UCG Technologies

IBM i Cloud Backup & DRaaS
VAULT400

From tape to cloud

The journey to efficient backup has reached heightened urgency due to fallout from COVID-19.

React quickly to this “new normal” by re-assessing risks and ensuring that detection, response, and mitigation efforts are aligned accordingly.

UCG Technologies

IBM i Cloud Backup & DRaaS
VAULT400

Businesses must review business continuity plans and develop strategies to account for the new challenges presented by COVID-19

This report highlights the top five reasons why businesses are leaving tape technology and moving to the cloud for data protection.

To the First Responders serving on the front-lines during the COVID-19 pandemic, we extend our heartfelt gratitude.

Changing the conversations about cloud and tape

Anyone who works in IT knows the old arguments:

"Tape is dead!"

"No, tape was dead. Then LTO-9 brought it back!"

"No, tape never died, and never will!"

Every day, more companies are adopting cloud-based data protection strategies—especially in the small and midsize market—for reasons related to costs, staffing and space, and with a new urgency in light of COVID-19 risks. At the same time, tape is seen as a critical component in larger organizations, especially for archival data that is seldom accessed.

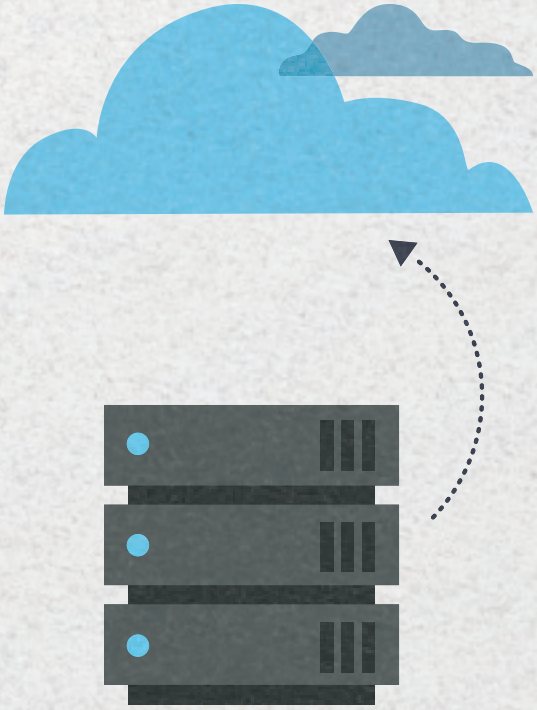
A new ESG report, "Data Protection Cloud Strategies," states the cloud "is and should be part of most IT transformation conversations" —but the report also highlighted the role tape continues to play in data protection strategies. In part, the report reads, "ESG believes that cloud services should be used to supplement data protection for reasons other than wholesale tape displacement." While many organizations will increase agility and BC/DR capabilities through the use of cloud services, those organizations could also be expected to continue to use tape to support retention requirements beyond six years, according to ESG.

Yet we know that many small and midsized companies are looking to eliminate or reduce their reliance on tape, often for economic efficiencies. Many organizations eliminate tape entirely, but others will rely on it for long-term data retention.

There's probably never going to be a better time to ensure your business continuity and DR plans are the best they can be.

UCG Technologies

IBM i Cloud Backup & DRaaS
VAULT400



Five motivations for moving to cloud backup

When talking about the move to cloud backup, there are five motivations IT pros typically focus on:

1. DRaaS

Many cloud service providers are moving from providers of basic backup and storage services to more robust DR as a service (DRaaS) providers, offering emergency application hosting capabilities once delivered by a subscription data center operator or "hot site." If your continuity plan involves replication of your virtual machines at the DRaaS site, it may make sense to have your backup data already at that location, too.

2. Remote offices

Clouds can provide backup services in branch offices or remote offices where you don't have tape technology or the staff to operate it correctly. And remember, simply getting a copy of data outside the walls of your facility is helping to safeguard it against loss or compromise.

3. Selective restore

Cloud-based backup and restore may also be simpler for end users when recovering a single file or dataset that has been deleted or corrupted. A good cloud service will provide a listing of files, objects or datasets to the user, enabling selective on-the-fly restore.

4. No upfront hardware investment

In many cases, there is no upfront investment in hardware, though you may need to beef up your metro or WAN connectivity.

5. Staff resources/training

A good cloud service provider can also insulate you from the need to train your folks in tape operation or to pay maintenance on tape systems over time. The cloud service provider also takes on the responsibility for staying on top of the tape technology refresh cycle, if it uses tape in its own data centers. This insulates you from the time, resource and budget requirements for keeping your tape facilities up to date.

On your way to cloud backup

Moving to cloud backup, however, isn't just a matter of installing some software and pointing it toward a URL. Here are the top five things you should do to get the most out of your cloud backup strategy.

1. Data classification

You would be surprised how many otherwise thoughtful server administrators or end users think of backup as a "one size fits most" undertaking. It is important to make the backup process as simple as possible (so that it actually gets done), but simple, efficient backup processes are the result of careful, upfront planning.

Things to review about your data include:

- How much data do you have and how fast is it growing? These characteristics of your data determine the sizing requirements for both your cloud-based backup repository and the bandwidth that will be required to move data to the cloud efficiently.
- How often does data change? It is key to understand the volatility of your data to determine the frequency with which backups must be taken and the form(s) of the backups (incremental snapshots, full volumes, etc.) themselves.
- Priority of restore. IT pros must consider how quickly data can be restored to you by a cloud backup provider in the wake of an interruption or corruption event. Mission-critical data—data that supports critical "always on" business applications—needs to be prioritized for restore and needs a service that will enable restore at the speed you expect.

2. Investigate DDC

Now you need to determine whether a "DDC approach" is a better one for your environment. DDC stands for "disk to disk to cloud" and it embodies a two-prong strategy for dealing with localized logical and physical disruptions and events with a broader geographical impact.

A DDC strategy envisions backup data first being written to a production storage repository then to a local backup storage repository (flash, disk or tape). The local backup set can be accessed quickly to restore a damaged file or to circumvent a ransomware attack in the production environment. Then data in the local backup repository can be copied into the cloud backup repository. This is a hedge against a facility-wide or regional disaster that compromises both the production repository and the onsite backup.

The COVID-19 pandemic brings the urgency of a of business continuity plan into top-of-mind focus.

3. Software-only or standalone?

Software-only solutions use your network equipment and your production server processing cycles to select, prepare and copy data to the cloud service provider; appliance-based solutions require the implementation of a server/gateway in your LAN to collect data from production servers and storage (or perhaps secondary backup servers and storage) and to handle the communication of that data to the cloud provider. There are good reasons for selecting either option, with software-only solutions tending to be preferred in environments where there is limited connectivity or skill to deploy and manage hardware. However, in heavily virtualized server environments, concerns are often raised about sharing precious workload processing resources with "IO hogs." Try before you buy to see what the impact of backup software is to your environment.

4. Research cloud facility locations

Before finalizing a specific cloud backup strategy, do your homework on the cloud service provider and facilities. With so many managed hosting service providers hanging out shingles describing themselves as online backup experts, you need to be careful that the provider you choose knows the nuances of backup and restore and has facilities, personnel and processes to provide secure 24x7 backup.

5. Factor distance into the equation

If you have a lot of new data to back up each day, you will likely be looking for a service that offers the right amount of band width at the right cost. But distance is also important. Selecting a vendor that offers big bandwidth MPLS network connections at a low cost may seem like the best option, but if that vendor's facility is actually across the street or a few blocks away, it is subject to the same kinds of interruption events as your primary facility (floods, hurricanes, earthquakes, ice storms, etc.). So, you need to know where the cloud service provider's facility is physically located in relation to your location. The time-honored wisdom still applies: Good backups need to be removed offsite and to a safe location "out of harm's way." Just putting them in a cloud isn't sufficient. The physical location of the cloud data center must be considered.

Keeping these in mind will help you to define a workable cloud backup strategy that can be just as effective as traditional strategies for backup and offsite storage.

Request data analysis and proposal for cloud backup & DRaaS at
vault400.com/proposal

UCG Technologies, Inc.
Toronto Airport Corporate Centre
2425 Matheson Boulevard East - 8th Floor
Mississauga, Ontario L4W 5KW Canada

ucgtechnologies.com/cloud

800.211.8798

Mississauga Data Centre
2920 Matheson Boulevard East - Suite #200
Mississauga, O ntario L4W 5J4
Canada