

SaaS-based DR can help organizations by lowering administrative overhead on upkeeping DR software and providing a global management plane to simplify the deployment, operation, and cadence of testing disaster recovery strategies.

Global Management with SaaS-Based Disaster Recovery

May 2023

Written by: Johnny Yu, Research Manager, Storage and Computing

Introduction

When planning and implementing disaster recovery (DR), many organizations will focus on how quickly and accurately the DR software can bring applications and data back online. However, it's also important to account for the management aspect of the entire DR system, especially for enterprises with a global presence. The backbone of a good DR system is a solid management system to keep everything on track, but this is difficult to do on a large scale.

The Importance of a Global View

Organizations can have applications running in a wide variety of environments, from on-premises to cloud to containers, and the DR method for each can be equally varied. To manage DR implementations at such complexity, organizations need tools that can monitor and visualize the entire DR estate.

A global view of DR deployments helps organizations be proactive by surfacing potential points of failure before a disaster scenario occurs. Administrators can now gain important information such as the health of the failover site's hardware if it's on premises or network connectivity if it's cloud based. A global management console could also tell when particular DR deployments were last tested, schedule those tests on a regular basis, and report the test results.

DR testing is one of the most important methods of ensuring recoverability in a disaster scenario. The larger and more complex an organization's infrastructure is, the harder it becomes to stay on top of DR testing. A global view of all DR deployments would address this issue. A DR system is only as good as its last test, so proper DR management will invariably involve managing DR testing.

A Matter of Control

Every DR deployment model is a balance of control over the storage environment and cost overhead, which includes both monetary cost and administrative bandwidth cost. Understanding the trade-offs is how organizations determine the right deployment model for their workloads.

AT A GLANCE

KEY TAKEAWAYS

- » Managing DR deployments at scale is challenging — infrequent or inconsistent DR testing is a symptom of a larger problem.
- » All DR models come with administrative overhead. The more that can be minimized, the more admins can focus on DR management.
- » SaaS-based DR offers many of the benefits of DRaaS by simplifying DR management and operations.

Traditional site-to-site failover is one end of the spectrum, where an organization has full control over the secondary environment, including how and where data and applications are stored, as well as what DR software is used. The drawback is the administrators are fully responsible for the upkeep of the secondary environment, which includes power and cooling as well as keeping up with hardware refreshes.

The other end of the spectrum is disaster recovery as a service (DRaaS), where the overhead cost is simply paying a subscription, and the management is handled by the service provider. However, with DRaaS, control over the DR system is entirely in the service provider's hands, so it is often not possible for DRaaS providers to cater to every specific storage accommodation such as where the data is stored or what media it must be stored on.

Somewhere between those models are cloud-based and hybrid DR, where the failover site is fully or partially in a public cloud. This method lowers the cost overhead of standing up a second physical datacenter, as the elasticity of the cloud allows organizations to only pay for storage and compute when they use it. This method requires a reliable internet connection, and it means relinquishing some control over the storage as it is restricted to whatever the cloud provider can provide, but administrators still have the choice of the DR software they wish to deploy.

Finally, there is SaaS-based DR, where the DR software itself is served over an internet connection. This model can be described as one step away from full-blown DRaaS. The administrators are still self-servicing their own DR, but this allows them to retain more control over how DR is carried out. With this approach, minimal administrative bandwidth is spent on maintaining the DR software, allowing organizations to focus on DR management.

Benefits of SaaS-Based DR

SaaS-based DR is the best DR model for organizations looking to minimize the physical and management overhead of DR infrastructure without relinquishing as much control as with pure DRaaS. This is especially the case for large enterprises with global, complex DR deployments. The global view from a SaaS-based management console helps mitigate that complexity, and depending on the SaaS provider, it can offer other DR management capabilities as well.

Other benefits of SaaS-based DR include:

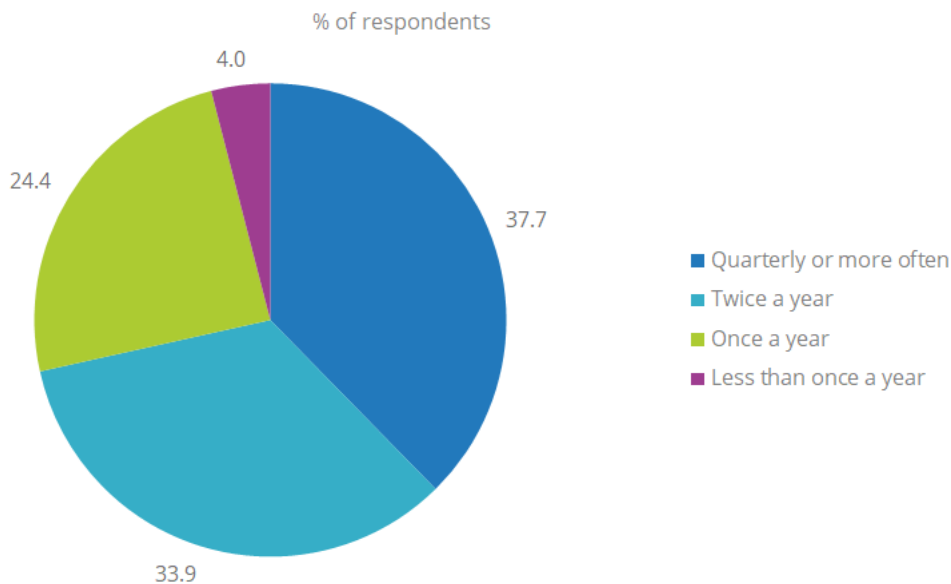
- » **Automated updates and patches:** As with any SaaS product, SaaS-based DR software pushes out updates and patches automatically without any work from administrators. This saves organizations from doing this themselves, which would involve scheduling downtime, testing the updates, planning a rolling deployment, and other often tedious tasks associated with software updates.
- » **Lower cost of entry:** Another benefit common to all SaaS products, SaaS-based DR has a lower up-front cost than traditional software deployments, where organizations must determine licensing costs and how many licenses they need to buy as well as have hardware or a cloud target to install it on. SaaS products not only follow a simple subscription-based pricing model but tend to deploy faster.
- » **An extra layer of security:** Since SaaS-based DR isn't hosted in the organization's datacenter, it's harder for malicious actors to compromise it. An attacker that has infiltrated an organization's systems won't easily be able to touch the DR control plane because it is completely out of band.
- » **Market opportunity for managed service providers (SPs):** SaaS-based DR provides managed SPs with a platform on which to sell DRaaS. In this use case, the SaaS' global view isn't used to monitor one organization's DR deployments but to monitor the deployments of the managed SPs clients instead. This allows managed SPs to add DRaaS to their services portfolio without investing as much into DR infrastructure.

Trends

Testing is an important aspect of DR, as it reveals any shortcomings of the recovery process and allows organizations to address issues before a real disaster event occurs. However, recent IDC survey data found only about 38% of organizations test their DR quarterly or more often (see Figure 1). Ideally, DR testing is done regularly and nondisruptively, and ad hoc tests should be run every time a major application is upgraded or introduced.

FIGURE 1: **Most Organizations Don't Test DR More than Twice a Year**

Q How often do you run a disaster recovery test?



n = 818

Base = respondents who indicated they often run a disaster recovery test

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *The State of Cyber Resilience Survey*, February 2023

Untested DR will inevitably lead to slower recoveries and an inability to meet service-level agreements (SLAs). The cost of this extra downtime can add up significantly. An IDC research study found the cost of downtime averages about \$250,000 per hour (across all industries and organizational sizes). With such severe costs, businesses will increasingly find any amount of avoidable downtime to be unacceptable.

Between containers and hybrid cloud adoption, organizations' infrastructure is getting more complex. DR and DR plans need to keep up with this evolution, but companies are finding this challenging. SaaS-based DR can help address this by lowering administrative overhead on upkeeping the DR software and providing a global management plane to keep organizations on a DR testing cadence.

Considering HPE GreenLake for Disaster Recovery — a DR Command Center

HPE GreenLake for Disaster Recovery combines HPE's GreenLake hybrid cloud platform with Zerto's continuous data protection to deliver SaaS-based DR. HPE GreenLake allows organizations to unify data everywhere from edge to cloud onto a "single source of truth," providing functions such as analytics, data protection, and security to this nexus of data. HPE GreenLake for Disaster Recovery is the DR cloud service of the overall GreenLake platform.

HPE GreenLake for Disaster Recovery is built with Zerto technology, a DR software vendor Hewlett Packard Enterprise (HPE) acquired in 2021, and exhibits many of Zerto's core capabilities. This includes its patented journaling technology that captures restore points down to the second, allowing organizations to achieve very low recovery point objectives (RPOs). Other inherited Zerto capabilities include orchestrated recovery, automatic recovery for apps using predefined plans, new VM detection and policy assignment, automatic failover testing, and nondisruptive testing.

HPE GreenLake for Disaster Recovery serves as the management plane for all DR deployments. The management dashboard provides real-time monitoring and reporting on DR deployments, informing users of SLA status and current RPOs. The console allows customers to provision and deploy DR sites quickly and easily, and unlike with traditional site-to-site failover, HPE GreenLake for Disaster Recovery doesn't require like-for-like failover environments. So long as the secondary environment is running VMware, it can be used as a DR site.

HPE GreenLake for Disaster Recovery tackles the issue of administrative overhead through a single globally available console. When organizations are using separate and disparate tools for DR or letting individual business units implement DR any way that they want, they're increasing infrastructure complexity. The HPE GreenLake cloud platform reduces that complexity by standardizing customers to a single DR management console with a global view.

Challenges

Automation and other ways of streamlining the DR workflow are difficult for most organizations operating at the enterprise scale. HPE GreenLake for Disaster Recovery has built in automation and orchestration to resolve those issues. Other solution features that help improve the information-to-action flow could include a means of calculating a resilience score and then suggesting ways to improve the scores based on what the console data is showing.

The main potential drawback of HPE GreenLake for Disaster Recovery, as with any SaaS platform, is the commitment to that software platform across the entire enterprise. However, consolidating to one DR software solution isn't as simple as it is for customer record management (CRM) or company email. Individual business units within a large enterprise may use and prefer different DR tools, and in some cases, they may have deployed them without going through proper IT channels. HPE GreenLake for Disaster Recovery calls for a level of standardization that some companies may not be internally prepared for.

Finally, like all data protection vendors, HPE GreenLake for Disaster Recovery will soon need features to specifically address the cyber-recovery use case. Virtually every vendor in this market is working on or improving features such as ransomware and anomaly detection, the ability to easily set up isolated recovery environments, and integrations with security tools to allow security teams to perform threat assessment or forensics functions.

Conclusion

DR management at scale is a significant challenge as organizations grow, go through digital transformation, and adopt new applications and technologies. Improper DR management allows testing and general resilience hygiene to fall by the wayside, leading to longer recovery times during disaster scenarios. This leads to extra hours of downtime each year, and those costs can quickly add up.

Traditional DR models have a heavy administrative cost. IDC survey data found most organizations test their DR twice a year or less, indicating this is a widely accepted cost. However, IDC believes any tool that can free up administrative bandwidth so companies can instead focus on DR management is a positive.

SaaS-based DR offers a solution that is as close an organization can get in terms of minimal DR infrastructure-related management overhead without adopting DRaaS. While DRaaS can offer the same level of minimal overhead as SaaS-based DR, it takes many fine-grain control options out of the hands of administrators, making this approach less enticing for companies with strict or specialized storage needs for DR.

HPE GreenLake for Disaster Recovery puts forth a strong offering in the SaaS-based DR space. With its SaaS deployment model, automation and orchestration for DR, and nondisruptive DR testing, the product is heavily focused on lowering administrative overhead. The demand for data resiliency will only ever increase, and IDC believes if HPE and other vendors in this space continue to make achieving resiliency easier and simpler, they will have a constant stream of interested buyers.

DR management at scale is a significant challenge as organizations grow, go through digital transformation, and adopt new applications and technologies.

About the Analyst



Johnny Yu, Research Manager, Storage and Computing

Johnny Yu is a research manager within IDC's infrastructure software platforms research group. He covers storage controller software, data replication, protection and archiving, storage device management, and container data management, with a focus on how businesses optimize costs and secure their storage environments as their infrastructure expands beyond their datacenters.

MESSAGE FROM THE SPONSOR

HPE GreenLake for Disaster Recovery radically reduces data loss and downtime through continuous data protection using industry-leading DR technology from Zerto on a global, scalable hybrid cloud platform. Modernize your business with a cloud operational experience and flexible billing, by deploying and managing your DR from a single console, right alongside other data protection services like storage and backup. To learn more, please visit:

- » <https://www.hpe.com/us/en/hpe-greenlake-disaster-recovery.html>
- » <https://www.hpe.com/us/en/greenlake/data-protection.html>



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2023 IDC. Reproduction without written permission is completely forbidden.