

VMware Cloud Disaster Recovery

Disaster recovery as a service (DRaaS) with VMware Cloud on AWS

“With VMware Cloud Disaster Recovery, VMware users have a true DR option that works automatically and on demand, regardless of the complexity of their environment.”

STEVE DUPLESSIE
FOUNDER AND SENIOR ANALYST
ESG

CUSTOMER SCENARIOS

- Establish new DR for on-premises apps (no DR solution today)
- Replace existing DR site/solution for on-premises apps
- Complement existing DR site/solution for on-premises apps

KEY USE CASE: RANSOMWARE RECOVERY

A big challenge with ransomware recovery is determining which backup copy is clean and should be failed over. With instant power-on of virtual machines (VMs), administrators can rapidly inspect dozens of recovery points in a short period of time because there is no need to copy data or rehydrate VMs before they can be powered on. This capability is enabled via a live NFS datastore mounted by the VMware ESX® hosts in the VMware Cloud™ on AWS software-defined data center (SDDC) cluster.

Disaster recovery has become critical for every business

In a recent analyst survey, 76 percent of respondents reported an incident during the past two years that required an IT disaster recovery (DR) plan, while more than 50 percent reported at least two incidents.¹ At the same time, cyberattacks are on the rise, increasing business risk. In 2019, 52 percent of global enterprise network security decision-makers had experienced at least one sensitive data breach in the past 12 months.² It is not surprising that CxOs and board members increasingly care about DR.

Although many organizations realize the importance of implementing a robust DR solution for reasons such as business continuity, compliance with industry regulations, protection against disasters, ransomware and security breaches, traditional DR solutions can be complex, expensive, and not scale or provide the required levels of protection.

The VMware Cloud Disaster Recovery solution

VMware Cloud Disaster Recovery™ offers on-demand disaster recovery to IT administrators who are responsible for IT infrastructure and services resiliency, and face DR being complex, expensive and unreliable. It also helps security and compliance teams ensure operations can resume after a disaster event. Delivered as an easy-to-use software-as-a-service (SaaS) solution with cloud economics, VMware Cloud Disaster Recovery combines cost-efficient cloud storage with simple SaaS-based management for IT resiliency at scale. Customers benefit from consistent, familiar VMware operations across production and DR sites, a pay-when-you-need-failover capacity model for DR resources, and instant power-on capabilities for fast recovery after disaster events.



On Demand

Instant power-on without need for VM conversions for faster recovery



Easy to Use

Consistent VMware operations, continuous health checks, automated audit reports



Cloud Economics

Cost-efficient cloud storage with pay-when-capacity-needed model

FIGURE 1: VMware Cloud Disaster Recovery benefits and capabilities.

1. Gartner, Inc. “Survey Analysis: IT Disaster Recovery Trends and Benchmarks.” Jerry Rozeman, Ron Blair. April 30, 2020.
2. Forrester. “Top Cybersecurity Threats In 2020.” Josh Zelonis, Sandy Carielli, Joseph Blankenship, Elsa Pikulik, Benjamin Corey, Madison Bakalar. January 24, 2020.

“Cloud-based disaster recovery is attractive to organizations since it takes advantage of the elasticity of cloud and only consumes production resources when they are activated in a failover.”

HENRY BALTAZAR
RESEARCH DIRECTOR
451 RESEARCH³

ON DEMAND

- Instant power-on (live mount)
- Pilot light option
- No VM format conversions
- Rapid ransomware recovery

EASY TO USE

- Consistent, familiar operations
- SaaS-based management
- Continuous DR health checks
- Automated built-in audit reports

CLOUD ECONOMICS

- Pay when capacity is needed
- Efficient cloud storage
- Simplified pricing model
- Optimized failbacks

LEARN MORE

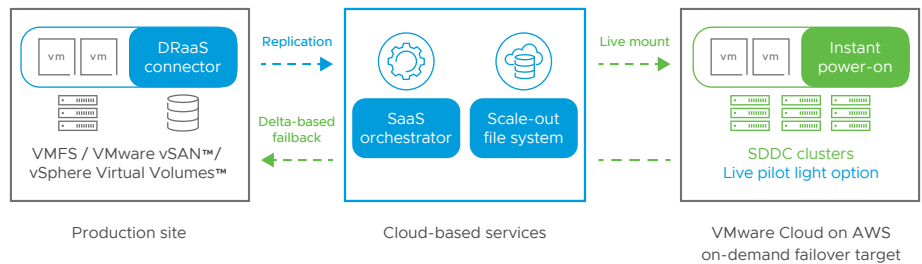
Visit cloud.vmware.com/cloud-disaster-recovery.

On demand

VMware Cloud Disaster Recovery delivers fast recovery with zero copy and no rehydration of data from cloud storage to VMware Cloud on AWS hosts required. For achieving production-level performance, workloads can be promoted (i.e., rehydrated) to VMware Cloud on AWS hosts after initial power-on of failover VMs. Using optional pilot light clusters makes the recovery time even faster. VMs are maintained in their native VMware vSphere® format, eliminating the need for brittle and time-consuming VM disk format conversions. Instant power-on of VMs is very powerful for rapid identification of the best recovery point when recovering from a ransomware attack.

Easy to use

During transient events, such as DR testing or failover, customers don't need to learn new operational processes and tools of cloud infrastructure. They can manage both the cloud DR site and production sites with VMware vCenter® and retain access to familiar vSphere constructs—such as clusters, resource pools, datastores, virtual switches and port groups—following a failover. The SaaS-based management console simplifies DR maintenance operations, eliminating the customer burden of lifecycle managing the DR software, and scales up to 1,500 VMs across multiple SDDC clusters. DR health checks occur every 30 minutes, increasing the confidence that the DR plan will work when needed. Audit-ready, built-in, automated audit reports help meet a company's internal policies and regulatory compliance requirements. A sophisticated DR workflow engine allows users to create customized and flexible recovery plans for hundreds to thousands of workloads. The scale-out cloud file system checks the data integrity every day to confirm the backup data is ready and usable when needed.



Blue: Steady state; Green: Activated on failover

FIGURE 2: Steady-state protection and failover conceptual diagram.

Cloud economics

Leveraging the elasticity of cloud computing, VMware Cloud Disaster Recovery spins up VMware Cloud on AWS infrastructure only during a DR testing or failover event. It utilizes a highly efficient cloud storage layer for storing backups, lowering DR costs. With a simplified pricing model, customers do not need to figure out all the underlying detailed infrastructure costs (such as compute, networking and storage charges), they just need to determine how many VMs and how much total data to protect.⁴ Failbacks result in minimal AWS egress charges because only data deltas/changes are transferred.

3. 451 Research, a part of S&P Global Market Intelligence. “With costly outages on the rise, disaster recovery is still a top issue.” Henry Baltazar. August 17, 2020.

4. VMware Cloud on AWS SDDC capacity for testing and failover is paid for separately.