The VMware Guide to Disaster Recovery Readiness

Accelerate disaster recovery and empower your DReam Team with VMware Cloud Disaster Recovery™

GET STARTED

The Dawn of Disaster Recovery: Is it the Need of the Hour?

When it comes to data, planning for the unexpected has become paramount in today's modern era. But long-term problems shouldn't be solved with short-term solutions. Protecting data has become a shared responsibility, and disaster recovery is the last line of defense when everything else goes wrong. As such, it should be treated as a business decision that could impact the future of your organization.

Are you living the DReam or losing sleep anticipating a disaster recovery nightmare? Here is why you should be thinking about disaster recovery:

Did you know?

$250K
per hour is the average cost of downtime for enterprises[1]

76%
reported an incident in the last two years that required a DR plan[2]

75%
changed their data protection and recovery strategies as a result of COVID-19[3]

In the aftermath of an attack, tension will be high, and the less thinking on the fly that needs to be done, the better.

1. IDC's Enterprise IT Infrastructure Survey, 4Q20: Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions
2. Gartner, "Survey Analysis: IT Disaster Recovery Trends and Benchmarks", J. Rozeman, R. Blair, 30 April 2020
3. IDC's Enterprise IT Infrastructure Survey, 4Q20: Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions

DRaaS vs. Traditional DR: Make Informed Choices

Disaster Recovery as a Service (DRaaS) or Traditional On-premises DR?

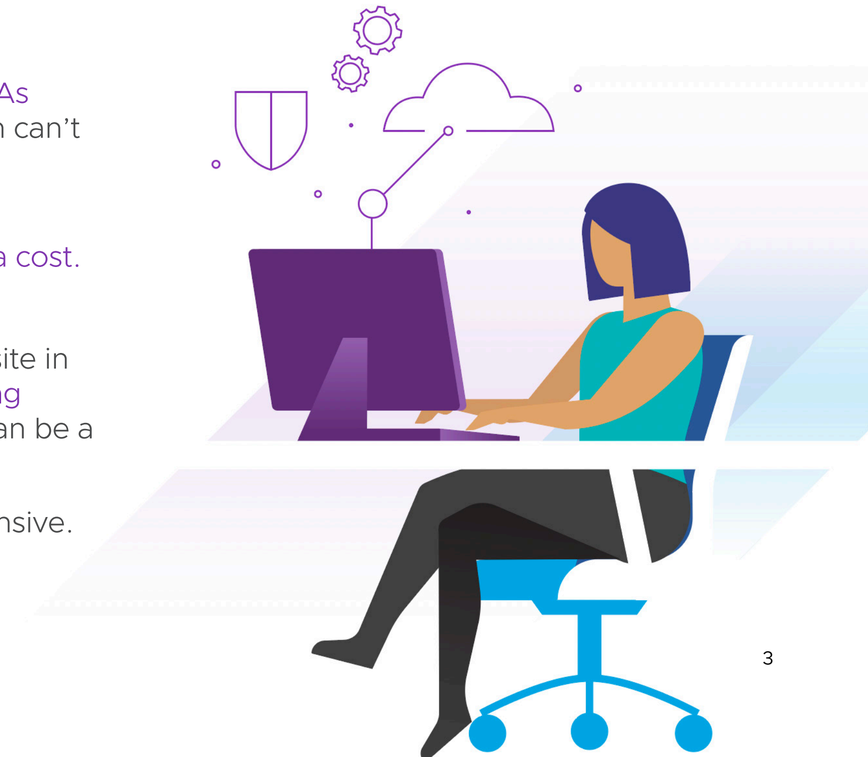
With the rapid evolution of disaster recovery, having a tested and proven DR plan has become vital to keep businesses running. Learn more about the differences between DRaaS and Traditional DR to make the right choice for your needs.

DRaaS (Disaster Recovery as a Service)

- OpEx-intensive: No initial investment in hardware.
- No lifecycle management: Auto-update without the need for manual operations or complicated renewals.
- Non-disruptive testing streamlines DR operations and boosts recovery confidence.
- Up to 60% Lower Total Cost of Ownership compared to Traditional DR. *Learn more*
- Serves most workload SLA requirements.
- SaaS-based service abstracts complexity from DR operational and maintenance tasks.
- Vendor-managed solutions minimize IT resources required to operate.

Traditional DR (On-Premises)

- CapEx-intensive: requires upfront investment in hardware, which is then amortized over time.
- Will serve workloads with the most stringent SLAs (RTO and RPO under 5 minutes), or those which can't yet be stored in the cloud due to compliance regulations.
- Can provide near-instant RPO and RTO, but at a cost. *Learn more*
- Testing requires shutting down the production site in order to conduct a failover—this increases testing friction, driving lower testing frequency which can be a crucial pain point in DR implementation.
- Customer-managed solutions can be labor-intensive.

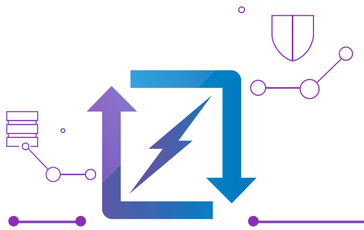


DRaaS vs. Traditional DR: Make Informed Choices

What's even more important than having a DR strategy, is having one that works. You might have a plan in place, but how often do you test it? How confident are you that you'll be able to recover if disaster strikes?

Pro-Tip

Easy, non-disruptive testing is your best friend when it comes to data recovery. Have a plan, test it frequently. Planning and testing your DR operations will help you recover seamlessly when it's time.



Want to see how the cost efficiencies of VMware Cloud DR apply to your environment? Check out our TCO Tool

Let's unpack the five essential steps to DR readiness

Did you know?

Only 38%

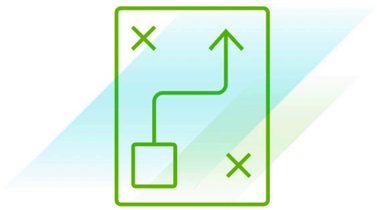
Test their DR plans more than twice a year[1]

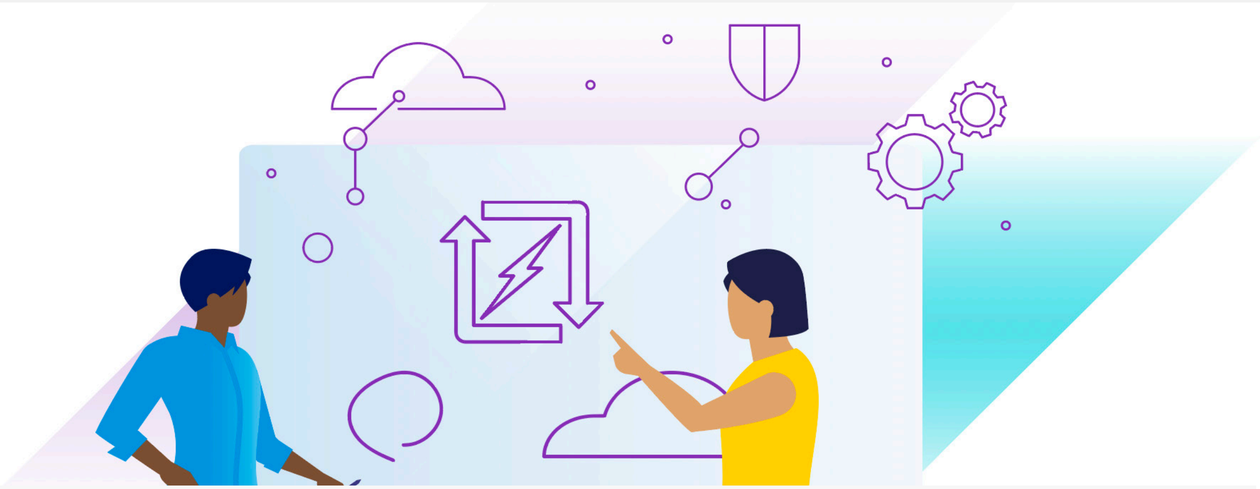
1. 451 Research Voice of the Enterprise DR Survey 2021

Day 1: Plan

The first step to DR Readiness is, guess what? Planning. Start by understanding your data estate. You can't protect what you can't see. Here's where you map applications, select SLAs and catalogue your on-premises infrastructure. Doing this right will save you time and resources down the road.

Not all your applications will have the same SLA or retention requirements, which is why this will end up being an iterative, VM-level customizable process based on the protection groups you create and their corresponding times of recovery. This is also a business decision—What protection do your workloads need, and how can you optimize the resources you assign to your DR operations without compromising on reliability? Here's where having a customizable solution will help.





Pro-Tip

Figure out what you're going to protect by mapping your applications and organizing your on-prem infrastructure. Then, ask yourself the following questions:

- What are your critical applications?
- What applications are you recovering?
- What application dependencies exist?
- How often does each VM need to be replicated to the cloud-based service?
- How long do the immutable cloud-based snapshots need to be stored for?
- What are your required SLAs for different workload tiers? Lower RPO and RTO requirements will have a direct impact on cost, so here's where you should match your business-required SLAs to TCO and assign your workloads the protection they need to maximize value in your DR solution. How do you do that? With a tiered approach to DR

Day 2: Define

It's time to define the scope of your DR plans. Now you've catalogued your infrastructure, identified your critical applications and understand what dependencies exist. The next step will be to build DR sites from the intuitive web-based UI by accessing the corresponding tab. Then, create Protection Groups. Select the VMs you want to protect by seamlessly conducting a tag-based search. Set up a test Protection Group (Here's where the SLAs you chose in Day 1 will be essential). Once you make sure your test Protection Group works, you can start taking manual snapshots of all your remaining Protection Groups—better known as data replication. This is the first step to successful recovery.

Pro-Tip

Ask the following questions when you're thinking about defining your protection groups:

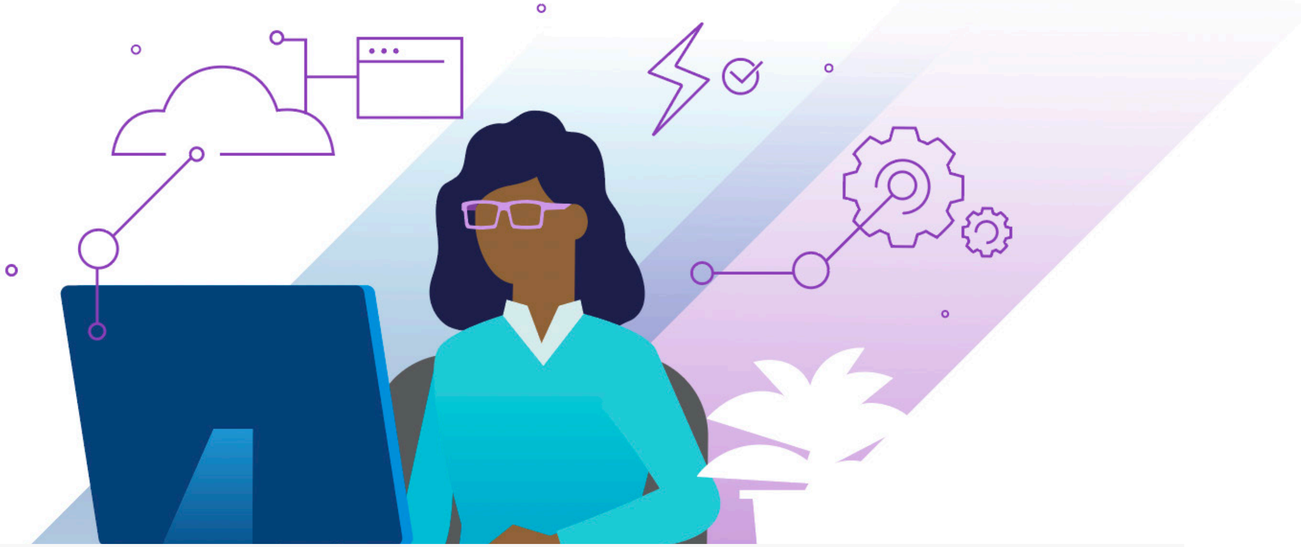
- Align your protection groups to recovery goals—do you need granular recovery?
- What is your protection schedule?
- How long will protected data be stored for? (This will impact your TCO)

Day 3: Configure

A DR plan has been outlined, and your protection groups are created. What now? You need a place to failover to, so the next step is to build the recovery SDDC. Once that's completed, deploy a cloud test. Set up the production and DR site so that you have operational consistency and familiarity, usually referred to as "aligning the sites."

Now that both sites are deployed, build and test your DR plans. Choose the protection groups and do the vCenter folder, compute resources and virtual network mappings. The tool provides user guidance, so you don't need expert IT skills.

Once your protection groups are created and adjusted to fit your DR Plans, you are ready for Day 4.



Pro-Tip

- When building plans and doing the mappings, try it out first in a small SDDC footprint—test, test, test.
- A Tiered approach to DR: If you want to minimize RTO, leverage Pilot Light Mode, which removes the need to wait for the DR SDDC to deploy.
- For enhanced ransomware protection, set up an isolated network in your SDDC so you can quarantine and test any backup snapshots before conducting failovers. This will give you an air-gapped environment to safely test your snapshots for malware before failing over your entire environment.
- Keep a record of your mappings and keep that with your runbooks and configuration test reports.

Day 4: Test

Once the protection groups are created, it's time to failover. But first, test your plans. It is easy, non-disruptive, and it's the cornerstone of your DR strategy. When running the test, the applications will start populating in the recovery SDDC. Once the test has been performed correctly, the SaaS Orchestrator will clean up the test environment. Access reports on your DR tests from the UI and deploy your DR failover plans non-disruptively.

Pro-Tip

- For deployments with Pilot Light Mode, this process will be faster as there's no need to wait for the failover SDDC to get provisioned. So for critical applications, you should consider Pilot Light as part of your tiered approach to DR.
- You can leave VMs and files in the cloud filesystem if you only want to test your plans without doing a full failover.
- Here's where you validate your Protection Groups and optimize the granularity and frequency of replication to the cloud-based service. Iterate on this until your protection groups fit your DR needs.

Day 5: Operate

You've made it to Day 5! Here's what you'll be doing today to make sure you're all set to operate.

Look at the progress of the protection groups and make sure everything's running. Next, access the Monitor dashboard and check overall DR conditions. Last but not least, run reports for audit compliance—these will serve as proof that your DR plans are being tested and executed correctly.

Pro-Tip

- Delete the SDDC you deployed for your tests to achieve maximum cost optimization. Or, if using Pilot Light Mode, utilize those SDDCs for other purposes to maximize the value of your cloud footprint.
- Review your DR reports and match them to your required SLAs—you might have to change your protection groups or make adjustments.

Unlocking the Power of DRaaS with VMware Cloud DR

Access on-demand disaster recovery delivered as a SaaS solution with cloud economics. Learn how VMware Cloud DR can help you drive your business growth with smarter DR

Compare DRaaS vs. Traditional DR for your environment with our TCO Tool

Flexible Deployment Options

Get the flexibility to choose between deployment options-set up failover capacity 100% on-demand or with minimal footprint through Pilot Light Mode

Optimized Costs

Leverage the elasticity and reliability of cloud to balance effective DR operations and optimized IT resource allocation to achieve up to 60% lower TCO

VMware Operational Consistency

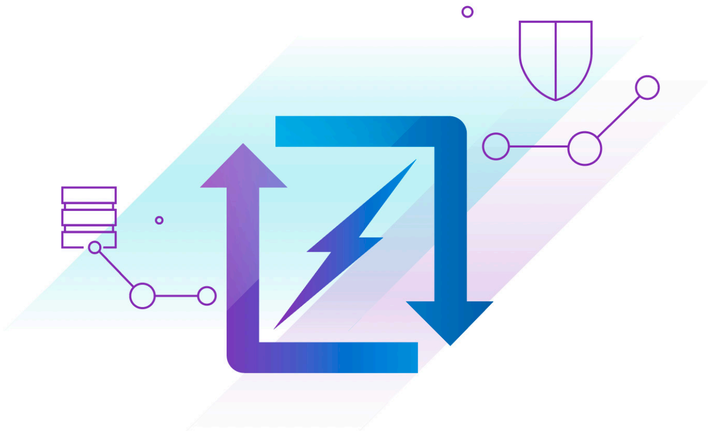
Maximize ease of use—use a consistent operating experience on-premises and in the cloud with automated failover and failback

Features

Power your disaster recovery plans with VMware Cloud Disaster Recovery solutions:

- **Pilot Light:** Provision a small failover footprint capacity in the cloud and scale on-demand
- **Instant Power-on:** Instantly power-on your VMs in the cloud when testing or orchestrating your DR plans
- **Immutable Snapshots:** Protect your data from malware thanks to a deep history of immutable snapshots
- **Continuous DR Health Checks:** Essential for ransomware recovery, DR health checks drive recovery readiness and are run every 30 minutes
- **Delta-based Failback:** Minimize cloud data egress charges and optimize DR operational costs
- **Detailed DR Reports:** Provide proof that DR plans are being tested and executed correctly

Modernize your existing DR, optimize operational costs, and accelerate ransomware recovery with **VMware Cloud DR**



Accelerate Your Disaster Recovery Journey with VMware

Defining and implementing your DRaaS strategy has many moving parts and requires a focused effort. You need the appropriate resources (staff and time) to deploy and validate your solution.

VMware Professional Services can help streamline and expedite your DRaaS implementation. We can create and implement an end-to-end disaster recovery strategy that meets your RPO and RTO objectives, accelerate time to protection, and simplify disaster recovery operations. We use a proven, scalable, and repeatable approach to ensure your implementation is effective, and establish ongoing processes that enable you to continuously validate DR plans and remove configuration drift with a high success rate.

VMware Professional Services

Get started today

Assumptions

1. Assuming a 1 Gbps link to AWS provides about 10TB/day data rate to enable up to ~20 TB to be protected in 2-3 days to enable protection of VMs to be tested.
2. Does not include a major site overhaul to run applications in a hybrid cloud environment. That is more NSX/HCX/VMC/AWS related and outside the scope of this proposal.
3. Assumes network connectivity from on-premises to cloud has been established, and the team has all of the necessary privileges and access needed to perform tasks.
4. Does not include core infrastructure modification to support hybrid or cloud-only operations (e.g., DNS, DHCP, load balancing, VPN, firewalls, etc).
5. Does not include DR plan Script VM customizations – a sample Script VM can be included in the prepare and test phases as an example only.

Get Started Today

Learn more about how you can create and implement your cloud-based disaster recovery strategy faster with VMware Cloud DRaaS Services.

Learn More

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMware-guide-to-DR_Ebook_v3 8/21