costs, to name a few. But moving data to a public cloud introduces a host of new concerns that organizations must address when evaluating providers.

To further complicate matters, no two enterprise cloud storage providers are alike. Service-level agreements, pricing models and regulatory compliance know-how differ greatly from one service provider to another. Here are the top factors to consider when choosing a cloud storage provider. If you take the time to weigh these factors, you can proceed with confidence.

DETERMINE WHAT DATA TO STORE IN THE CLOUD

Before you begin evaluating specific enterprise cloud storage providers, you must determine what type of service you need. Are you looking for a backup and recovery service or primary data storage? This will help determine what data you wish to move to the cloud. If you plan to use the public cloud as your primary data storage, a bottleneck can occur between your data center and the WAN. Avoid data sets that are new, very active across the entire data set or extremely large. Instead, choose data sets in which only a small percentage of the data is active at any point in time. Large but granularly accessible, inactive data sets also work well. In both cases, small data sets can be easily cached locally on an appliance or virtual machine, while the remaining data sets are stored in the cloud.

SECURITY

Encryption is the primary security mechanism used to protect data stored in the cloud. When evaluating enterprise cloud storage providers, ask the provider where and when data is encrypted. At the very least, your data should be encrypted when it is at rest, and you should maintain possession of the decryption keys. This gives you some control over who can see your data if the provider must hand over data to legal authorities as a result of a subpoena. Some providers also encrypt data in motion -- that is, while it's transmitted to the cloud. If the provider uses local storage to cache data as it moves back and forth between your site and the provider's cloud, then the local storage should be encrypted as well.

REGULATORY COMPLIANCE

Storing regulated data in a public cloud can complicate compliance efforts, but it doesn't have to impede your move to the cloud. Look for an enterprise cloud storage provider with experience working with auditors and meeting the same regulatory requirements as you. To avoid data residency issues, look for a provider that stores data locally. This extends to disaster recovery, too. Get it in writing that the cloud storage provider is completely localized and does not use remote data centers for disaster recovery. Because regulatory requirements often change, consider detailing in the SLA the provider's role in helping you comply with changing requirements and the fee for doing so.

AVAILABILITY

Availability varies from one cloud storage provider to another. Your requirements should be dictated by your use case. Determine your availability needs, what you can expect from your provider and how you'll augment that if needed. Availability is critical if you're using cloud storage as your primary backup, to store primary block-based storage or as a NAS storage area. You can increase availability by using two different cloud providers or by choosing a provider that can provide redundancy. Regardless of which you choose, make sure you know how to connect to the redundant copies when a failure occurs.

PERFORMANCE

Cloud storage providers have addressed many of the problems associated with low bandwidth. Nightly backups and individual file restores aren't an issue. However, initial backups and full-server recoveries are still problematic, even when providers use deduplication and compression to minimize the amount of data transmitted over the wire. An initial baseline backup must be competed for deduplication to work. During this process, which can take days or weeks, you don't have a second copy of data offsite. An onsite disaster could result in permanent data loss. For full server recoveries, many providers will fire up your servers in their cloud while restoring them to your data centers. This buys them time, but doesn't guarantee the performance you need.

The simple answer to both of these problems is to work with a provider that is willing to supplement your storage and backups with tape. During your initial baseline backup, make a tape copy and overnight it to the provider. Similarly, when a full server recovery is necessary, have your cloud storage provider put the server on tape and overnight it to you.

THE SERVICE LEVEL AGREEMENT (SLA)

Cloud storage providers typically use a boilerplate service-level agreement (SLA) for all their customers. While some terms, like average data access time, are typically fixed, IT organizations can negotiate other terms. Pay close attention to availability and downtime. Providers differ in how they measure downtime, so read the fine print and make sure it matches your business' requirements. Also look at the terms pertaining to geography, security and privacy. It is up to you to ensure that suitable measures are in place to meet your security and regulatory requirements. Make sure the SLA specifies the scenarios under which the provider can read your data. While the provider needs to read your data to move it, the provider should not be able to read your data for any purpose other than support. Finally, ensure the cloud provider has the technology, design and architecture to support the SLA.

GETTING YOUR DATA BACK

Sooner or (hopefully) later, your relationship with the cloud storage provider will come to an end. Before you move any data to the provider's cloud, make sure you know how and when you'll get your data back if you decide to move your data to another cloud or back on premise -- or in the event the cloud provider goes out of business Find out how long it will take to get your data, what form your data will be in, and whether you can get all copies of your data. Also ask the provider if there are fees associated with these processes and if you have to pay for storage while data is returned to you. All of these points should be addressed in your SLA.

PRICING MODEL

A cloud-based storage solution will not necessarily save you money. It will, however, shift storage spending from a capital expenditure to an operating expenditure. As you evaluate enterprise cloud storage providers, it is important that you understand pricing models so you can accurately compare cost benefits. Most providers charge customers based on average storage consumption during the month. Other factors can also come into play, such as availability and redundancy. Storing extra copies or having a redundant means of accessing data will increase your cost. Additional services like data management can also impact cost. Alternatively, a provider may charge based on the amount of data you recover during the course of a month.

HYBRID CLOUD STORAGE

Moving data to the cloud is not an all-or-nothing proposition. IT organizations are increasingly deploying a hybrid model, whereby on-premise storage is supplemented with public cloud storage. New or frequently used data is stored onsite while inactive data is stored in a storage provider's cloud. All of this should happen seamlessly. It can occur via the provider's proprietary software, or a cloud storage appliance or a gateway. However, be cautious of cloud storage gateways that aren't fully integrated with the cloud storage solution.

Crystal Bedell is a freelance technology writer specializing in security, cloud computing and mobility. As the principal of Bedell Communications, she helps technology providers and IT media companies create engaging thought leadership content. Prior to launching Bedell Communications, Crystal worked for TechTarget where she was the editor of SearchSecurity.com for eight years.