Affordable Enterprise-Grade Disaster Recovery Using AWS

aws

CloudEndure
An AWS Company

Introduction

Until recently, enterprise-grade disaster recovery had been prohibitively expensive for most organizations. Thanks to the rapid development of cloud infrastructure, organizations can now attain top-of-the-line disaster recovery capabilities into AWS at a fraction of the cost.

The Challenge

An enterprise-grade disaster recovery (DR) solution is no longer something that is "nice to have." Nor can it be a document approved by the Board of Directors but hasn't been touched or tested in years. Why not? In addition to the probability of damaging your hard-earned reputation, downtime also comes with major costs. Gartner estimates the average cost of IT downtime at $5,600 per minute, which can add up quickly.

If your organization is like other large-scale businesses today, you understand the critical need to recover rapidly from IT outages, application failures, or malicious attacks in order to ensure business resilience, stay competitive, and avoid regulatory penalties. Not only do your employees need to access company systems 24/7, but your global customers also expect constant availability.

So what's the problem? Why don't all enterprises have airtight, 100% reliable, and frequently tested disaster recovery strategies in place? Can't IT departments just set up multiple data centers that continually replicate workloads, and when a disaster strikes, redirect to the DR site?

It turns out that for many organizations, traditional enterprise-grade DR solutions – with near-zero Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) – are prohibitively expensive due to heavy capital expenditures (CapEx) and/or costly duplicate third-party software and services.

As a result, some organizations choose to take the risk of having only a backup system, which enables data retrieval, but does not prevent costly downtime because of its long data recovery times. Other companies choose to protect only the most essential servers, which leaves their business vulnerable. Many companies that do lay out a substantial initial investment in DR later dedicate resources to other pressing IT needs. But "set it and forget it" doesn't work for DR — a system that quickly becomes obsolete if not tested frequently.

The solution to this challenge lies in the cloud. Today, **businesses can attain top-of-the-line IT resilience at a fraction of the cost** by moving their DR to the cloud.

In this white paper, we examine the three main DR strategies that are currently used by enterprises **— On-Premises Disaster Recovery, Disaster Recovery as a Service (DRaaS), and Cloud-Based Disaster Recovery –** with a focus on the expected costs of each strategy. We will also touch upon the benefits and risks of each strategy, to help your organization decide if leveraging the cloud, and specifically AWS, for DR is the right approach for your business.

On-Premises Disaster Recovery

Enterprises have traditionally handled IT disaster recovery internally. Keeping a robust on-premises DR solution in place and up-to-date requires a large investment of resources.

Hardware: Most on-premises DR solutions depend on the purchase of duplicate servers on-site or at a secondary location to be used in the event of an outage. These servers incur both CapEx and ongoing IT operating expenses (including power and cooling). Moreover, they typically require a hardware refresh every three to five years.

Software Licenses: In order to launch recovery machines when source machines fail, on-premises DR solutions commonly require maintaining duplicate third-party software licenses and, in some cases, application- or DR-specific replication software. This can lead to high expenditures, especially for enterprises that use costly applications from vendors such as Oracle, SAP, and Microsoft.

DR Infrastructure & Services: Any IT resilience solution must be able to restore entire systems to their pre-disaster state. On-premises DR solutions require the purchase of data protection software and, in certain cases, replication appliances. If the organization needs enterprise-grade RTOs and RPOs, they have to pay for duplicate compute and storage infrastructure at their DR site.

Management & Monitoring: IT staff resources are necessary to continually manage and monitor the DR hardware, software, and infrastructure.

Disaster Recovery as a Service

In light of the high costs and expertise needed to implement on-premises DR, many organizations turn to third-party Disaster Recovery as a Service (DRaaS) providers to administer failover support in the event of a disaster. The quality of this kind of DR solution depends on the particular DRaaS provider's technology, processes, and service-level agreements (SLAs).

Hardware: When using DRaaS, organizations do not need to purchase duplicate servers or maintain a duplicate data center on their own. Rather, their duplicate servers are located in data centers or colocation centers run by their DRaaS provider.

Software Licenses: Depending on the applications protected and replication methods used, organizations may still need to purchase duplicate licenses for their applications if they want them to be available quickly during a disaster.

DR Infrastructure & Services: Given the underprovisioning of hardware based on an assumption that not all customers will require failover at the same time, DRaaS providers are able to offer lower costs for standby machines as compared with an on-premises DR implementation. Nonetheless, a DRaaS provider's ability to underprovision servers effectively is negligible compared to the economy of scale provided by the cloud, and is therefore a more costly option. In addition, there may also be added costs associated with third-party application licenses, depending on the replication method used.

Management & Monitoring: Organizations rely on their DRaaS provider to handle most of the management and monitoring of their DR site. While they do not have to pay for additional IT staff, they do have to pay their DRaaS provider. Such costs differ among the various vendors.

Cloud-Based Disaster Recovery

A revolution in disaster recovery came with the advancement of cloud technology and the enormous growth of public cloud infrastructure, which allows you to pay only for the resources you use. In parallel, replication technologies evolved to leverage cloud infrastructure cost-effectively, forming a "perfect marriage" between DR and the cloud.

As a result, organizations can now achieve enterprise-grade DR at a dramatically lower cost than was previously possible. There are numerous cloud-based DR technology solution vendors. Top-of-the-line solutions provide enterprise-grade recovery objectives, and agnostic protection for any application, workload, or database, without any impact on your source servers. When evaluating a DR solution, make sure to ask the right questions about the software capabilities and limitations, based on your environment details and recovery objectives.

Hardware: When using AWS as target DR infrastructure, no hardware is needed, and you only pay for your cloud DR site when required, such as during a disaster or DR drill. This means no CapEx investment or unnecessary duplicate provisioning of resources.

Software Licenses: One of the easily overlooked but significant cost savings factors when using AWS as target infrastructure and an appropriate replication tool for DR is eliminating the need to purchase duplicate software licenses for your standby DR site. The reason for this is that when an appropriate replication technology is used, there's no longer a need to maintain a duplicate standby system with standby licenses (of an Oracle DB, for example).

Instead, the DR solution keeps servers continuously in sync in your preferred AWS region, without running any licensed OS or application. In the event of a disaster or a DR test, you can launch your servers within minutes, and only then require the third-party OS and application licenses. In other words, you get the resilience of a highly available system with near-zero RPOs and RTOs, at the cost of a cold standby solution.

DR Infrastructure & Services: Whereas traditional enterprise-grade DR solutions require duplicate compute and storage infrastructure provisioned in the DR site, cloud-based DR solutions allow you to pay for fully provisioned workloads only in the event of an actual disaster, thereby dramatically cutting DR infrastructure costs.

Management & Monitoring: Cloud-based DR solutions leverage the elasticity of the cloud and provide much better DR automation than traditional solutions, which means fewer IT resources are required to launch or maintain the service. Automated machine conversion technologies ensure that the heavy lifting typically involved in converting machines from one infrastructure to another is rapid and simplified. As a result, machines can boot natively into AWS, even if they originated from a dissimilar infrastructure.

Lastly, a DR solution that offers automated orchestration of the application stacks, which can be performed in advance during the implementation stage, can eliminate the need for time-consuming, manual network configurations during a disaster.

Additional Benefits of Disaster Recovery Into AWS

While cloud-based disaster recovery into AWS is clearly the least expensive approach, you may be wondering whether this "cheaper" option is as effective and enterprise-grade as an on-premises or DRaaS solution. The answer is yes. Not only does cloud-based DR technology provide top-of-the-line DR, but it provides capabilities not available with other DR strategies, including:

- **Easy Testability** — Quickly spin up machines for your periodic DR drills without disrupting your source environment.
- **Self-Service DR** — Configure your AWS environment, replicate your servers, and perform DR drills whenever you want. Deployment is easy, and access to cloud resources is instantaneous.
- **Flexibility Between Infrastructures** — Protect physical, virtual, or cloud-based source machines by replicating them into a DR site in any AWS Region.

FAQs About Cloud-Based Disaster Recovery Into AWS

For some enterprises, moving DR to the public cloud may seem like a radical move. However, in recent years, more and more enterprises, government entities, hospitals, and flagship academic institutions have done so. AWS and other leading public clouds offer enterprise-grade security, compliance, and data integrity. As such, many organizations have declared cloud-first initiatives to outsource infrastructure to the public cloud wherever possible, with DR being one of the first candidates.

The technology you choose for your cloud-based DR solution can vary greatly from one vendor to another. Some DR solutions cannot guarantee consistency or support all of your applications, which would impact your implementation success rate. Other technologies may impact your server performance or deliver inadequate RPOs or RTOs. The right technology, however, will enable you to achieve the enterprise-grade resilience and performance of on-premises and DRaaS solutions, with the dramatic cost reduction of leveraging the cloud for DR.

Below, we address some of the concerns you may have specific to cloud-based DR into AWS, as well as questions to consider when evaluating the right DR solution for your enterprise.

What RPO can I achieve when using AWS to protect my workloads? How much data loss might I experience during a disaster?

When using continuous block-level replication DR technologies, you should expect near-zero RPO (normally seconds or less), depending on the latency and network quality between your source servers and target AWS region.

What RTO can I achieve when using AWS as target infrastructure? How long will it take me to failover into AWS during a disaster?

Two key capabilities that enable quick recovery into AWS are: 1) automated machine conversion of your source servers into AWS instances, and 2) automated large-scale DR orchestration. Cloud-based DR technologies that include these two capabilities deliver recovery times of minutes and can launch all of your target machines in parallel, on a mass scale.

Can AWS support my physical and virtual machines? What about legacy applications?

A cloud-based DR solution must perform replication at the OS level (rather than hypervisor or SAN level) in order to support recovery of any type of infrastructure into AWS, including physical, any type of virtual hypervisor, cloud-based, and colocated servers. When the replication is conducted at the block level, any file system or application is transparently supported. Common workloads include the suite of databases and applications from vendors such as Oracle, SAP, and Microsoft.

Features & Benefits of 3 Disaster Recovery Strategies

	On-Premises	DRaaS	Cloud-Based
Enterprise-Grade	✓	✓	✓
Total Cost of Ownership	High	Medium	Low
Automated Deployment & Maintenance	✗	✓	✓
Easy Testability	✗	✗	✓
Easy Scalability	✗	✓	✓
Self-Service DR	✗	✗	✓
Flexibility Between Infrastructures	✗	✗	✓
Software-Defined DR Site	✗	✗	✓

Is it possible to use AWS for disaster recovery without moving my primary workloads to AWS?
Absolutely. When you use AWS as DR target infrastructure, you simply have a dormant copy of your workloads as AWS instances, which can then be fully launched whenever you choose to do so. You can continue to use any infrastructure you choose for your production environment, as long as your DR solution performs block-level replication.

Isn't putting my DR in the cloud a security risk?
As long as your DR solution uses proper data-at-rest and data-in-transit encryption, your data is secure. If desired, request that your DR solution allow you to be in control of the data path for the replication traffic over your private networks. Ask AWS about any specific questions you might have about meeting the regulatory compliance requirements applicable to your business.

Won't setting up DR in AWS disrupt my source system?
This entirely depends on the DR solution. Some cloud-based DR solutions require rebooting your system, or taking frequent snapshots, and may impact system performance or require local storage at the expense of your primary applications; others are designed to be non-intrusive.

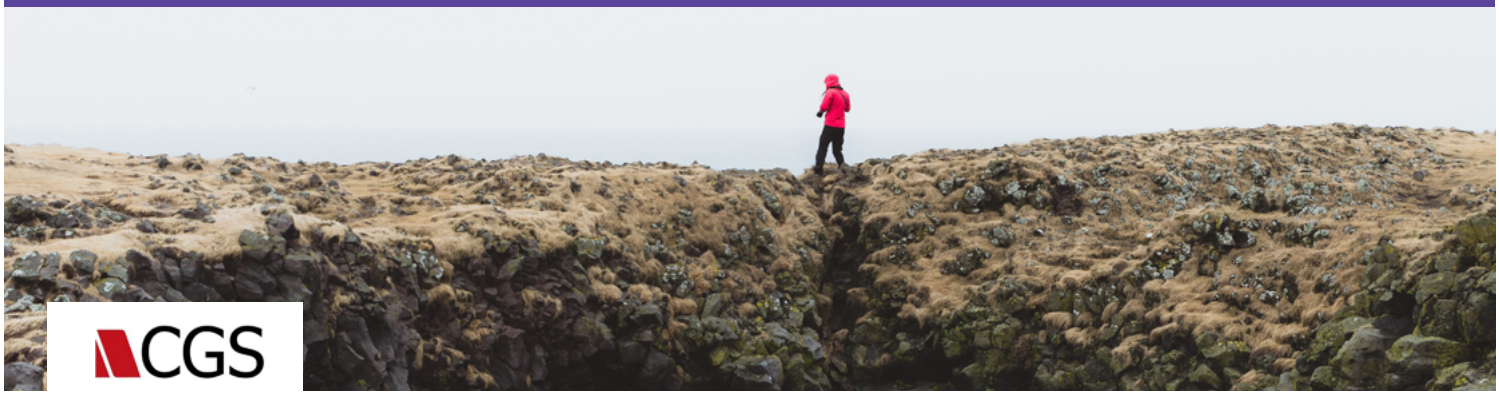
How can I conduct DR drills with a cloud-based DR solution?
DR drills are much easier when using the cloud as a target. On-premises and DRaaS DR strategies require you to ensure that the resources needed for the drill are provisioned and paid for in advance, and in some cases require disrupting source applications to avoid network conflicts.

However, when using AWS as a DR target, you can simply request the resources when needed, and only pay for them upon use. Furthermore, you can spin up your target AWS machines in complete isolation, thereby performing DR drills without any impact or conflict with your source applications.

If I run my DR servers in AWS, how time-consuming and costly will the failback into my primary infrastructure be, once the disaster is over?
With some solutions, this can be a cumbersome manual process of setting up your source servers and applications from scratch, moving the data, and then keeping it in sync until the point of failback. Other solutions allow you to simply reverse the replication directly and keep the data in real-time sync back to your primary site within minutes, once the disaster is over and you're ready for failback.

What if my servers experience a virus, hacker, or ransomware attack that compromises my data, or a database corruption that requires me to recover to a previous point in time. Is point-in-time recovery possible?
Yes. With the appropriate cloud-based DR solution, you can recover back to previous consistent points in time.

Success Story: AWS Disaster Recovery



"We're moving forward with replication on a client-by-client basis. As we phase out clients, we decommission their replicas in the secondary facility. When we've replicated all of the clients in AWS with CloudEndure, we can start to decommission the facility and realize the cost savings we are looking for."

Michael Brandi
Vice President of the Technology Solutions Division at CGS

The Challenge

As their business scaled up, CGS had to keep buying duplicate hardware, software, and connectivity resources for their secondary data center – all of which might never actually be used. Given that they needed duplicate resources for hundreds of mission-critical servers, this became a very expensive project.

Solution Testing

CGS tested their enterprise resource planning (ERP) environment, which included large, write-intensive databases and applications based on Microsoft platforms such as .NET, SQL Server, and IIS. They used CloudEndure Disaster Recovery to replicate their environment to AWS, and tested networking, failover, and automation. CGS saw that they would be able to decommission their secondary data center and realize immediate disaster recovery cost savings of 50% or more by leveraging the scalability of AWS. In addition, they would achieve enterprise-grade business continuity through CloudEndure's automated cloud orchestration and machine conversion, continuous data replication, and automated failback.

Result

Launching CloudEndure Disaster Recovery into AWS means that CGS has an on-demand disaster recovery solution that eliminates the need for duplicate resources. In addition to annual cost savings, CGS and their customers also benefit from sub-second RPOs for all workloads, including complex ERP applications, and a significant reduction in recovery time, with no performance impact.

Business as Usual. Always.

CloudEndure, an AWS company, accelerates the journey to the AWS cloud with solutions that provide business continuity during the migration process and additional protection once there. Enterprises use CloudEndure to replicate their most critical databases, including Microsoft SQL Server, Oracle, and MySQL, as well as enterprise applications such as SAP. CloudEndure Migration simplifies, expedites, and automates large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS. CloudEndure Disaster Recovery protects against downtime and data loss from any threat, including ransomware and server corruption. With CloudEndure it's business as usual, always.

For more information about CloudEndure's Disaster Recovery and Migration solutions:
www.cloudendure.com | cloudendure-info@amazon.com

CONTACT US