

E-BOOK

STEP-BY-STEP PLANNING FOR DISASTER RECOVERY

 NetApp



CONTENTS



Introduction	03	→
Phase 1: Strategy	04	→
Phase 2: How to take action	06	→
Phase 3: Testing	08	→
Disaster recovery plan template	10	→
Summary	12	→

INTRODUCTION

Disaster recovery remains the most pressing concern for businesses in the cloud today. Although ransomware is a chief concern, additional threat vectors such as human error, natural disaster, network failures, and software vulnerabilities make developing a disaster recovery strategy the top IT priority for every business today, whether it operates in the cloud or not.

This e-book discusses a three-phase process companies can use to begin to conceive, design, and enact secure disaster recovery plans. Starting from the initial strategy sessions, through the design phase, to testing the solutions you put in place, this guide gives step-by-step instruction to making sure of business continuity when the worst takes place.





PHASE 1: STRATEGY

Your disaster recovery plan starts with building a thorough strategy. Here you discover the limits of your company's ability to tolerate a disaster event, lay out and document all of the goals and procedures for your company's response to that disaster, and establish the tools you use to get your operation back online.

1

Define recovery objectives

Your overall operation has a bottom line for how long it takes to recover from an attack or failure before it begins to cause harm. There are two measurements for disaster recovery that are universal to business continuity: your deployment's recovery point objective (RPO) and recovery time objective (RTO). Your RPO is the length of time that your business can withstand a loss of data before full recovery. Inability to access after the RPO is considered to be harmful to the business and its ability to operate. The RTO is the length of time it takes from when a system is affected to full system recovery. A company must be aware how long it can tolerate a loss of function without severe loss of business, traffic, or SLA. In some cases there can be not only financial losses but also legal repercussions if RTO is missed.

PHASE 1: STRATEGY

2

Know your response team:

In this second step of the strategy phase, you have to identify all of the individuals who make up your disaster recovery response personnel. This list should include obvious team leaders such as the CEO and CTO (and possibly the CFO and COO, depending on your company). It should also extend to the engineers and system administrators who are instrumental in bringing the system back to normal.

Additional team members to include in the response team are the public relations department head and the contact persons at any major customers, partners, or vendors who might rely on your company for their normal business operations. This list of personnel should also—to the extent that anything that happens in a disaster is predictable—outline some of the expected tasks those individuals would be expected to perform in a crisis.

3

Set up lines of communication

After personnel have been identified and their roles in the course of a disaster and its recovery are established, the next step is to establish clear lines of communication, which are followed during the disaster. You should also be prepared to notify the proper authorities to contact in case of a malicious attack or other failure.

Specific communication applications should be selected to use in the disaster scenario. In addition to the electronic channels of communication, a physical site should be designated for face-to-face crisis response conferencing. Another crisis communication hack is to store backup cell phones—with sufficient plan coverage and battery charge—that can be used for phone calls or SMS, because normal communications over your network might be disrupted.

4

Document your resources:

The next part to drawing up your plan is to document your resources. Resources to list in this document include all of the network connections, all of your system's requirements, your system's rate of usage, OS system details, running applications, and the location of all stored data and backup data. In short: You want every aspect of your IT deployment to be laid out in full. This information is no small amount, but it is crucial in a disaster event.

5

Select a disaster recovery location and minimize the costs

Whether you deploy in the cloud or still have your data center in the building with you, choosing the right disaster recovery tools is an important part of the planning process. The cloud, however, has a few resources available that make it the more attractive choice for disaster recovery. A backup site can easily be run using cloud resources, giving you a failover site that can be ready to act instantaneously. With so many elements in play for a disaster recovery, your TCO might become a point of concern at this stage. Costs are a significant challenge in maintaining effective disaster recovery solutions. One way to manage costs is to select tools that reduce the amount of storage space or bandwidth it takes to maintain backup data. NetApp offers solutions to both those problems: NetApp Cloud Volumes ONTAP® can help reinforce your company's disaster recovery capabilities by offering timesaving and cost-cutting storage efficiencies, using NetApp® SnapMirror® data replication technology.

Cloud Volumes ONTAP acts to save on storage space by using powerful features such as tiering infrequently used data to Azure Blob Storage, data compression and deduplication, and thin provisioning. Combined, these features utilize storage more effectively, which creates a significant savings for keeping up-to-date copies of your business-critical data.



PHASE 2: HOW TO TAKE ACTION

In this phase of your disaster recovery planning, you design the actions that you take in the course of a disaster event. A useful document to create based on the steps outlined in this phase is a flowchart outlining the cascading reactions to the initial threat detection. This flowchart should be appended to the disaster recovery information that you compiled in the strategy phase.

PHASE 2: HOW TO TAKE ACTION

1

Know when to react:

This step is where everything hinges. How can you tell if an incident can be easily addressed or if it is going to cause harm to the business?

One best practice for knowing when to react is to employ an alert and monitoring system that can notify you as soon as red flags are raised. Another useful resource for determining disaster activity is from your business's users themselves: When they can't access the site, you'll know about it.

When it seems as if an event might be taking place, the first steps to take should be to assess all of your server hardware, cloud service, logs, network, and anything else IT-related to look for problems. If any one of these components isn't operating normally, it may be time to put your disaster recovery plan into effect.

2

Know how to react:

When it's clear that what you're dealing with is in fact a disaster, immediately activate your backup failover site. Booting up the backup site is not the end of this step. A lot of verification has to be done to make sure that the site can operate as close to the normal production environment as possible. That means verifying that data is synchronized and that critical site features are operating. These processes and the teams responsible for them should all be listed and labeled in the disaster recovery plan document.

3

Get back to normal operation:

Backup sites aren't meant for continuous deployment, because they aren't designed for a full production workload; the sooner you can get back to the primary site, the better.

Anticipate the order in which elements of your application will return to normal operation, and estimate how long the failback will take, including any anticipated loss of services. Some cloud providers have solutions that offer automatic failback when the primary site is back online; these solutions can be helpful in making sure that there is no break in services.



PHASE 3: TESTING

Things might have bounced back to normal, but that doesn't mean you can rest easy. After you know how your disaster recovery plan will react to a catastrophic event, you need to design the part of your plan that tries to make sure that it doesn't happen again—or ever. A big part of that means testing, but it also means staying on top of updates and paying constant attention to your deployment.

PHASE 3: TESTING

1

Test everything, then repeat:

Every part of your disaster recovery plan should be fault-tested. After that happens, test it again. If you don't test your plan, it might not work. Failover tests to backup sites should be planned to take place at least once or twice a year. Not every company can afford it, but the ideal is to perform failover tests once every quarter. These tests won't just give you an assessment of the health of your sites. They also give you a chance to see your personnel in action and make any necessary changes to the structure of the disaster recovery plan that was outlined in your strategy phase.

These tests don't always need to be full-on war-game scenarios. Testing can be integrated with the normal operation of your business. Shifting less-important workloads to the backup site in order to offload usage on the primary site is not out of the ordinary; such shifting gives administrators a good idea of how well the backup site holds up to usage.

2

Update routine regularly:

Testing gives an idea of how your disaster recovery system will perform in a crisis, but you need those elements to run at the latest build possible to make sure you aren't vulnerable to the latest threats. Patching and updating should be scheduled to automatically bring your system up to date with the latest fixes.

Another important area to keep up to date is your disaster recovery plan documentation. These documents should detail how every aspect of your disaster recovery plan behaved during each test and accurately assess the performance of team members. This information should be used to adequately adapt to any weaknesses that might have been discovered during the test or actual disaster event.

3

Stay vigilant:

Even after all the previous steps have been taken, there is always a reason to worry about the vulnerability of your deployment. This situation is not necessarily a bad thing; one of the biggest mistakes a company can make when it comes to cybersecurity and its disaster recovery preparedness is negligence. Remaining vigilant against all possible threats is a sure way to keep one step ahead of the next attack.

Ways to stay vigilant include employing threat-monitoring systems that can keep an eye on your primary and failover sites. Using a cloud service provider makes it possible to take advantage of additional tools for monitoring.



DISASTER RECOVERY PLAN TEMPLATE

Although the following template can't fully simulate the actual length of the average company's disaster recovery plan document—something that can span as many as 50 pages—this template gives you an example of the kind of information that your plan should include in a layout you can use.

DISASTER RECOVERY PLAN TEMPLATE STAGES

	System definitions	Incident detection and response	System restoration
Time frame	Months to years before incident occurs	Up to 24 hours from initial detection until response takes effect	Up to 36 hours from initial detection until system is fully restored
Action items	Determine your RPO and RTO points. Draw up definitive steps for disaster recovery procedures.	<ul style="list-style-type: none">• Receive notification of threat by monitoring service or complaint.• Deploy response team.• Analyze situation to determine if restoration can be achieved before RTO or if disaster recovery steps should be taken. If disaster recovery is put in motion, activate the backup site. Ops should take all necessary steps to restore VMs, telecommunication, SAN.• Validate data integrity of database, looking for potential data loss.• Reroute all customers to failover site.	<ul style="list-style-type: none">• After the disaster has been addressed, move to restoration.• Verify that normal site operations are functional.• Check network, application, and other component Services.• Test use of primary site before returning services to the site.
Reference material	Disaster recovery strategy document (sections on RTO/RPO information, response personnel contact lists)	<ul style="list-style-type: none">• Disaster recovery strategy document (sections on infrastructure details, failover steps, cloud service support details, if any)• Response and resolution flowchart	<ul style="list-style-type: none">• Disaster recovery strategy document (infrastructure details, failback steps)• Response and resolution flowchart

TRY OUT CLOUD VOLUMES ONTAP FOR FREE

Incur no software charges for any trial under 500GB



SUMMARY

The three planning phases described in this guide offer an essential outline for recovering from debilitating events. Although this guide is a good way to start, it isn't a one-size-fits-all solution. You have to tailor your company's response to your specific needs.

No matter how much you value the full operation of your business, a skyrocketing budget may make you hesitate to fully invest in an appropriate disaster recovery plan. Turning to the cloud-based disaster recovery solutions offered by NetApp is one way to reduce the costs of on-premises disaster infrastructure, but even that might not be enough.

The best approach in that scenario is to turn to trusted third-party vendors for further cost-cutting and disaster recovery capabilities in the cloud, such as Cloud Volumes ONTAP. Efficient RTO and RPO require full backups to be stored at all times. Cloud Volumes ONTAP provides you with a way to keep storage costs for that data under control through the use of powerful space-saving features, and makes migration easy and efficient. If you are ready to take the next step in creating a disaster recovery plan that is both effective and cost-conscious, NetApp can help you with a free trial of cloud volumes ONTAP.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:
THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp. The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications. RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987). Trademark Information NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.



About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry’s best data management. As the only enterprise-grade storage service natively embedded in the world’s biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. www.netapp.com



[Contact Us](#)

