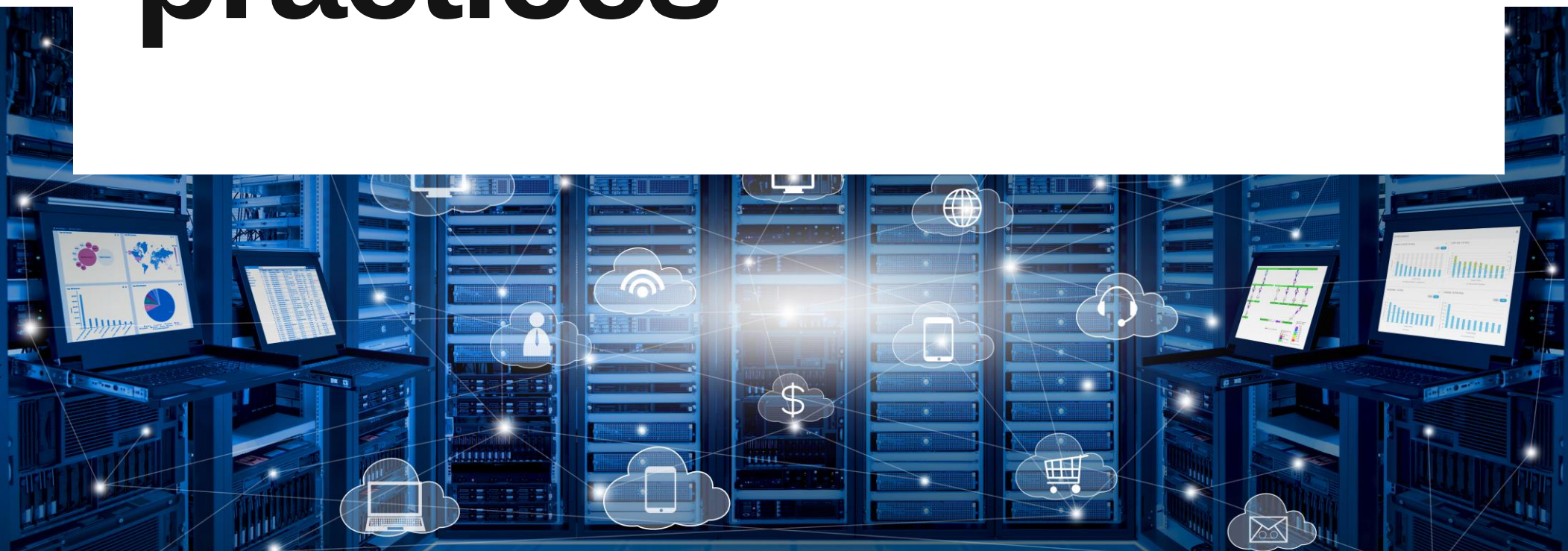


Multi cloud backup and recovery best practices



In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

In this e-guide:

As organisations move more data into multiple clouds, user concerns about data availability and safety continue to grow. In response, data protection vendors are offering products that can help organisations with their multi-cloud backup and recovery strategies.

And despite being in the early phases of the multi-cloud movement, experts have provided some good guidelines to users to help them implement this additional layer of protection.

This guide details multi-cloud backup and recovery best practices, and presents potential pain points.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

How do I know if multi-cloud backup is the right approach?

Paul Kirvan, Independent IT consultant/auditor

We have been taught that putting all of one's eggs into a single basket is risky. The same philosophy is true with cloud-based products.

Despite many vendor claims of high uptime, [multiple outages](#) and disruptions among cloud vendors have occurred, and so relying on a single vendor's platform is not advisable. That's where multi-cloud backup comes in.

Fortunately, there are numerous cloud service providers on the market, offering you a broad range of choices. There are, however, numerous elements to consider before [employing multi-cloud backup](#).

Among the challenges of a multivendor architecture are the following 12 considerations:

- [compatibility across vendors](#), such as failing over a system from one cloud vendor to another;
- security provisions offered by each vendor;
- retention of legacy systems;
- customer service;
- financial offerings and service packages;

In this e-guide

■ How do I know if multi-cloud backup is the right approach?

■ 3-2-1: Get started with a multi-cloud backup plan

■ Multi-cloud data backup: Choices and challenges

■ Does multi-cloud backup have a future, or is it hype?

■ 5 multi-cloud use cases for better storage

■ Consider multi-cloud disaster recovery for added protection

■ 5 crucial multi-cloud disaster recovery principles

- maintenance options;
- vendor willingness to sign [service-level agreements](#);
- ability to test service offerings, especially those relating to data recovery and system recovery;
- compliance with accepted standards for security, networking and storage;
- issues associated with moving systems and data from one vendor to another;
- training on cloud services; and
- experiences and recommendations from other multi-cloud backup customers.

Of this list, the last is one of the most important. Given the number of cloud offerings available, speaking with a vendor's customers is one of the most critical actions you'll take.

Security and testing are also key deciding factors. You'll want peace of mind that your systems and data are not likely to be hacked from the outside -- or the inside. And it's very important that you regularly [test and verify](#) that the data you're backing up can be [accessed quickly](#) in an emergency. The same is true with your systems, such as virtual machines and specialized applications.

Having more than one cloud vendor also gives you the opportunity to have them compete and see which provider offers you the best deals.

Given our initial reminder from childhood and the realities of today's highly diversified world of technology, a multi-cloud backup strategy makes good sense. You may still decide to keep certain assets close at hand due to their

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

sensitive or classified nature, but a [multi-cloud strategy](#) -- if that makes sense for your organization from a business perspective -- can provide peace of mind and long-term support for your organization.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

■ 3-2-1: Get started with a multi-cloud backup plan

Brien Posey, Microsoft MVP

Planning for multi-cloud backup tends to be tricky, because every environment involving multiple clouds is different. As you develop an approach for [protecting a multi-cloud environment](#), you must consider which clouds you are using, what services you are running within each cloud and what your data protection goals are for each the cloud-based resources.

One the most long-standing best practices for on-premises data protection is the [3-2-1 rule](#). That rule essentially states you should have at least three copies your data, on two different types backup media, with at least one backup copy residing off-site. Unfortunately, this rule can't be directly applied to multi-cloud backup -- we'll detail the reason later -- but you can still adhere to the spirit of the rule.

The main idea behind the 3-2-1 rule is you don't ever want to find yourself in a situation in which your backup can potentially become a single point of failure. The requirements for multiple backup copies and [off-site backup](#) storage are meant to guard against the possibility that your one and only backup becomes damaged.

In this e-guide

- How do I know if multi-cloud backup is the right approach?

- 3-2-1: Get started with a multi-cloud backup plan

- Multi-cloud data backup: Choices and challenges

- Does multi-cloud backup have a future, or is it hype?

- 5 multi-cloud use cases for better storage

- Consider multi-cloud disaster recovery for added protection

- 5 crucial multi-cloud disaster recovery principles

In a multi-cloud backup environment, I recommend storing a copy on the same cloud where your primary data resides but also [replicating that backup](#) to the other clouds you use. If a data recovery operation becomes necessary, you would ideally want to restore the data from the backup in the same cloud as where the primary data had been kept. After all, it is going to be much quicker to restore a local cloud backup than to have to transfer backup data across the WAN link that exists between clouds. At the same time, though, having backup copies stored on other clouds can protect you against a [cloud-level disaster](#).

Part of the 3-2-1 rule is the idea that your backup should be stored on at least two different types of media. That part of the rule doesn't really work in a multi-cloud backup environment. What you can do instead, however, is to take advantage of [cloud regions](#). If the bulk of your primary data is stored in a U.S. cloud data center on the West Coast, then you might consider using an East Coast -- or even a European -- data center to store one of your backup copies.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

Multi-cloud data backup: Choices and challenges

Stuart Burns, Virtualization and Linux expert

Many vendors are now touting the latest must-have multi-cloud data backup support.

It is quite simple to have local and globally available resiliency within a cloud of choice. However, the ability to fail over is most often controlled by the cloud provider and is designed for data center-level disaster recovery events, not customer DR events, such as application failure or corrupted disks.

As is often said, [DR is not backup](#). No matter what a business does, it cannot leave the backup to chance with a cloud vendor.

Choices for multi-cloud backup

Ensuring sufficient multi-cloud data backup is more of a business process than a technological one. However, the more complex the environment, the more difficult the job becomes -- before even thinking about which cloud vendor to use. Also, the more cloud providers used, the more complex service-level agreement (SLA) management becomes. Not all SLAs are created equal.

In this e-guide

■ How do I know if multi-cloud backup is the right approach?

■ 3-2-1: Get started with a multi-cloud backup plan

■ Multi-cloud data backup: Choices and challenges

■ Does multi-cloud backup have a future, or is it hype?

■ 5 multi-cloud use cases for better storage

■ Consider multi-cloud disaster recovery for added protection

■ 5 crucial multi-cloud disaster recovery principles

There is no single best provider. What is important is that your potential multi-cloud data protection integrates with not only your current cloud providers but those you may be using in the future.

The field of multi-cloud data backup is frequently changing, but some of the best-in-breed vendors include:

- **Zerto**: Simple to use, ideal for smaller environments;
- **Veeam**: Similar capabilities to Zerto, supports additional cloud providers beyond Microsoft and AWS, has an easy road to quick implementation because of its simplicity; and
- **Veritas**: Ideal for larger companies that want to support more complex setups and a larger group of vendors, coming at a cost of increased complexity and management.

Challenges with multi-cloud backup

Compliance is an issue with multi-cloud data backup. A business cannot and should not just throw a backup into the cheapest cloud available. Some businesses have to prove compliance -- for example with the Health Insurance Portability and Accountability Act and the Sarbanes-Oxley Act. Being a specialized area, it is key to sort out compliance before any data is put anywhere near the cloud vendor of choice.

It should go without saying that any agreement should be in written form and looked over by someone who understands the ramifications, such as someone

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

in legal. Any company that has compliance requirements needs to choose carefully where it puts data.

Be careful about the restrictions in resources that can be consumed. Some backup products, for example, use [S3 to store backups](#) in an inexpensive way, but converting those to executable virtual machines (VMs) is not a quick process. It can take tens of minutes to perform this task because of limitations placed on the speed with which VMs can be imported. There is no way around it. There can be limitations on various cloud providers. Check for such issues before signing up.

Administration can also be a challenging issue. An administrator who uses several different cloud vendors must have knowledge beyond just the backup application and needs to fundamentally understand how to [manage and use the cloud](#) in question.

Choosing the provider, however, is only one part of the issue. With an ever-changing field of applications within your cloud environments, it is all too easy for items to fall through the cracks. If a business has 30 to 40 applications on each cloud environment that will [require active management](#), it is imperative to check that all these systems are backed up.

In the end, do your due diligence, know your requirements and be careful when selecting a multi-cloud data backup vendor.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

Does multi-cloud backup have a future, or is it hype?

Nick Cavallancia, Consultant, Writer

Many organisations see the value of a multivendor platform. It enables taking different approaches to a problem and doesn't put all your eggs in a single vendor's basket.

A number of backup vendors are beginning to tout the support of [multiple cloud vendors](#) as a way to appeal to just about everyone. But is multi-cloud backup necessary or even beneficial?

Let me cover this issue by discussing it from a few perspectives.

Backup

The idea of backing up to both say, AWS *and* Azure, does follow the [3-2-1 backup rule](#); each vendor represents one of the two mediums required, as well as meeting the one copy off-site requirement. The ability to back up to multiple clouds also enables organisations that are operating in a multi-cloud mode to use a single backup vendor.

In this e-guide

- How do I know if multi-cloud backup is the right approach?

- 3-2-1: Get started with a multi-cloud backup plan

- Multi-cloud data backup: Choices and challenges

- Does multi-cloud backup have a future, or is it hype?

- 5 multi-cloud use cases for better storage

- Consider multi-cloud disaster recovery for added protection

- 5 crucial multi-cloud disaster recovery principles

Recovery

There is a benefit for those organisations using a [multi-cloud operational strategy](#) to minimize egress fees on recovery by backing up and recovering within a given public cloud vendor. So, from this perspective, there is a tangible benefit to using multi-cloud backup.

Recoverability

This question should be asked: "Are you better able to recover *because* you use a multi-cloud backup strategy?" The answer for most organisations is *no*. Using a single-cloud strategy will give you just as much benefit, while going multi-cloud possibly overcomplicates both the backup and recovery strategies.

Availability

Even [public cloud vendors have outages](#). Service-level agreements often provide little in the way of compensation, however. So, there can be some benefit to using more than one vendor here. However, given that the likelihood of a public cloud vendor ever going down exactly at the time you need to recover is so small, using multi-cloud backup to offset this potential issue is probably a bit of overkill.

With each of these perspectives in mind, what does the future hold for multi-cloud backup?

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

It feels like a niche play here -- some enterprise and midmarket organisations will require the ability to use multiple clouds as part of their backup and recovery strategy. But, for the vast majority of organisations, that's not a major concern.

While [there's value](#) in multi-cloud backup, I believe its future is going to strictly rely on organizational backup strategy rather than just the mere presence of multiple clouds alone. Time will tell, but for now, multi-cloud backup is an option and not a driver for backup and recovery.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

5 multi-cloud use cases for better storage

John Edwards, Freelancer

Multi-cloud storage is gaining momentum, with a growing number of adopters coming to appreciate the technology's cost, flexibility, adaptability and security attributes.

The number of multi-cloud use cases aimed at storage is expanding rapidly. Take a look at the following five ways organisations can use a [multi-cloud environment](#) to enhance their storage infrastructures.

Data backup and archiving

Among the most common multi-cloud use cases is data backup and archiving. Multi-cloud storage makes [backup and archiving](#) cheaper, easier and more reliable. It enables the replication of data off site, reducing Capex and Opex related to tape storage, expanding retention periods and improving recovery point objectives, noted Robert Illing, enterprise architect for IT transformation at hardware and software reseller SHI International, based in Somerset, N.J.

"Thanks to user-friendly cloud interfaces, moving data across clouds and making multiple copies of data sets in one click results in the reduced investments in development resources," said Andrei Lipnitski, information and

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

communications technology department manager at ScienceSoft, an IT consulting and software development company, based in McKinney, Texas.

Resiliency

Another multi-cloud use case for storage is [risk mitigation](#).

"Having data in different locations, especially in terms of primary and secondary data, means that the customer doesn't have all his eggs in one basket," explained Charles Foley, senior vice president of Talon Storage, a firm specializing in enterprise-class file sharing, based in Mount Laurel, N.J.

Resiliency is a natural benefit of multi-cloud storage, said Geoff Tudor, vice president and general manager of cloud data services at Panzura, a firm specializing in unstructured data management in the cloud, based in Campbell, Calif. Human error is at the heart of many cloud storage outages, he said.

"Spreading data across two cloud storage providers greatly reduces exposure from these types of outages," he added.

A multi-cloud storage strategy is essential to unify data storage for applications running in different clouds, whether they're public or private clouds.

"It allows data to be abstracted away from specific cloud applications and stored in a common shared pool," said Sazzala Reddy, CTO and co-founder of unified

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

hybrid cloud computing and data management company Datrium, based in Sunnyvale, Calif.

A multi-cloud approach can also prevent data fragmentation, reduce data duplication per app and improve data governance, Reddy said. Such benefits can be handy when there's an application running across clouds that needs to access shared data, particularly when the data is sensitive and stored in a private cloud.

"This allows companies to get the best of both public and private cloud offerings, choosing what best fits their needs and being able to adjust as those needs and their data changes," Reddy explained.

Multi-cloud storage also keeps organisations from relying on a single cloud storage provider. Multi-cloud adopters can ensure data resiliency and eliminate application downtime from the failure of an object storage service by having consistent replicas of objects in another cloud or location, said Joel Horwitz, senior vice president of WANdisco, a software company focused on distributed computing, based in San Ramon, Calif.

Compliance

For many enterprises, compliance is becoming an effective multi-cloud use case. Increasingly, data must reside in specific geographic areas to meet data governance and compliance regulations. For some companies, a majority of

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

data may reside with cloud A in one country, while a subset of data that is pertinent to a division or subsidiary in a [GDPR](#)-governed country may be stored with cloud B in another country, Talon Storage's Foley said.

For large or publicly traded companies, the requirement to use risk mitigation best practices will drive the need to take a multi-cloud storage approach.

"For global companies, the need to keep certain data assets in certain geographic domains will factor into the multi-cloud adoption equation," Foley noted.

AI and machine learning

Because each hyperscale cloud provider is developing its own analytical platform, AI and machine learning data must be easily transportable across clouds.

"By having your data portable across multiple clouds, you can take advantage of all of these new tools to extract value from your data," Panzura's Tudor said.

Software development

DevOps and [continuous integration and continuous delivery](#) are among the most powerful multi-cloud use cases for storage. This approach allows the most important components of an application -- the data it produces and consumes -- to travel between environments based on the needs of the developers and end

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

users, said Irshad Raihan, a director of product marketing on Red Hat's storage team.

"When multi-cloud storage is driven by policies that assign data to specific locations, it enables more automation and scalability, ultimately enabling more efficient development," he said.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

■ Consider multi-cloud disaster recovery for added protection

Brien Posey, Microsoft MVP

When it comes to cloud-based disaster recovery, one of the most important things to remember is that there is no such thing as 100% reliability. Cloud service providers spend huge amounts of money to implement redundancy on every level of their infrastructure, yet we still hear about cloud outages. The best cloud-based option is a multi-cloud disaster recovery strategy.

Major public clouds tend to be just as reliable -- perhaps more so -- as any on-premises infrastructure, but [using multiple clouds](#) is one way to ensure a higher level of protection.

This option can be a little bit tougher to implement, because each cloud provider [has different standards](#) for its virtual machines. Even so, a multi-cloud disaster recovery strategy provides another layer of security.

A major problem with [disaster recovery planning](#) is that you never know exactly what a disaster might entail or how widespread the effects of the disaster might be. Under "normal" conditions, the chances of a cloud provider experiencing a major outage at the same time that your organization is dealing with a disaster

In this e-guide

■ How do I know if multi-cloud backup is the right approach?

■ 3-2-1: Get started with a multi-cloud backup plan

■ Multi-cloud data backup: Choices and challenges

■ Does multi-cloud backup have a future, or is it hype?

■ 5 multi-cloud use cases for better storage

■ Consider multi-cloud disaster recovery for added protection

■ 5 crucial multi-cloud disaster recovery principles

are near zero. However, a large-scale disaster could conceivably impact both your organization and the cloud that you use for disaster recovery. A major storm for example, can span many hundreds of miles, and if a [cloud provider's data center](#) is in close enough proximity to your own, then you might both be impacted by the same storm.

If you opt to use a single cloud, don't keep all of your resources in the same region. It's fine to replicate mission-critical resources to the cloud region that is geographically closest to you, but, ideally, you should be using multi-cloud disaster recovery to replicate your resources to a second cloud region further away.

Why bother with [multiple clouds](#) if you can already replicate to multiple regions with just one? With one cloud, the data centers are all part of that same cloud. If the cloud provider were to experience some sort of global failure, then all of its regions could conceivably be impacted. On the other hand, there is almost no chance that two different cloud providers will both experience a catastrophic [global outage](#) at the same time.

If you opt to use a multi-cloud disaster recovery strategy as part of your [cloud-based DR plan](#), then you should try to avoid overlapping regions. If, for example, you use one provider's east coast United States region, then you should use a different region with your other cloud provider. That way, a regional disaster can't take down both of your clouds at the same time.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

5 crucial multi-cloud disaster recovery principles

John Edwards, Freelancer

When a cloud provider's services suddenly become unavailable, the business impact can be serious and even traumatic. In addition to lost productivity, employees, customers and business partners may become frustrated and angry if order is not restored quickly. The longer the outage continues, the greater the likelihood that your organization will experience a significant loss revenue, not to mention major and perhaps even long-term damage to its reputation.

By creating a reliable multi-cloud disaster recovery (DR), these issues can be more easily avoided. A well-designed strategy will help you maintain essential business operations, even if your usually reliable cloud partner experiences a hiccup. As you begin mapping out your [multi-cloud strategy](#), consider these five key points.

1. Location, location, location

If your cloud provider stores your applications and data in a single location, it's time to look for a partner that can supply a wider and more [flexible multi-cloud](#)

In this e-guide

■ How do I know if multi-cloud backup is the right approach?

■ 3-2-1: Get started with a multi-cloud backup plan

■ Multi-cloud data backup: Choices and challenges

■ Does multi-cloud backup have a future, or is it hype?

■ 5 multi-cloud use cases for better storage

■ Consider multi-cloud disaster recovery for added protection

■ 5 crucial multi-cloud disaster recovery principles

[footprint](#). Adopting a multi-cloud disaster recovery approach will make your assets more accessible and better protected from accidental deletion.

The safest strategy is to use multiple clouds within the same country but located in different geographic regions. Moving data across international boundaries isn't usually a good idea, since it creates unnecessary legal and regulatory constraints and complications.

2. Safety in numbers

For maximum protection, include at least [two different cloud providers](#) in your multi-cloud disaster recovery strategy. Many providers operate separate regional cloud infrastructures, but if one infrastructure fails, the firm's other infrastructures may become overloaded to the extent that they become unusable.

On the other hand, the odds two providers faltering simultaneously, even if they are based in the same country, are relatively infinitesimal.

3. Test your initiative

As with any new initiative, it's wise to begin a multi-cloud disaster recovery with a small, limited-scope [test project](#). Many organisations launch their strategy by replicating a select number data sets in a nonessential area, using two or more cloud providers.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

The next step would be to analyze the results and, if the outcome warrants it, move on to progressively more critical assets.

4. Use the right tools

With the right tools in hand, replication [across multiple cloud providers](#) can be just as easy as having cross-region capabilities. Services such as [CloudEndure](#) can help you automate the process. And DR and live migration products, like [CloudEndure](#) and [UnitedLayer](#), can replicate workloads to different clouds and automate multi-cloud migrations.

5. Conduct regular drills

Cloud technologies and provider requirements are continually evolving, so a best practice is to regularly run drills of your multi-cloud disaster recovery to ensure smooth and rapid failovers. This enables you to learn how every function will perform in the event a disaster.

While testing typically targets and analyzes separate components a , a drill runs through the strategy from start to finish. Similar to a [tabletop exercise](#), DR drills more closely simulate how a will be used following a disaster. If the results aren't satisfactory, work with your cloud provider(s) to iron out any problems.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

How to overcome multi-cloud disaster recovery challenges

George Lawton, Contributor

As enterprises continue to spread their data across cloud platforms, backup and disaster recovery grows increasingly complex. CIOs must find a way to balance the cost savings they enjoy from the cloud tech with adequate protection from growing threats like malicious hackers and unintended deletions.

A growing ecosystem multi-cloud disaster recovery services are emerging to help, but it's important to evaluate these through the lens [specific enterprise goals](#).

"Multi-cloud is the latest cloud-related buzzword," said David G. Hill, principal and founder Mesabi Group, an IT analyst firm. "It implies that an on-premises private cloud interfaces with one or more off premises clouds provided by third-party vendors."

The step in cutting through the hype is concentrating on the type service that you want, such as disaster recovery, or [DRaaS](#), when making the decision, Hill said.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

But because there are so many different kinds [multi-cloud scenarios](#) to consider, it is vital to test recovery processes to make sure the service works when it counts. It's also important to assess latent cloud disaster recovery limitations: Hill and others said to be prepared to adopt or develop new [disaster recovery tools](#) as the technology and services improve.

Different DR use cases

There are a few ways customers interpret backup and [disaster recovery for the multi-cloud world](#), explained Naveen Chhabra, principal analyst at Forrester.

- Backing up the cloud service from the cloud source itself.
- Backing up the traditional on-prem infrastructure.

Tools for backing up on prem data are more mature than for backing up SaaS apps, however, creating a tough gap to fill.

Another big problem is that few vendors deliver a solution with a strong policy-based engine, particularly for cloud apps. This means more [work for backup admins](#) as the environment grows. This has fueled the growth new vendors like Rubrik, Cohesity and Reduxio that are challenging incumbents with better tools for backing up from cloud apps with some policy and governance capabilities. These are more advanced than traditional disaster recovery apps for on-premise apps.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

Prepare for different scenarios

The cloud makes several processes easier: It's easier to move data and connect it to apps. It also makes it easier for rogue employees or hackers to do bad things -- including deleting data. The trick is to bring the same level of protection as traditional on-prem disaster recovery to the cloud. For example, the [ticket service Live Nation](#) implemented a multi-cloud disaster recovery solution to help back up 120 applications it recently moved to the cloud.

Jake Burns, vice president cloud services at Live Nation, looked at using native cloud backup services like AWS Glacier that would have worked well for physical protection but would have left the data exposed to hackers or rogue employees with AWS credentials.

"They could delete the production and backups as well," said Burns. "You don't want all your eggs in one basket."

Burns advocates against keeping the primary and backup data in the same account to prevent the same credentials or individuals from having access to both. A multi-cloud disaster recovery [strategy creates a stronger firewall](#) between the primary data and backup, but costs more than doing everything on one cloud platform.

"You can get 95% the benefit with far less complexity using just one cloud provider," Burns said, but added that the peace of mind that comes with the [multi-](#)

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

[cloud environment](#) was worth it. Every CIO has to weigh the tradeoffs between a slightly higher level of reliability and the additional costs for running across multiple clouds.

Test recovery scenarios

The real test of any disaster recovery service lies in ensuring that it is easy to roll backups into enterprise production. Although the testing process can be difficult and time consuming, it is better to incur an outage during a maintenance window rather than as a surprise after it has failed.

"Everyone implements backup, but few test it," Burns said.

There are two strategies for doing this: Full recovery from a backup, or maintaining a second running system which can be rolled over to when required. The latter approach makes it easier to do [QA and testing](#) on this copy and, if successful, to promote it to a primary application.

"If you have the DR system in place, you can count on it because you are periodically switching between them," said Burns.

This same strategy can also be used for cost optimization to take advantage of price fluctuations between different regions. In theory, this would also make it possible to [migrate across cloud platforms](#), but this would also increase operational complexity.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

Focus on trust and simplicity

Finding a vendor or vendors with whom you are comfortable with and have great confidence in is critical, Mesabi's Hill said. This means developing an ongoing and evolving [checklist requirements](#) and using it to compare multiple vendors.

"But you must be careful because vendors are good at getting checkmarks," he cautioned.

Going forward, [analytics-driven policies](#) could become a major differentiator between [disaster recovery providers](#), Chhabra said. Enterprises could develop these policies based on data allocation, sensitivity and recovery point objectives.

"This is a clear application analytics for the backup space, unfortunately, none the vendors are delivering such insights," Chhabra said.

In this e-guide

- How do I know if multi-cloud backup is the right approach?
- 3-2-1: Get started with a multi-cloud backup plan
- Multi-cloud data backup: Choices and challenges
- Does multi-cloud backup have a future, or is it hype?
- 5 multi-cloud use cases for better storage
- Consider multi-cloud disaster recovery for added protection
- 5 crucial multi-cloud disaster recovery principles

■ Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting
www.computerweekly.com/eproducts

Images; stock.adobe.com

© 2019 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.