Windows IT Pro

THE ESSENTIAL GUIDE TO:

The Biggest Challenges with Cloud Backup & Cloud Disaster Recovery

By Orin Thomas

The last few years have seen some big changes in backup and disaster recovery. As with almost every other aspect of IT, the cloud is making its presence felt. Integrating the cloud into a backup and disaster recovery strategy involves rethinking many of the ideas on how organizations go about managing these processes. In this essential guide you'll learn about some of the challenges around cloud backup and disaster recovery including:

- The traditional way of doing off-site backup and recovery
- Cloud security worries
- Concerns about pricing blowouts
- Managing and monitoring cloud backup and disaster recovery
- Taking advantage of Disaster Recovery as a Service

The traditional way of doing off-site backup and disaster recovery

To understand the new challenges that cloud backup and disaster recovery present, you need to remember some of the traditional ways of handling backup and disaster recovery. It's straightforward to remember that organizations with a great backup and disaster recovery plan back up critical workloads frequently and perform recovery drills to ensure that their disaster recovery preparations provide the needed coverage. One aspect of a great backup and disaster recovery plan is moving backed up data off-site to a secure location. Another aspect is having a separate disaster recovery site.

Moving backed up data off-site protects organizations from those events where the location that houses the original workloads itself is lost, such as when a critical site is destroyed by a natural disaster such as a flood during a hurricane. While the original on-premises site may be written off, the data, at a separate location, is still safe.

Traditionally in scenarios where a critical site is lost, a special site, known as a disaster recovery site, is brought online. This disaster recovery site has the necessary infrastructure to host the critical workloads from the original site. The backed up data at the secure site is recovered to the infrastructure at the disaster recovery site and the organization retains access to critical workloads while the original site is restored to operation.

Getting backed up data off-site has, in the past, involved organizing a courier to come to your site and physically move the backup media from your site to the safe storage facility where the backup media is kept. This process has often been cumbersome and bureaucratically intense. Backup administrators also dreaded the occasional call from reception informing them that the courier hadn't arrived to do the pickup of the most recent set of backup media before the organization's doors were shut for the night. For

many small businesses, they might simply skip the costs associated with such a service and the IT Pro might simply throw company backup tapes in the trunk of their car and store them at home – talk about compliance, regulatory and security issues!

The cloud as a way of moving recovery data off-site

Several factors have come together to make moving data off-site using tapes less common than it used to be. These factors include:

- The cost of shifting data massive amounts of data over the Internet has declined dramatically.
- Broadband speeds continue to increase, making it feasible to shift gigabytes of data every day between an on-premises location and the cloud.
- The cost of storing vast quantities of data in the cloud has declined dramatically.
- The functionally limitless storage capacity of the cloud, as long as organizations are willing to pay for it.
- The concept of hybrid cloud is building a lot of momentum. By keeping copies of data on-site as well as in the cloud, you can cover the majority of recoveries on-site from recent copies.

Rather than have to deal with the complexities of ensuring that physical media is physically transported from the organizational location to a secure off-site facility that specializes in storing backup media, recovery data can be transmitted over the organization's Internet connection and stored in the cloud.

Cloud security worries

It's been said that change can resolve existing challenges only to introduce brand new ones. Shifting from a process where backup media is driven to a special off-site facility by a courier to having data moved off-site to the cloud is the sort of change that brings new challenges and concerns.

Perhaps one of the biggest concerns that organizations have about cloud backup and disaster recovery is that of security. A well-executed data protection plan backs up all the information that an organization might need to restore to ensure that the business can continue operating.

A challenge around backups is that if a nefarious third party gets access to that backed up data, they have access to all of the critical information generated by and owned by the organization. If you look at the advertising around off-site storage of backup data, much of it uses imagery of something of a cross between a nuclear bunker and a bank vault. This imagery is used because it is designed to reassure organizations that their backed up data is in a secure location, somewhat similar to a bank vault.

With a traditional off-site backup provider, access to the backup tapes involves multiple layers of security. Someone can't just turn up at the off-site backup provider and request tapes. They must provide appropriate physical identification before someone hands over the tapes. An additional layer of security allows organizations to encrypt the backup media so that the data stored there cannot be accessed by anyone except for a person who has access to the decryption key. Encrypting backed up data means that even if someone at the backup storage facility did manage to steal backup media, they couldn't recover the data stored on the tape.

The cloud doesn't provide those obvious external signifiers of security. Imagery around the cloud involves long rows of server racks, rather than Fort Knox style security. Organizations that are unsure of the process might be concerned that someone may be intercepting protected data as it is transmitted from the organizational site to the cloud. These organizations might also be concerned that data stored in the cloud may be accessible to hackers. You will be hard pressed to find a media article written that "Cloud X successfully protects customer Y's data," yet almost every week brings a story of data stored in the cloud being improperly protected and exposed. People naturally worry that by shifting their backed up data to the cloud rather than to a secure storage facility similarly means that their data may end up exposed by malicious third parties should they make a configuration error or other slip.

The reality is that, if properly implemented, protected data can be protected by encryption before it even leaves the company's network, it can also be encrypted in transit to the cloud and at rest while it is stored in the cloud. The key to ensuring that protected data remains secure is to partner with an organization that is experienced in securely shifting and storing protected data in the cloud.

Concerns about pricing blowouts

Another concern that organizations have about moving backed up data to the cloud is around cost. While it might be cheap to export data from organizational sites to the cloud, organizations are concerned that significant expense will be incurred when that data needs to be brought back from the cloud in the event recovery is necessary. They worry that while shipping data to the cloud is cheap, the cloud provider has the organization over a barrel when that data needs to come back as a part of your recovery process.

There is also the concern that while things may be cheap during an initial trial period, once an organization becomes locked in and dependent on the cloud provider, the cloud provider can turn around and increase their rates.

By partnering with an organization that is experienced in these matters, organizations can get reliable estimates of the cost of any or all operations related to cloud backup and recovery, including implementing Disaster Recovery as a Service (DRaaS). You'll learn more about DRaaS later in this guide.

How quickly can I recover my data

One thing that many have learned about storing data in the cloud is that the cost of cloud storage usually involves trading speed of storage for price of storage. You can get exceptionally fast storage from cloud providers if you pay an exceptional price. You can get exceptionally cheap storage, but your ability to write and read from that storage is going to be at a speed drastically lower than that of the more expensive option. While it's great to be able to store petabytes of data cheaply, it's less wonderful if it takes days or weeks to restore that data should it be required. Some providers specialized in off-site backup offer services to speed up the restoration process by allowing large volumes of data to be repatriated to the on-premises environment through physical media, though the amount of time that this might take to organize will vary depending on service level agreement.

An advantage of shipping tapes off-site in a courier van is that even though it is an old technique, it's a very effective method of moving terabytes, even petabytes of data from one location to another and can, in many cases, be much faster than transferring the same amount of data over the Internet.

By partnering with an organization that is experienced with cloud backup and recovery, it's possible to find a balance that's right between the cost of cloud storage and the speed at which data can be recovered from the cloud. Often you might find you need a mix. For business critical applications and data, you

might be willing to pay a higher price, and for other less business critical components, you forgo certain write and read privileges. Organizations that are experienced in working out this balance are going to be able to do a better job at finding the right mix for your company than you would if you attempted to determine this information for yourself.

How long can I store my data in the cloud?

One big challenge for the storage of data in the cloud is compliance regulation. Most compliance regulation requires data to be stored for periods in years or more, with 7 years being a common requirement in many jurisdictions. With the traditional specially climate-controlled off-site vault approach to storing backup media, backup media can be stored indefinitely for the right price. Should auditors require data from backups taken in years past, then that backup media can be retrieved and recovered as necessary.

Using the cloud for long-term data archival may not replace this type of off-site storage entirely; it may simply reduce your need to utilize such facilities. Many organizations now store their protected data in the cloud, whilst also sending backup media to a secure location on a periodic basis to a secure location to meet compliance requirements. It's critical to note that using cloud-based backup and disaster recovery isn't an all-or-nothing proposition. It's possible to still use off-site locations for some types of protected data while primarily using the cloud to host the majority of the protected data workload.

Similarly, many organizations that adopt a cloud backup and disaster recovery strategy still initially back data up to on-premises data storage. Data then replicates from the on-premises storage to the cloud for longer-term off-site storage. Most recovery operations, which almost always involve recent data, occur primarily using the on-premises storage. Those recovery options that require older protected data are able to retrieve it from storage in the cloud. This aligns with an industry best practice known as the "3-2-1 Rule," stating that a business could maintain three copies of their data, on at least two types of media, and that one of those copies should be off-site.

Managing and monitoring cloud backup and disaster recovery

Organizations are often looking for solutions that integrate into their existing products or work in a similar manner. A solution that requires administrators to immerse themselves in a new way of thinking as well as a completely new toolset isn't going to work as well as a solution that is an extension of an organization's current administrative tools.

The best cloud backup and disaster recovery tools use a "single pane of glass" to allow backup administrators to perform all important tasks related to backing up data from on-premises servers to the cloud, as well as recovering data when necessary, either from an on-premises store of protected data, or from data stored in the cloud.

Recovery scenarios are often stressful, and the last thing that backup administrators need when they are under duress is a user interface that is so complex that it makes the startup procedure for a nuclear submarine appear intuitive.

Also while under duress, it is critical that the IT administrator has confidence that the backup is recoverable. Many automated backup and replica testing technologies exist to frequently test backups within an isolated environment to ensure their recoverability in those difficult, pressure-packed situations.

An effective cloud backup and disaster recovery solution requires meaningful monitoring and telemetry functionality. It will include a console that provides information about the success and or failure of backup jobs, detailed data about the amount of data backed up, the amount of data that can be backed up, retention information, and everything else an organization might need to know about their cloud-based backup and disaster recovery solution.

A great solution will tell you about problems as they occur and should provide actionable guidance towards remediation. It's important to be able to see the state of the solution at any point in time, rather

than having to wait for a report to be emailed through informing you whether or not a backup or recovery operation has completed successfully. This provides an IT administrator with the ability to be proactive in correcting issues, opposed to reacting in more common pressure situations.

Taking advantage of Disaster Recovery As a Service

Disaster Recovery As a Service (DRaaS) provides an alternative to the traditional model of recovering data to an on-premises server in the case of failure. With DRaaS, when a hardware failure occurs that requires a server be recovered entirely, instead of performing the recovery to another server on premises, you can instead recover that workload so that it runs in the cloud. DRaaS is ideal for small businesses looking to get their data off-site without the cost and complexity of building or maintaining a second infrastructure, but it is also becoming more appealing to larger enterprises because it is becoming increasingly cost-effective.

DRaaS allows customers to failover an on-premises infrastructure to a multi-tenant cloud environment. Organizations pay for the infrastructure in the cloud as they use it, as opposed to the cost of maintaining a remote DR site with hardware that replicates the on-premises infrastructure.

In the past, DRaaS was relatively simple for small organizations with a simple, straightforward network infrastructure – because it was relatively easy to recreate a simple infrastructure in a cloud environment. Today, DRaaS capabilities have evolved to the point where complicated network infrastructures can be replicated in the cloud. Rather than having one or two important servers fail over to the cloud, all of the workloads in a large site can run in the cloud until normal operations are established. While this makes DRaaS more effective for more complicated infrastructures, it passes some of the networking complexities and challenges to the service providers. Some solutions in the market today are designed to remove these networking challenges, eliminating networking complexity from the service provider.

The advantage of DRaaS over a traditional DR site is that organizations don't need to maintain a remote DR facility, with all the expenses associated with maintaining idle server hardware that needs to closely mirror the on-premises environment just in case something terrible happens and the original on-premises site can no longer be used.

Instead with DRaaS, the DR site infrastructure and workloads exist in the cloud only as long as they need to. The moment they are not needed, they can be removed and no longer will incur charges.

Another advantage of DRaaS over a traditional DR site is that as all the protected workload data is already stored in the cloud, restoring the virtual DR site is a far faster operation than recovering a traditional physical DR site would be. All that needs to happen is for the protected data to be moved from one part of the cloud provider's infrastructure to another, instead of having to be transmitted down an Internet connection to the physical DR site.

Conclusion

The cloud offers a variety of advantages over traditional approaches to off-site disaster recovery, including reducing the need to physically move backup media from one location to another and to take advantage of the increasingly cheap and functionally limitless storage capacity and flexibility of the cloud.

As the public cloud providers become better at being able to replicate complex on-premises environments, and as software vendors develop more powerful DRaaS enablement technology, DRaaS becomes a more powerful option for organization than the traditional disaster recovery site.

A cloud-based backup and disaster recovery solution isn't an all or nothing proposition– a hybrid cloud approach is more likely to be found successful. Organizations are likely to still need some level of on-premises protected data storage capacity as well as still needing to transport backup media to secure off-site locations for the purposes of ensuring that compliance responsibilities are met.

The key to successfully implementing a cloud-based backup and disaster recovery solution is finding the right vendor as a partner. A great vendor partner will be able to answer complex questions you may have as well as provide you with a turnkey availability solution that makes disaster recovery in the cloud a process that's far simpler than recovery to a special off-site physical location.

Orin Thomas, MCITP, MCT, MVP is an author, trainer and regular public speaker who has authored more than 30 books for Microsoft Press. He is the convener of the Melbourne System Center, Security and Infrastructure Group His most recent books are on Windows Server 2012 R2 and System Center 2012 R2. Orin is a contributing editor for *Windows IT Pro* where he writes the Hyperbole, Embellishment, and System Administration Blog.

VEEAM
IT JUST WORKS!™

AVAILABILITY
for the Always-On Enterprise™

Over 157,000 companies — **50,000 in the last 12 months** —
ditched their legacy backup software for something fundamentally different...
Availability from Veeam®

Ditch your
BACKUP

Upgrade to
AVAILABILITY

Find out more at **veeam.com/availability**

The DRaaS Opportunity

Fast, Secure Cloud-based DR with Veeam Cloud Connect

VEEAM DRaaS DEFINED

Available in NEW Veeam Availability Suite *v9*

Find out more at **vee.am/cld**