SPONSORED CONTENT Redmond MAGAZINE

gamechanger Game Changing Technology for Managing Cloud Data

Why Is It Important to Manage Backups in the Cloud?

Don't count on cloud providers to protect your data.

There's a common but dangerous misconception about application availability in the cloud. Essentially, it's the belief that cloud providers are responsible for backing up and guaranteeing availability for client workloads running in providers' data centers. Isn't that why companies pay for cloud services?

The answer is yes and no, and it should be pretty clearly stated in most cloud service contracts. Yes, the provider is responsible for protecting the infrastructure that runs workloads, meaning the equipment that the provider itself owns and manages.

But protecting and guaranteeing access to actual data and applications is a responsibility that falls squarely on the shoulders of the client, and it's one companies have to take seriously.

Business-critical apps simply can't go down in an era in which customers, partners and even employees have very little patience for downtime. Outages can lead directly to lost customers and, as a result, lost revenue. The results can be devastating.

That's why backup and recovery—the backbone of application availability—can get a little complicated. Cloud backup might not be as straightforward as it seems. Just because an app runs in Azure or Amazon Web Services (AWS), that doesn't mean old school operating systems aren't involved.

The fact is that many cloud deployments today have Windows or Linux instances running behind them and managing workloads. That means cloud backup has to be flexible enough to accommodate multiple platforms and operating systems.

VERSATILITY IS CRITICAL

There is probably no more important quality to have with cloud backup, in fact, than versatility. Availability shouldn't come down to whether a company uses Azure, AWS or some other cloud provider, and the operating system managing apps in the background shouldn't be a factor, either.

A backup and recovery system should cross platforms, and any vendor that offers cloud backup and recovery should have the capability to back up data regardless of which operating system manages workloads.

But there's more to versatility than just working with multiple cloud providers or OS setups. Take, for instance, the need to move data from a cloud provider to an on-premises data center. Several scenarios could necessitate that move, such as ending or changing a relationship with a cloud provider, dealing with an unexpected provider outage, or just simply wanting to have the option to manage some data or workflows in-house.

The right backup and recovery system will facilitate moving data—or an entire workload—

Pixome / Shutterstock.com

from the cloud provider to a company's own data center. Similarly, the right system will also handle moving data and workloads to another cloud region if necessary, should traffic spike in, say, Asia-Pacific and necessitate a move.

The point is that backup and recovery has to be flexible in how it works across platforms and with disparate operating systems, as well as how it enables an organization to move and shift data and workloads running in the cloud. Anything less leaves companies susceptible to problems such as major management headaches, cost overruns and paralyzing downtime.

AND SO IS GRANULARITY

Of course, versatility and flexibility are only really useful if they facilitate providing exactly the kind of backup a company needs. In other words, it's fine to be able to back up a whole system or workload across multiple environments, but it's rare that an organization needs to recover everything in a system all at once.

The much more likely scenario is that a particular element in a cloud deployment will need recovering. For instance, it's far more common to need to bring back just one file, a single folder or a procedure store in SQL server than it is to have to revive a whole system all at once.

If a backup and recovery system can't find just one element and bring it back in line, its value is limited. It's a waste to have to reboot a whole system when only one file or folder is corrupt and needs recovering. The right backup system will offer granular recovery so that IT professionals don't have to get bogged down in recovering elements of their systems that aren't causing problems.

All of the data movement that a good backup and recovery system should facilitate in the cloud is useless if encryption breaks down.

Granularity conserves both human and system resources and enables IT professionals to recover what they need quickly and without complex management requirements. In an environment in which downtime can quickly become devastating, granular recovery enables companies to react with speed and precision in keeping workloads available.

DON'T FORGET ENCRYPTION

Of course, no system of any kind can be effective if the data in it isn't secure. The danger of breaches is obvious and well documented, but some companies still don't pay enough attention to one critical element of their cloud deployments: encryption.

Yes, cloud providers do provide a level of encryption. However, data security has long been one of the primary concerns surrounding moving applications into the cloud, and it should be. While provider encryption might be adequate, companies should take no chances. They need to have encryption capabilities of their own.

The right backup system will offer granular recovery so that IT professionals don't have to get bogged down in recovering elements of their systems that aren't causing problems.

All of the data movement that a good backup and recovery system should facilitate in the cloud is useless if encryption breaks down and puts data security at risk. Running encryption on top of what cloud providers offer isn't just a precaution—it's a necessity, and it's one that many companies overlook to their peril. With the right backup and recovery system in place, strong encryption ensures that data and workload movements are safe and helps bolster availability.

MANAGING BACKUP ENSURES AVAILABILITY

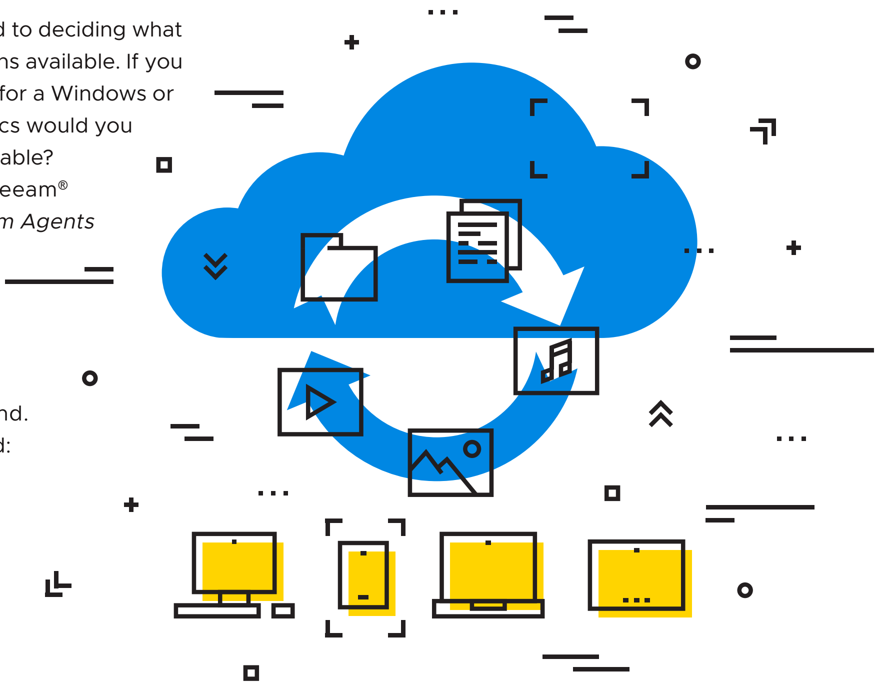
The cloud has introduced efficiencies and cost savings to companies running hosted applications, but simply migrating workloads to the cloud isn't enough to guarantee availability. The popular myth that cloud providers take care of everything is dangerously false.

On a data and workflow level, backup and recovery—availability, essentially—are the responsibility of the company that owns the app, not the provider that owns the equipment that hosts it. That's why overlooking backup and recovery is a huge and possibly devastating mistake.

But with the right backup and recovery setup, one that offers versatility in design, granularity in backup and strong encryption, companies can manage highly available apps with confidence and without unnecessary risk.

Backup and Recovery with Veeam Agents for Microsoft Windows and Linux

Veeam is rethinking data and application availability.



It is an interesting time today in regard to deciding what and how to make data and applications available. If you were to make a new backup product for a Windows or Linux operating system, what characteristics would you include to keep data and applications available?

That's exactly some of the logic that Veeam® went through in launching the new *Veeam Agents for Microsoft Windows and for Linux*. These new products are recently available from Veeam and provide the ability to back up these operating systems, but from the start were built with new use cases in mind. The use cases are rather straight forward:

- Workloads in the public cloud
- Physical servers
- Mobile workforce (PCs/laptops)
- Workloads on alternate hypervisors

This is a broad step and Veeam has been working on this initiative for years. Starting in 2014, finally the most recent milestone in *Veeam Agent for Microsoft Windows* was becoming available just this May at VeeamON. Highlighting the workload in the public cloud use case is particularly useful today.

There is a strong set of capabilities for Windows and Linux workloads with the Veeam Agents. This includes the ability to recover files, application items, the entire system, volumes and more. Additionally, for systems running on-premises or as a mobile system, the Veeam Agents have the capability to restore the backups directly to Microsoft Azure.

What is clear is that if workloads are to run in the cloud, there is a need to keep them available. Additionally, organizations have a responsibility with that data (much like what they have for on-premises workloads). With the *Veeam Agents for Microsoft Windows and Linux*, backups can be taken of systems in the public cloud and then those backups can be moved to on-premises storage resources as well as other targets. This is an important aspect of data management, it's not a discussion on whether one cloud may fail; it is about an organization managing the flow of their data and keeping it available.

Additionally, of interest about the *Veeam Agents for Microsoft Windows and Linux* is the fact that there are three editions: Free, Workstation and Server.

This is very versatile in that the free edition is attractive to a PC or laptop user but also maybe lesser critical cloud workloads. The Server edition is attractive in that advanced features such as file system indexing, application consistency and log truncation are configurable options for critical workloads.

Whether the workloads are on-premises as physical servers or PCs and laptops, running on alternate hypervisors or in the public cloud: There is a need for the Availability experience that is required to meet the demands of an Always-On Enterprise™ today.

You can download free editions of Veeam Agent for Microsoft Windows and Veeam Agent for Linux at www.Veeam.com.

VEEAM

Alecs Orel / Shutterstock.com