Protecting Workloads with Dell EMC VxRail and VMware Cloud Disaster Recovery

February 2021

H18643

White Paper

Abstract

Using both Dell EMC VxRail and VMware Cloud Disaster Recovery provides a disaster recovery as a service (DRaaS) solution for protecting on-premises workloads that yields outstanding performance, and is easy to update and maintain.

Dell Technologies Solutions

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Revisions

Table 1. Revisions table

Date	Description
February 2021	Initial release

Executive summary

Disaster recovery (DR) is a topic that many organizations do not like to discuss because disasters of any type are painful. Often, recovery plans are flawed, costly, and require a significant amount of time and resources. Additionally, DR has often required a separate dedicated recovery site with identical hardware to support some or all of the organization’s critical systems.

These challenges can be overcome by using Dell EMC VxRail and VMware Cloud Disaster Recovery. VxRail provides outstanding performance, and is easy to update and maintain. VMware Cloud Disaster Recovery is a disaster recovery as a service (DRaaS) solution that makes disaster recovery easy for workloads ranging from a few VMs on a small cluster to entire data centers. Because DRaaS is cloud-based, it is not necessary to have a separate DR site with idle equipment to maintain. Instead, it is easy to test a wide variety of scenarios without having to go to a DR site or even to travel to the office.

When used together, organizations can realize additional value from the reliability and performance of VxRail, and from the robust protection of workloads delivered as a service and provided by VMware Cloud Disaster Recovery. Through simple DR orchestration and testing in VMware Cloud Disaster Recovery, the already-trusted virtual environment built on VxRail is reliably protected against disasters ranging from ransomware attacks to power outages and other natural disasters.

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by email or provide your comments by completing our documentation survey.

Author: Tony Foster

Contributors: David Glynn; Victor Dery; Bill Leslie; Bob Percy; Conor Duffy; Amanda Burkhardt; Mark Chuang (VMware); Damian Karlson (VMware); Jeff Hunter (VMware); Michael McLaughlin (VMware)

Note: For links to additional documentation for this solution, see Dell Technologies Info Hub for Integrated Solutions - VxRail.

Disclaimer: This document may contain language from third third-party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Introduction

Modern infrastructure is more resilient than ever. Virtualization, storage technologies, and even containers reduce the chances of a crippling IT disaster that could bring the organization to a full stop. However, a DR plan is still essential. It is still commonplace to hear stories of woe and despair when an organization is hit by a ransomware attack. Such attacks can require rummaging through countless recovery points to find one that is not infected. Even mundane events like cutting an important network uplink or experiencing a power outage in the data center can necessitate implementation of a DR plan.

A few decades ago, the answer to DR was tape—a slow and bulky approach to protecting workloads. This was replaced by replication technology, which allowed near real-time copies of data to be transmitted to one or more separate sites. This enabled many organizations to achieve a much quicker recovery time objective (RTO). However, it was still typically a manual and error-prone process to find and retrieve the correct recovery point and then to restore all the virtual machines in the right order to reinstate the end-to-end business processes. It was also necessary to have sufficient, compatible hardware to support the recovery of all critical workloads in a DR environment. Most of the time, that hardware would sit idle until required. This approach allowed for a relatively quick recovery but required a significant investment of time and IT resources to maintain. It also proved financially impractical for smaller organizations that could not justify the additional cost to duplicate, patch, and maintain their IT environment in order to preserve, protect, and resume using their data. Additionally, even if failover worked, failback was often an even bigger nightmare.

Today there are better tools to facilitate DR, reducing the time and resources IT needs to invest for recovery. A modern DR strategy uses cloud resources for DR. Organizations can take advantage of cloud economics for DR instead of enduring all the capital expenses needed to achieve the same level of DR preparedness.

This paper analyzes the advantages of implementing Dell EMC VxRail with VMware Cloud Disaster Recovery Service to achieve a highly reliable, fast, and consistent DR solution that leverages cloud economics. This solution harnesses VMware's technology to replicate data to a highly resilient cloud service, where it can be easily recovered. DR is made easier through the implementation of VxRail, which provides a high level of consistency, making it easier to expand an environment. It also allows IT to focus on making the organization successful instead of trying to remember how to deploy a host.

In this paper, we define the unique advantages that VxRail brings to modern disaster recovery. We consider VMware Cloud Disaster Recovery—how it works, and how it modernizes DR. Finally, we explore the benefits that leveraging VxRail and VMware Cloud Disaster Recovery together can bring to the organization.

An Overview: VxRail

Figure 1. Front view, Dell EMC VxRail

VxRail is a jointly engineered hyperconverged infrastructure from Dell EMC and VMware. It is the only fully integrated, pre-configured, and tested HCI system optimized for VMware vSAN software-defined storage and the VMware vSphere ESXi hypervisor. Managed through the VMware vCenter interface, VxRail provides existing VMware customers with a consistent and familiar operating experience. VxRail is the only jointly engineered HCI system with full VMware Cloud Foundation integration, delivering a complete and automated hybrid cloud platform.

VxRail is a distributed system consisting of common modular building blocks powered by the highly differentiated VxRail HCI System Software. VxRail allows customers to start small and grow, scaling capacity and performance easily and non-disruptively from two to 64 nodes in a cluster. VxRail HCI System Software with intelligent lifecycle management (LCM) is used to automate non-disruptive upgrades, patches, node additions, and retirement to ensure that the VxRail infrastructure remains in a continuously validated state. Coupled with detailed health reporting using machine learning from SaaS multi-cluster management, it has never been easier to keep infrastructure running smoothly.

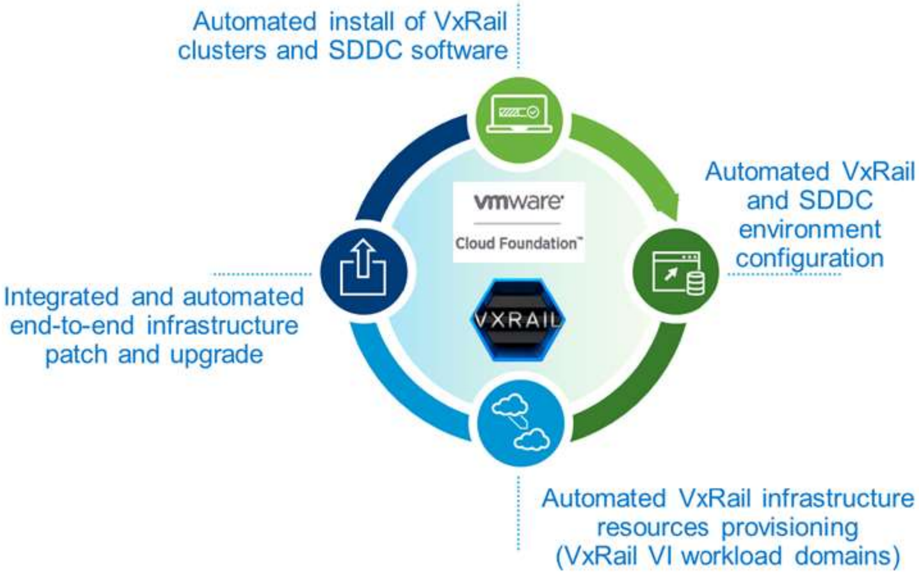

Automated install of VxRail clusters and SDDC software
Automated VxRail and SDDC environment configuration
vmware
Cloud Foundation™
VXRAIL
Integrated and automated end-to-end infrastructure patch and upgrade
Automated VxRail infrastructure resources provisioning (VxRail VI workload domains)

Figure 2. VMware Cloud Foundation on VxRail automation

VMware Cloud Foundation on VxRail is the first hyperconverged system fully integrated with VMware Cloud Foundation SDDC Manager. This means that both the hyperconverged infrastructure layer and the VMware Cloud software stack are managed as a complete and automated platform. Full integration between VMware SDDC Manager and VxRail Manager gives users consistent operations with familiar VMware tools to deploy and manage clusters and workloads across the hybrid cloud infrastructure.[1]

VxRail HCI System Software intelligent lifecycle management helps customers confidently and non-disruptively execute upgrades without the need to do extensive research and testing. Simply choose the next VxRail version and VxRail automatically upgrades the fully integrated hardware and software stack, keeping clusters in continuously validated states. IT productivity skyrockets with single-click, non-disruptive upgrades no matter what hardware generation or node types are in the cluster!

VxRail supports vSphere updates within 30 days after VMware general availability, which involves rigorous testing and a single point of contact for support. This helps to predictably evolve and expand your HCI footprint across the core, edge and cloud.

VxRail is the only jointly engineered HCI system with deep VCF integration that delivers automated lifecycle management to streamline operations and reduce TCO by 47 percent.

VxRail provides an easy method for updates, ensuring that the environment is operating at or near the same version of vSphere that is being used in the VMware Cloud Disaster Recovery ecosystem. This means that virtual machines can operate consistently across active and DR environments without the need for time-consuming upgrades during a disaster.

Even before disaster strikes, VxRail helps organizations to align more closely with operational compliance, and therefore to be better prepared for disaster. VxRail provides consistency and repeatability in the data center and at the edge.

Simply put, when a repeatable process doesn’t exist, disasters are harder to recover from. This is especially true of do-it-yourself (DIY) environments. IT staff are required to be experts at how to install and configure all the different bits that make up today’s modern IT infrastructure. From installing the virtualization platform to configuring storage and joining it to a cluster, many tasks must be done precisely and correctly.

Furthermore, in a DIY environment, being able to deploy IT infrastructure quickly and correctly doesn’t make the organization more money or improve performance at their core competencies, but it can have disastrous outcomes when deployed incorrectly. For example, if storage is misconfigured, a tiny ‘hiccup’ can cause a catastrophic loss of storage.

These are the perils to be faced in the DIY environment: minimal benefit to the organization for all the extra work to get it right, and massive consequences when something fails. IT should be focused on areas that enhance, accelerate, and set the organization apart from its competitors, without having to be IT infrastructure deployment specialists.

[1] IDC White Paper, sponsored by Dell EMC, Benefits of the Consistent Hybrid Cloud: A Total Cost of Ownership Analysis of the Dell Technologies Cloud, April 2019. Results based on U.S. costs of the Dell Technologies Cloud deploying common cloud environment workloads over a five-year period v. a leading native public cloud service provider. Actual results will vary.

In contrast to ominous DIY environments, VxRail provides a repeatable process for creating and maintaining data center infrastructure, because it helps operationalize the details of what must be configured in order to create or expand the data center. This means that VxRail can easily be incorporated into an operational compliance model that delivers consistent results in the data center. It also means that IT can be more focused on driving organizational value.

VxRail also helps with disaster avoidance and recovery. Because a VxRail environment is inherently consistent, there is less likelihood of the kind of misconfiguration that occurs when infrastructure is only being deployed occasionally. And when disaster does strike, a consistent environment is easier to recover.

These attributes make VxRail an outstanding choice for planning continuity of the organization’s applications. Since applications are the lifeblood of many organizations, being able to recover applications quickly means being able to keep moving forward.

An Overview: VMware Cloud Disaster Recovery

How can an organization protect its applications with VxRail?

One of the best ways to approach this challenge is by deploying a DRaaS solution that protects data and optimizes business resources. VMware Cloud Disaster Recovery is a SaaS-based solution that allows snapshot replication of on-premises data and IT infrastructure onto a third-party cloud computing environment. DR orchestration and testing can be done frequently, using an intuitive dashboard that guides users through the steps to effectively failover and failback their VMs with minimal disruption. This empowers organizations to restore access and functionality to IT infrastructure after a disaster. It also allows them to choose from snapshots ranging from hours to months old to conduct recovery. The as-a-service model eliminates the need for organizations to own and manage an entire site for disaster recovery, and instead uses the service provider’s cloud infrastructure only when a disaster occurs.

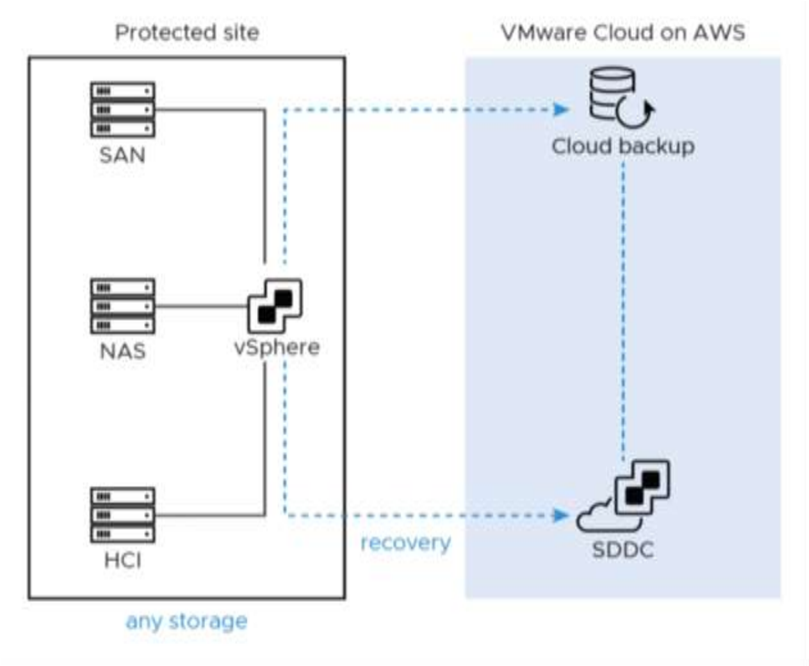


Figure 3. Protection and recovery with VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery consists of a DRaaS Connector for the protected virtual environment and a set of cloud-based services that run as native cloud services and also utilize VMware Cloud on AWS. This allows VMs to be protected through delta-based replication that is scheduled every 4, 6, 8, or 12 hours, daily, weekly, or monthly. Relatively small amounts of data are transmitted for each replicated copy. This reduces the time required to complete a replication while providing comprehensive protection of the environment. The replication sets are then stored securely in the cloud for testing or DR.

Because the DR VMs are not running in the cloud all the time, they consume only storage resources. This reduces the overall capital outlay for a DR plan, because other costs (such as cloud compute capacity) are only incurred when a virtual machine is running in the cloud environment. This also means that IT staff members are not responsible for maintaining or patching infrastructure, freeing them to focus on other organizational needs.

It is also possible to run VMware Cloud Disaster Recovery with a “Live Pilot Light” option so that an initial footprint of resources for DR is available for instant consumption and testing. This means that a minimum of three VMware Cloud on AWS hosts are always running. These three hosts can have core elements, such as SDDCs, running prior to a DR. In the event of a disaster, this would allow rapid provisioning of a full-scale production environment utilizing the critical core services already running with Live Pilot Light. When these hosts are not being used for DR-related activities, they can be utilized for other business tasks.

VMware Cloud Disaster Recovery can facilitate an elegant DR solution for organizations with:

- Multiple smaller satellite locations (satellite locations at the edge)
- Up to 20 vCenter instances that require IT infrastructure

- Two-node VxRail deployments that deliver specialized local IT capabilities

These satellite locations may not be large enough to justify a complex data protection solution or an independent hardware device. However, the VMs and data at edge sites are just as critical as those at larger sites. VMware Cloud Disaster Recovery protects these sites at the same level as primary sites, enabling operations to continue in the event of a disaster at the edge.

How VMware Cloud Disaster Recovery works

Many businesses with lean IT teams are simply unable to perform all the work required to maintain a DR site, from patching and updating to failover testing. DRaaS takes the burden of maintaining DR sites from the organization and puts it into the hands of experts in disaster recovery. It can also be much more affordable than hosting your own DR infrastructure in another region with servers running in air-conditioned rooms that no one ever visits, waiting for a disaster to strike. If a disaster doesn't happen, that expensive second infrastructure, a capex investment, just ages. Even if that second datacenter is used for other purposes besides DR capacity, it can be very time consuming to maintain compatibility with the main datacenter.

VMware Cloud Disaster Recovery offers on-demand disaster recovery not only to large IT organizations, but to smaller organizations who may lack resources (staff and equipment). It is intended for organizations that need services resiliency and face complex, expensive, and unreliable DR. VMware Cloud Disaster Recovery also helps security and compliance teams ensure that 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.

The structure of VMware Cloud Disaster Recovery consists of a DRaaS Connector, a SaaS Orchestrator, Scale-out Cloud File System, and an On-Demand Failover Target. We will look at the details of how each of these is used to deliver a holistic DRaaS solution.

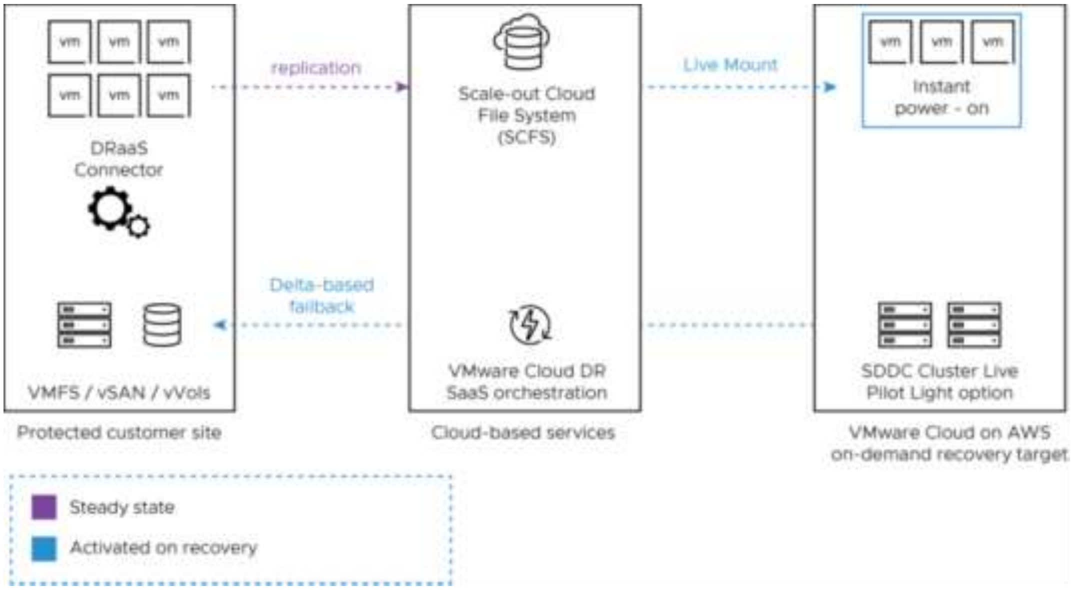


Figure 4. VMware Cloud Disaster Recovery components

The DRaaS Connector is deployed in VxRail and other vSphere environments. It provides the data protection service connection to the SaaS Orchestrator and Scale-out Cloud Filesystem. The connector is also responsible for triggering replicating copies of virtual machines (VMs) in the environment based on the protection schedule that is defined. All local activities are carried out through the DRaaS Connector vApp.

VMs can be included in a protection group by using one of three methods:

- A naming pattern that matches VMs to the pattern
- VM folders in which all VMs in each folder are protected
- vSphere tagging

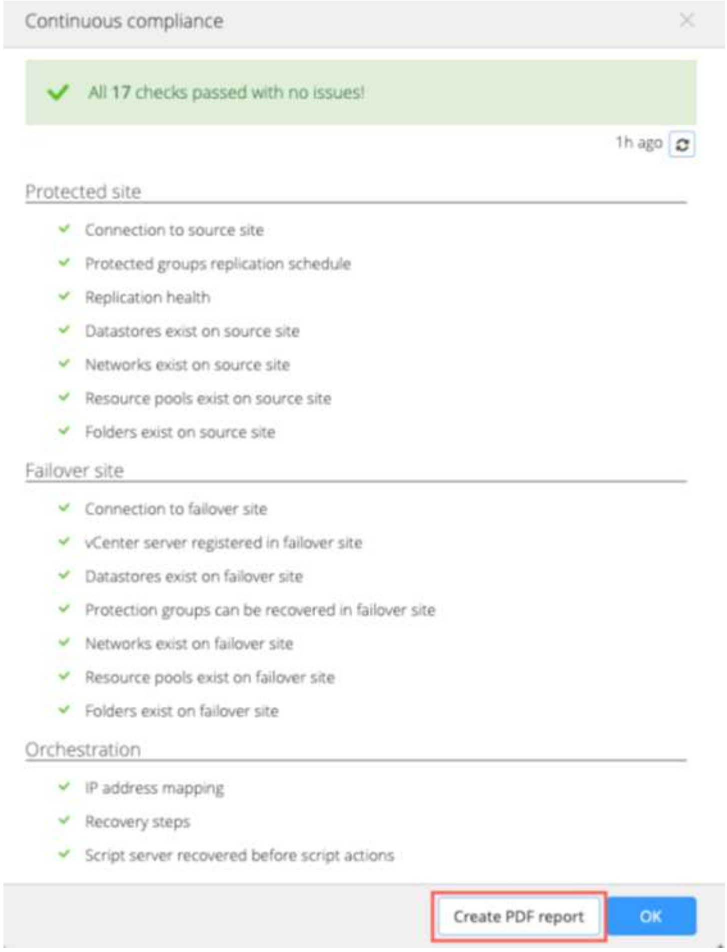
This enables new VMs to be protected automatically after they are created, making VM protection straightforward.

Replications initiated by the DRaaS Connector use change block tracking (CBT) technology. This ensures that only the parts of a VM that have been created or modified are transmitted as part of the backup instead of the entire VM. CBT can reduce the overall amount of data transmitted to the Scale-out Cloud File System. The exception to this is that the first time a VM is protected, the entire VM must be transmitted.

The DRaaS Connector is managed by the SaaS Orchestrator. The SaaS Orchestrator is a cloud-based service that controls scheduling, recovery, and other DR operations. The SaaS Orchestrator simplifies DR maintenance operations, eliminating the customer burden of lifecycle management for DR software. It can scale up to 1,500 VMs across multiple SDDC clusters. Compliance Checks occur every 30 minutes, increasing the confidence that the DR plan will work when needed. DR Plans can be run either as a failover, or as a 'Test Failover,' which performs all the plan's recovery operations in a test site for validation. Finally, VMware Cloud Disaster Recovery automatically generates detailed reports for events such as tests and failover, to comply with internal organizational policies and regulatory compliance requirements.

Compliance checks run automatically to verify the integrity of all constraints and definitions listed in the DR plan. For example, if the DR plan relies on replication of protection groups between different sites, compliance checks continuously monitor replication health and alert the administrator if, for example, replication stops because of the erroneous application of firewall rules. An alert is triggered at the time the firewall change is implemented, which provides a chance to address the firewall problem immediately instead of waiting for the next DR testing cycle to expose this problem.

Compliance checks also monitor many other components at protected and recovery sites. They perform integrity checks on the DR plan to make sure that referenced objects such as VMs, datastores, or virtual networks continue to exist and remain healthy. Below is an example of a continuous compliance report for a healthy plan.



Continuous compliance

✓ All 17 checks passed with no issues!

1h ago

Protected site

- ✓ Connection to source site
- ✓ Protected groups replication schedule
- ✓ Replication health
- ✓ Datastores exist on source site
- ✓ Networks exist on source site
- ✓ Resource pools exist on source site
- ✓ Folders exist on source site

Failover site

- ✓ Connection to failover site
- ✓ vCenter server registered in failover site
- ✓ Datastores exist on failover site
- ✓ Protection groups can be recovered in failover site
- ✓ Networks exist on failover site
- ✓ Resource pools exist on failover site
- ✓ Folders exist on failover site

Orchestration

- ✓ IP address mapping
- ✓ Recovery steps
- ✓ Script server recovered before script actions

Figure 5. Example of a continuous compliance report for a healthy plan

The DRaaS Connector connects to the Scale-out Cloud File System. It runs on cloud object storage, and stores replication point copies. These copies are immutable and encrypted for security. VMs are kept in the native vSphere format, making recovery quicker. You do not have to copy the replicas from the Scale-out Cloud File System to the VMware Cloud primary storage system before you power on the VMs. You can instantly power on the VMs as soon as the SDDC capacity is available and settings are configured. Also known as Live Mount technology, this allows the VM to be restarted without first copying the VM to SDDC primary storage. This also makes testing much simpler to carry out, as the VM can immediately start on the On-Demand Failover Target.

The On-Demand Failover Target is a VMware Cloud on AWS instance. That means VMs running in a local software defined data center (SDDC), such as those built on VxRail with VMware Cloud Foundation, can easily be recovered in the event of a site failure, ransomware attack, or other DR scenario. Both VxRail and VMware Cloud on AWS use the same virtualization technology. Because of this, it is easy to keep the primary site up to date and match the version of the On-Demand Failover Target, especially because it is easy to keep VxRail updated. Therefore, compatibility issues between versions are substantially reduced, allowing IT staff to focus on recovery instead of versioning during a disaster.

A faster recovery scenario is possible where SDDC clusters have reserved resources available to begin a DR at a moment's notice. This is available with the Pilot Light option of VMware Cloud Disaster Recovery. Pilot Light reserves resources in the On-Demand Failover Target and allows for configuration of critical services, like network resources and other service mappings, so they are already running. This reduces the recovery steps that must be completed before applications can be brought back online.

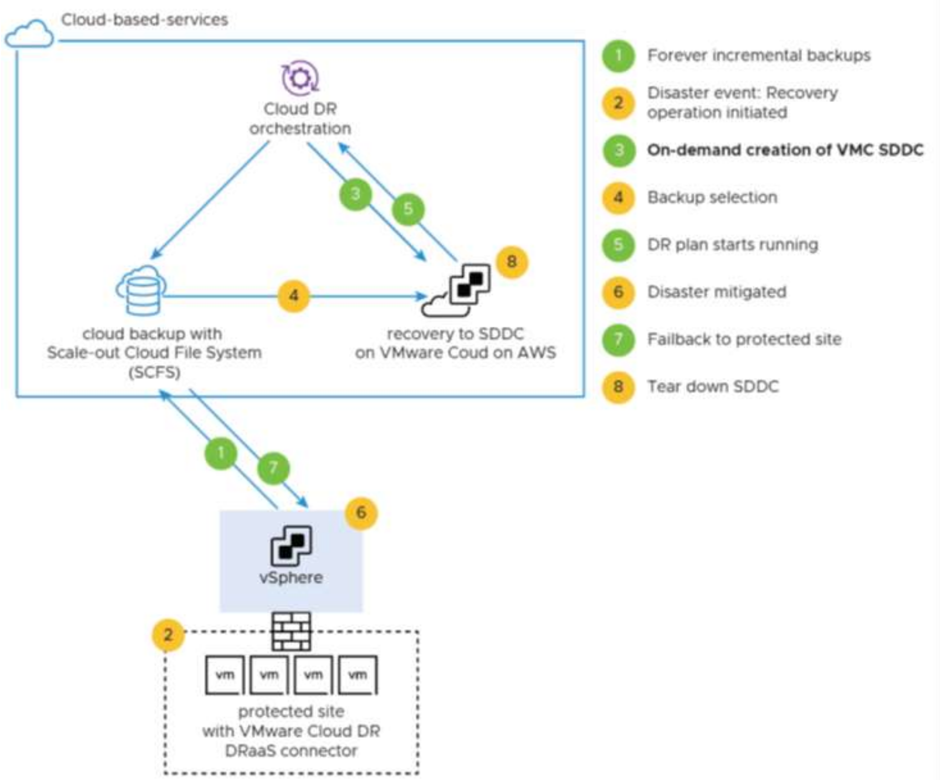

Cloud-based-services
Cloud DR orchestration
cloud backup with Scale-out Cloud File System (SCFS)
recovery to SDDC on VMware Coud on AWS
vSphere
vm
vm
vm
vm
protected site with VMware Cloud DR DRaaS connector
1
2
3
4
5
6
7
8
1 Forever incremental backups
2 Disaster event: Recovery operation initiated
3 On-demand creation of VMC SDDC
4 Backup selection
5 DR plan starts running
6 Disaster mitigated
7 Failback to protected site
8 Tear down SDDC

Figure 6. On-demand functionality of VMware Cloud Disaster Recovery

These factors create the basis for a simple and straightforward recovery. The elasticity of cloud computing means that there are only charges for the compute resources in use during a DR failover or DR test, reducing the cost of DR. Leveraging the cloud for DR eliminates the need for idle equipment that is being paid for but not used.

Returning to Normal with VxRail and VMware Cloud Disaster Recovery

Through the use of CBT technology, failbacks to the original site are optimized to send only what has changed. If the VM is still available at the primary site, there is no need to retransmit the whole VM, just the changed portion. This reduces egress charges as things return to normal at the primary site. It also reduces the time required to return to normal by shrinking failback times as compared to transmitting an entire VM.

VxRail provides a significant advantage to organizations through the quick availability of updates. Cloud platforms apply updates with an untiring cadence to provide users with optimal environments that are patched for vulnerabilities and security risks. When failing back to the primary site, it is important that both environments are at nearly the same version to minimize the possibility of any issues. This advantage makes VxRail the optimal on-premises platform for disaster recovery. The ability to keep VxRail up to date serves an important role as part of DR. It minimizes the time IT needs to spend ‘preparing’ to return to normal operations and allows them to spend more time on the real work of returning to normal operations.

One of the considerations of returning to normal operations is how quickly the primary site can be repaired, or a new site brought online. VxRail inherently accelerates the return to normal operations, because it is a hyperconverged infrastructure. The need to focus on individual data center silos is lifted and the focus shifts to addressing a unified environment.

By addressing the data center as a unified environment, IT can realize operational efficiencies that are unattainable with traditional siloed infrastructure. For example, there is no longer a pause as part of the hand off between infrastructure teams because those handoffs are unified as part of VxRail. This smooth transition translates to greater speed and agility when returning to normal operations.

When VxRail is coupled with the failback capabilities of VMware Cloud DR, the steps to return a site to operational status can be reduced. This reduction can allow IT staff to focus on other pressing issues that arise during a DR failback. When an organization has already been through one disaster, failback shouldn’t be another.

Summary

VMware Cloud Disaster Recovery with VxRail provides an outstanding disaster recovery solution for organizations.

DR can include dealing with the impacts of ransomware, human error, partial disasters, and full site disasters. No longer are organizations faced with having to maintain the capital investment of a DR site and all that goes with it. They can also avoid woe and despair when hit by a ransomware attack, or avoid guessing whether they retrieved all the tapes needed to recover a site when a ruptured water line floods the data center. With VMware Cloud Disaster Recovery, they can now feel confident in their ability to recover their virtual environment.

The foundation for such a virtual environment should drive consistency in the data center, easing the burden of a disaster. VxRail provides this consistency to organizations and enables operational compliance while providing a robust data center platform. This makes it easier to protect and recover the data center when disaster strikes. This consistency also makes the failback smoother, with less chance of delays due to siloed IT. Furthermore, organizations can leverage the substantial capabilities of VxRail while realizing the benefits of cloud for DR.

A benefit of DRaaS is that to support the DR site, on-premises infrastructure is no longer required. This lessens or removes the capital investment needed for DR, making DR accessible to organizations that might not have been able to afford a DR strategy. Additionally, cloud recovery can be performed quickly from almost any location, allowing teams to remain separate when travel may be difficult. Use VMware Cloud Disaster Recovery to replicate data to a highly resilient cloud from which it can be easily recovered.

At a high level, VMware Cloud Disaster Recovery consists of a DRaaS Connector, a Scale-out Cloud File System, a SaaS Orchestrator, and VMware Cloud on AWS. Additionally, a Pilot Light feature is available in which SDDC core services can be pre-staged and operational prior to a disaster, further decreasing the time it takes to perform a DR. This translates into less down time and fewer lost hours for the organization.

Automatic compliance checks in VMware Cloud Disaster Recovery provide confidence that the disaster recovery environment is ready whenever disaster strikes. This allows organizations to focus less on DR and more on the organization’s needs.

When VxRail and VMware Cloud Disaster Recovery are used together, organizations can realize the reliability and performance of VxRail while protecting the workloads running on them by leveraging the cloud. This makes both conversations about DR and DR events less taboo, and helps organizations to realize their full potential even when disaster strikes.

For additional information on VxRail and VMware Cloud Disaster Recovery, please reach out to your Dell Technologies partner or sales representative.

References

Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- Dell EMC VxRail Hyperconverged Infrastructure product page
- VMware Cloud Foundation on VxRail product page

VMware documentation

The following VMware documentation provides additional and relevant information:

- VMware Cloud Disaster Recovery
- Using VMware Cloud Disaster Recovery
- VMware Cloud Tech Zone - DRaaS