VAST
IT without Limits™

WHAT POTENTIAL IT DISASTERS KEEP YOU UP AT NIGHT?

Your Guide to Disaster Recovery as a Service (DRaaS)

VAST
IT without Limits™

What Potential IT Disasters Keep You Up at Night?

Your Guide to Disaster Recovery as a Service (DRaaS)

There are many kinds of disaster that can shut down your information technology (IT) operations:

- natural disasters, like a hurricane
- power outages
- a hardware crash that corrupts data
- employees who accidentally or deliberately delete or modify data
- malware that tampers with, erases, or encrypts data so you can't access it
- network outages due to problems at your telecom provider

Disasters happen, sometimes bringing down a single application, sometimes bringing down your entire data center. No matter how careful you are or how good your IT team is, eventually some event will shut down your applications when you really need them up and running. The Disaster Recovery Preparedness Council survey in 2014 found that 36 percent of businesses lost at least one critical application, virtual machine, or data file for a period of several hours, with 25 percent saying they'd lost a large part of their data center for a period of hours or days.

The costs of preparing for disaster can be high—at one extreme, companies maintain a secondary, standby data center with all the same equipment as at their primary site—but the consequences of not planning for disaster recovery (DR) can be even higher. The costs of downtime in 2016 ranged from a minimum of $926 per minute to a maximum of $17,244 per minute, with an average cost of close to $9,000 per minute of outage.

Those costs can completely cripple a business; Gartner found that only 6 percent of companies remain in business two years after losing data. Creating an effective disaster recovery plan is a key step to ensuring business survival.

The Elements of a Disaster Recovery Plan

A disaster recovery plan goes far beyond backing data up to tape. That's a necessary step, but recovering business operations requires more than restoring from last night's backup. Your disaster recovery plan is about restoring business operations, not just about restoring data. It should be a comprehensive guide with the detailed instructions you need for recovering virtual machines, applications, data, and business operations. The more complete the guide, the less you'll need to figure out during the crisis.

Servers and virtual machines: The DR guide should have a comprehensive list of the servers and VMs, along with critical configuration details.

Applications: You should also have a comprehensive list of the applications to be recovered. Document the startup processes fully, including any dependencies to ensure they are restarted in the correct sequence. If possible, provide an estimate of the restart time to help with monitoring the recovery process.

Data: Your DR plan should specify how data will be recovered. You're likely to have lost transactions due to the outage or have transactions that were incompletely processed. Document any manual procedures needed to identify gaps and recreate the missing data.

Business: Business users will need to be informed of changes in their normal procedures, perhaps because they need to access systems from a different URL, because some applications will be up with limited functionality, or because some systems won't be available at all. There may be manual procedures for doing some business before systems are recovered or after they're back online. Document all these new procedures for the business team, as well as the process for informing them when the new procedures are in effect and when normal operations have resumed.

Beyond the detailed technical instructions, the DR plan should include all the contact information needed to inform your organization and partners about the disaster. This includes the technical team needed to bring systems back online, the business teams affected by the outage, and any vendors or other third parties affected by your unplanned downtime.

Finally, disaster recovery procedures usually bring limited services up on alternate, DR hardware. Your DR plan should include a fallback process for restoring normal business operations at your primary processing site.

Once your disaster recovery plan is written, make sure it's distributed throughout the organization. Everyone should know what their responsibilities will be when the plan is invoked.

Test Your Disaster Recovery Plan

No disaster recovery plan ever works exactly according to what's written on paper. That's why it's important to do a test of the plan, allowing you to identify flaws and gaps in the plan before the disaster situation occurs.

At a minimum, you should do a table walkthrough of the plan, where the people who will be involved in executing the plan read through the document together to make sure the plan is complete and to correct errors and omissions.

The most thorough, but most complex approach to testing a DR plan is to shutdown the production systems and actually execute the failover process. This approach has the benefit of confirming the estimated timing of the recovery process as well as the validity of the documented procedures. If the business team is involved in the test and certifies they can complete a day's work after failover process is done, this robust test offers a high level of assurance that the DR plan is complete and workable—for now.

There should be a review after each DR test to evaluate how the recovery process worked, and the DR plan should be updated correct any problems identified during the test. It should also be updated throughout the year, and testing needs to be repeated, as new systems are brought online and older systems are retired.

VAST
IT without Limits™

10 Things to Do When Disaster Strikes

1

Declare a disaster.
As part of your DR planning, you should have identified managers who will assess the situation and determine that invoking the DR plan is necessary.

2

Send out notifications to all necessary parties.
Everyone who's impacted by the disaster needs to be informed of the situation.This goes beyond the tech teams who will fix the problem to also notifying the business users, your external partners, and potentially your legal and insurance contacts.

3

Assess the situation.
Not all disaster situations require executing the full DR plan to get operations back on track. Before any recovery procedures are performed, the team should review the status of all systems and determine the scope of the necessary recovery procedures.

4

Execute your DR plan.
Make sure everybody on the team is working from the latest version of the DR plan. Focus first on getting the critical networks and critical business applications up and running. Follow your plan carefully and make sure you've got good communication lines for sharing updates and working out issues.

5

Validate the system and turn it over to the business.
After doing a technical checkout of the recovered applications, turn the systems back over to the business. Make sure they're aware of any differences in procedures or capabilities when using applications at the DR site.

6

Monitor status and support users.
Business users may need to access the systems through unfamiliar processes when the systems are running in recovery mode, and they may encounter issues such as limited functionality and transactions that weren't fully saved when the disaster occurred. Be prepared with help desk and other support to get all users working and business data consistent.

7

Determine that the disaster is over.
Have a strategy for determining that the disaster is over and that you can start falling back to your primary site. This decision should be made by senior management, similar to how the decision to invoke the DR plan was made.

8

Execute steps to fall back to the primary site.
Restarting services and applications at the primary site can be as complex as the transition to the DR site was. Many of the same steps for migrating data, applications, and users will need to be followed; your DR plan should provide full details of this process. All systems need to be thoroughly tested before business operations resume. Unless you plan to run both sites in parallel for some time, the process should also include steps for safely shutting down the DR site.

9

Monitor status and support users.
Plan to have extra support coverage and keep a close eye on the systems for a day or two following the resumption of normal services.

10

Assess your DR response and update the DR plan.
No matter how detailed and comprehensive your DR plan is, reality never matches expectations. Schedule a review with the team to identify shortcomings and issues with the DR plan and make sure it's updated to reflect problems, solutions, and system configurations you encountered while resolving the current crisis.

VAST
IT without Limits™

7 Challenges When Executing a Disaster Recovery Plan

Even when a DR plan is written to be comprehensive, even when it's been through a detailed test, recovering systems is never as simple as following the script. The first problem is making sure everyone is working from the same version of the plan. Then you'll likely encounter other challenges including:

1. Deciding whether to follow all or just part of it. Small disasters happen much more frequently than big disasters. That means that the scope of the complete DR plan may be much broader than the scope of the disaster. Deciding to follow the full DR plan may mean a lot of unnecessary work, but executing just a subsection—or inventing a smaller, minimal recovery process on the fly—can introduce new risks.

2. The contact list is out of date. Being able to reach key participants is crucial to executing a DR plan effectively. But people leave the company, change their responsibilities, or are away on vacation when disaster strikes. Having pre-identified backups for each recovery role can help mitigate this risk.

3. Systems have changed since the DR test. If system configurations have changed since the DR plan was written and tested, the documented steps for bringing them online may no longer be correct. There may be entirely new, critical systems that aren't addressed by the DR plan.

4. The disaster recovery site doesn't match the primary site. If your process requires failing over to a secondary site, the secondary site needs to be kept in synch with the production site for the process to work. It's all too easy for patches and system updates to applied only at the primary site, leaving the secondary site out of date.

5. The data volume's grown since the plan was written. Your estimates of the time required to recover are based on the size of the applications and data when the DR plan was written. If your business and transaction volume has grown since then, restoring data and recovering applications can take longer than you estimated and leave your systems down longer than you expected.

6. You lose data. If you need to restore from last night's backup, you'll lose all transactions executed today. Even a replicated database may be missing the last few minutes of data.

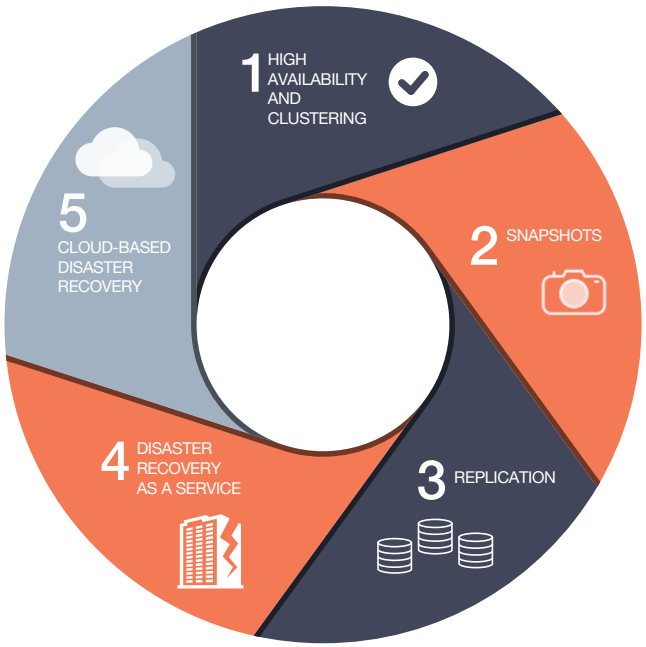
7. Falling back to the primary site is as complex as failing over to the DR site. In most cases, you'll want to call an end to the disaster and resume operations at your normal production site. Managing that process can be as complex as the initial response to the disaster.

VAST
IT without Limits™

Technology Choices to Make Disaster Recovery Easier

A traditional disaster recovery strategy requires maintaining a secondary site at a different location sometimes kept up and running as a hot standby location. Because this is very expensive, it's important to consider other options that can be more effective and, barring total disaster, enable you to continue operations at your primary data center.

These choices include:



- High Availability and Clustering
  With automatic failover capability, clusters enable processing to resume with minimal disruption when a single node fails.

- Snapshot
  Database snapshots on local storage enable rapid recovery from the loss of a database. Because the snapshot resides on the local server, it supports recovery only in limited circumstances.

- Replication
  Near real-time processes copy database updates to a backup database server either in the same data center or off-site. It's important to recognize that replication does not provide full disaster recovery capabilities; if the primary database is corrupted due to malware or user error, the same corruption will be replicated to the backup server. It's also possible to replicate VMs, allowing faster recovery of the applications running on that server.

- Cloud-Based Disaster Recovery
  Companies that build their secondary environment in the cloud can reduce the cost of maintaining a backup data center. With pay-per-use pricing, cloud DR means minimal costs when the secondary VMs aren't running. You can use the cloud as the backup site for your data and also replicate VMs to cloud servers.

- Disaster Recovery as a Service
  Like cloud-based DR, Disaster Recovery as a Service (DRaaS) uses the cloud as the backup data center. But rather than your company managing its own fail over process, the cloud provider offers a suite of services that coordinate and execute the failover to the DR environment. Through highly automated processes, DRaaS streamlines the recovery process and minimizes the risk of human error when manually executing an unfamiliar process.
  DRaaS allows companies to leverage the expertise and support of the cloud provider to make their disaster recovery successful.

By leveraging the capabilities of a DRaaS provider, companies can gain a reliable disaster recovery process and these benefits:

- expert support
- rapid implementation of a DR environment
- automated, rapid recovery process
- reduced capital expenditure and low, pay-per-use cost
- professional support and maintenance of the DR environment
- your staff freed to focus on other business-critical activities

Implement An Effective Disaster Recovery Solution

Start designing your disaster recovery solution by evaluating your needs and recovery objectives. You may choose to implement multiple disaster recovery solutions, combining strategies to address different kinds of failure and enable recovery both on site and off site depending on the scope of the disaster.

If you decide to use DRaaS, be sure to evaluate providers carefully from a technical as well as cost perspective. You should evaluate the scope of their offering, their support for your hypervisor, and their track record. Consider the level of automation they provide for starting your applications on their servers during a disaster, how easy it is to scale your DR environment as needed, and how easily you can run a DR simulation in their cloud. Because getting your data to the cloud is the key to recovery, be sure to assess how that data replication will occur and whether it will happen in real-time.

VAST Service

The team of experts at VAST can help your organization analyze your disaster recovery priorities, design and implement an effective solution, and then manage and monitor your DR environment on an ongoing basis. Leverage these services to provide the level of DR support your organization needs:

- Managed NetBackup. While backup isn't a full disaster recovery solution, no DR process is complete without the ability to restore data from backups. Our managed NetBackup service uses industry-leading Veritas NetBackup software and appliances to ensure that your backup process is complete and reliable.

- Infrastructure as a Service and Managed Amazon Web Services. Use IaaS or managed Amazon Web Services to build your backup data center in the cloud.

- Disaster Recovery as a Service. Our DRaaS offering builds on Amazon Web Services to provide comprehensive support when you need to transition applications to the cloud.

Contact the team at VAST to discuss which disaster recovery alternative offers the best protection for your business.

VAST

1319 Butterfield Road, Suite 504
Downers Grove, IL 60515

Phone: 630-964-6060
Toll Free: 800-432-VAST

info@vastITservices.com

www.vastITservices.com