

# Best Practices for Disaster Recovery of Virtualized Environments

There is no such thing as being too prepared for a disaster. In fact, according to a Disaster Recovery & Business Continuity Survey<sup>1</sup> conducted by Evolve IP in 2016, less than half of IT professionals feel that their organizations are “very prepared” for disruptive events. It follows that the prevailing majority of businesses are putting their operations in serious jeopardy.

Disasters do not refer exclusively to natural catastrophes, and may be caused by a variety of incidents, such as hardware failures, power outages, human errors, deliberate attacks, software failures and other events. Given that, any business is a potential victim of possible unpredictable circumstances.

According to Statista<sup>2</sup>, downtime is considered to be one of the biggest IT expenses that a business can experience in the event of a disaster – the cost of which accounted for over 5 million USD per hour for 14% of businesses in 2017. According to the same report, the majority (24%) of businesses worldwide reported that the average hourly downtime cost them between 301 and 400 thousand USD.

Furthermore, annual statistics provided by ITIC<sup>3</sup> indicate that the average cost of an hourly disaster has increased by at least 30% over the last 10 years, and this trend is not likely to be reversed, putting businesses under even greater financial risks in the future.

As a consequence of disaster, downtime does not only equal financial losses but can also entail other severe consequences, such as:

- > Loss of data
- > Inaccessibility of business-critical applications and information
- > Productivity loss
- > Inability to deliver services
- > Damaged business reputation
- > Customer retention issues
- > Loss of business to the competition
- > Bankruptcy

While no company is immune to disasters and their consequences, there are still options for mitigating the risks of disasters and ensuring a company’s survival. Unfortunately, only a very small percentage of disasters can be foreseen. However, by having proper strategies, resources, and tools in place, the consequences and impact of disruptive events can be minimized in order to ensure rapid and effortless recovery.

This white paper discusses the best practices and strategies for disaster recovery of virtualized environments. Furthermore, it introduces a new cutting-edge disaster recovery functionality (NAKIVO Backup & Replication’s Site Recovery) that, when used together with the practices and strategies, can grant businesses a guaranteed recovery under the shortest recovery time objectives.

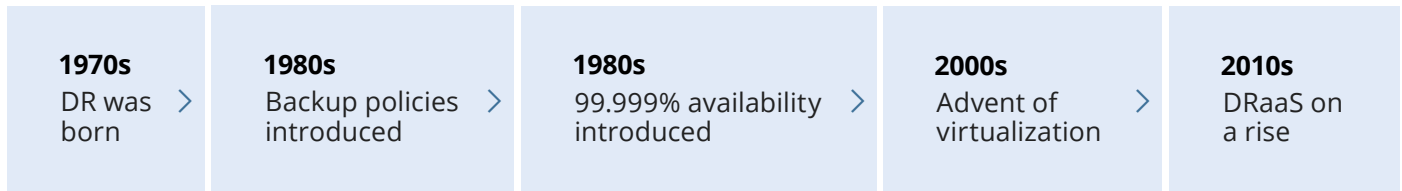
<sup>1</sup> “2016 Evolve IP Disaster Recovery & Business Continuity Survey”, Evolve IP (2016)

<sup>2</sup> “Average Cost Per Hour of Enterprise Server Downtime Worldwide in 2017 and 2018”, Statista (2017)

<sup>3</sup> “Cost of Hourly Downtime Soars: 81% of Enterprises Say it Exceeds \$300K on Average”, ITIC, (2016)

# What Is Disaster Recovery?

**Disaster recovery** (DR) involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster<sup>4</sup>.



Disaster recovery dates back to the 1970s, when the rapid rise of digital technologies led to the first technological failures. Back then disaster recovery emerged as a business, with the first disaster recovery firms basically offering organizations alternative locations to resume their operation when disaster struck.

During the 1980s and 1990s, along with the increasing dependence of businesses and organizations on their IT infrastructures, the US government introduced regulations that obligated national banks to have backup plans. Other industries gradually followed this trend. In the late 1990s and early 2000s, the dependence of businesses on their IT infrastructures, their uninterrupted operation, as well as disaster awareness continued to grow. The newly-introduced concept of five nines (99.999%) availability started to become an objective for an increasing number of organizations.

The late 2000s saw the advent of server virtualization, which made the recovery process and procedures significantly faster, winning over the backup-to-tape recovery method as well as revolutionizing the disaster recovery industry as a whole. The widespread adoption of virtualization technologies in modern IT infrastructures resulted in the emergence of new solutions that were designed to cater to the data protection and recovery needs of businesses that used virtualized environments.

In the 2010s, with cloud computing on the rise, traditional cloud services were offered along with a new type of service – disaster recovery as a service or DRaaS. DRaaS introduced businesses to multiple benefits, including better protection, flexibility, and affordability. NAKIVO, a fast-growing virtualization and cloud backup software company, released the first version of NAKIVO Backup & Replication in 2012. Over the past six years, the software has evolved into a complete disaster recovery solution for virtualized environments, offering DRaaS functionality in particular.

At NAKIVO, disaster recovery is recognized as a process or procedure of returning virtual infrastructure to a fully operational state with minimal data loss and interruption. The concept generally refers to specific steps that are to be taken in order to handle and recover from disruptive events. The backbone of modern disaster recovery strategies is formed by backup and replication technologies, which underpin NAKIVO Backup & Replication.

<sup>4</sup>Definition from Wikipedia

# Core Concepts and How They Overlap

In the disaster recovery domain, there are three core concepts that are interconnected and often used interchangeably. These are **business continuity**, **disaster recovery**, and **high availability**. These concepts have unique meanings but still happen to create confusion and misconceptions. It is important to distinguish between the three in order to understand the roles and objectives of each.

## Business Continuity

Business continuity (BC) is a broad term that refers to an organization's capability to plan processes and measures in order to resume normal business operations during and after disaster or other disruptive events. BC is business-centric and is aimed at reducing possible downtimes to a minimum or, in a perfect world, completely avoiding interruptions, and delivering 24/7 uptime.

## Disaster Recovery

Unlike BC, disaster recovery (DR) is data- and technology-centric. It is a set of procedures, in which the objective is to recover data and get IT infrastructure and components up and running after disaster. The faster the organization recovers its systems from disaster, the faster such organization can resume normal operations. It is for this reason that DR is considered a subset of business continuity, and a key aspect in BC planning.

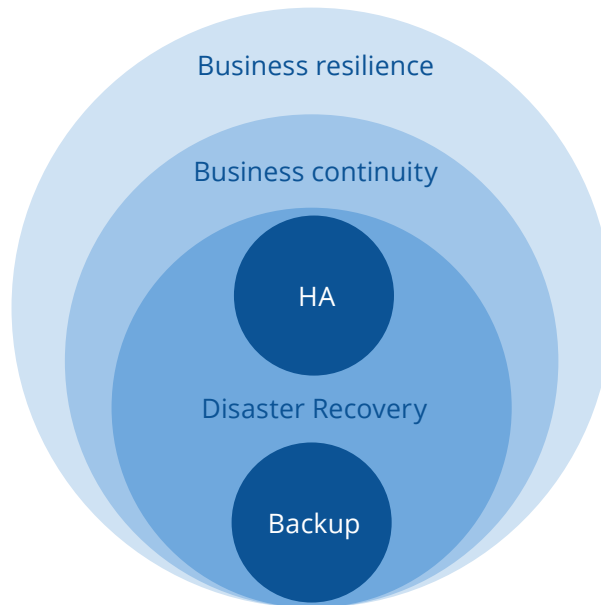
## High Availability

High availability (HA) is a concept that is often confused with both DR and BC. HA is a characteristic of a system or components to deliver the highest level of operational performance or 100% operational uptime. HA manifests itself only through technology and is usually achieved through the implementation of redundant and fault-tolerant components. The concept focuses exclusively on uptime, helping achieve a standard of 5 nines (99.999%) availability. HA does not guarantee recovery from disasters and does not prevent data loss, but disaster recovery can and should include high availability in its technological design.

The three concepts are not interchangeable but rather interdependent. To achieve business continuity, businesses must devise a solid data recovery strategy, while high availability should be included in this strategy as an integral part of the organization's technological design.

In some cases, a term such as "backup" is also mistakenly used as a substitute for disaster recovery. However, disaster recovery is not limited to backup since this technology is merely one component of a much larger process. Backups are integral to disaster recovery and cannot be used in isolation.

Another popular term used interchangeably with DR and BC is business resilience. By some industry experts, business resilience is considered as the next step after business continuity; in other words, to achieve resilience businesses must first deliver business continuity.



## Disaster Recovery Best Practices

Although considered rare, natural disasters cost the US 306 billion US dollars in 2017<sup>5</sup>. In addition to this, operational and man-made disasters take place frequently and are inevitable. Disasters have evolved over time (e.g., deliberate attacks are becoming more sophisticated) and, according to statistics, are on a rise. The odds of falling a victim to disaster at any time are also increasing. This necessitates having a well devised and thorough disaster recovery strategy, which is based on time-proven disaster recovery practices outlined below.

### Defining the Scope and Dependencies

Businesses that rely on virtualization technologies use VMs to run nearly every component of their infrastructures – servers, databases, ERPs, CRMs, applications, and so on. While some of the VMs are critical to ensure uninterrupted business operations, others, for example, can be used as file storage or for testing purposes.

<sup>5</sup>“Weather Disasters Cost the U.S. a record \$306 Billion in 2017”, Bloomberg (2018)

IT managers should work closely with each department to identify critical business services, VMs housing supporting applications for such services, and other VMs that are required for uninterrupted delivery of such services. Failing to include at least one link of the dependency chain to the recovery scope can be detrimental.

Business-critical VMs are of top priority; they require to be thoroughly monitored for failure, and should be replicated or backed up regularly. Less important VMs can be excluded from the recovery scope in order to achieve shorter RTOs.

## Identifying Responsible People & Staff Training

One of the key elements of successful disaster recovery is having a team that is responsible for recovery and proper staff training. This holds especially true for large organizations. Involving numerous people and ensuring that more than one person is aware of what recovery steps to take in the face of disaster leaves less room for failure and increases the chances of successful recovery.

## Remote Site Configuration

Having a secondary location ensures that you do have IT resources and data for restoration when disaster strikes. Best practices dictate that the secondary site should be located away from the primary site in order to prevent it from rendering unavailable by the same disaster or outage.

IT managers should clearly define hardware requirements for the secondary site in order to exclude the possibility of recovery bottlenecks. Since the workloads are going to be entirely or partially moved to the secondary location, you should have enough CPU, RAM, and storage space in place to run replicated VMs as well as store backups. Otherwise the VMs on the secondary server may lag and may not ensure sufficient performance for running business-critical services. Insufficient disk speed significantly reduces VM performance.

## Establishing the Right RTO and RPO

It's crucial to calculate for how long your IT services can be down without serious consequences to business, and how much data you can tolerate to lose. These numbers represent recovery point objective (RTO) and recovery time objective (RPO). Different VMs can be assigned different RTO and RPO values depending on how critical such VMs are for business operation.

For example, a corporate email system must be restored as soon as possible because internal emails contain important data, and a system's failure affects internal communication. Thus, there is no tolerance for downtime and data loss – both RTO and RPO should be minimal. A file server that is used to store annual reports from previous years can survive a longer RPO and RTO.

## Regular Testing and Optimization

Having properly established and documented DR workflows for multiple disaster scenarios does not guarantee successful recovery. DR workflows can only be considered reliable and effective after being rigorously tested for weaknesses. Oftentimes organizations overlook the importance of regular DR testing, and find themselves unable to complete the recovery process when actual disaster hits.

Your DR workflows should be optimized, revised, and updated on a regular basis to reflect all of the changes and implementations that take place in your infrastructure. Even minor changes in the infrastructural architecture and configuration can translate into vulnerabilities in the recovery workflow, which increases the likelihood of failure.

## Automation of Disaster Recovery Activities

In most cases, modern DR solutions provide for the automation of DR workflows and processes, allowing businesses to gain multiple benefits. Aside from being a strong timesaving technique that helps reduce manual effort, execution complexity, and recovery time; automation also helps you to benefit from another perspective. By automating key DR activities, you can significantly reduce the risk of human errors that most manual processes are prone to.

# Fulfilling DR Best Practices with NAKIVO's Site Recovery

## Site Recovery Overview

NAKIVO Backup & Replication is a robust and reliable backup and disaster recovery solution with built-in Site Recovery functionality. This feature allows you to automate and orchestrate the entire disaster recovery process, perform testing of DR workflows, run planned as well as emergency failover and failback, and simplify data center migration.

Site Recovery is designed to help businesses achieve continuous availability and uninterrupted operation by putting DR on auto-pilot. You can easily build automated recovery workflows (i.e., Site Recovery jobs) by combining available actions (start or stop VMs/instances; failover or failback VMs/instances; run, stop, enable, or disable jobs; wait; send notifications, etc.) and adding conditions.

Any of the created DR workflows can be run in either production or testing mode. The former is used specifically in the event of actual disaster, while the purpose of the latter is to assess the validity and efficiency of such workflows before disaster hits. You can also easily update and optimize DR workflows if needed in order to make sure that they deliver the desired outcomes, RTOs, and RPOs.



## Site Recovery Features

The Site Recovery functionality allows you to create automated DR workflows of different complexity levels depending on your objectives, and in order to fit multiple recovery scenarios. For instance, you can create simple monitoring jobs that will check the condition of your critical VMs on schedule and send you email reports. You can also build comprehensive workflows with multiple steps, including failover and failback of your entire infrastructure, once disaster hits.

The feature is intuitive and easy-to-use, requiring little to no technical expertise. It only takes five steps to create a Site Recovery job:

**At the first step**, combine actions from the given list to create a recovery sequence. The list includes the following actions:

- › Failover VMware VMs/Hyper-V VMs/EC2 instances
- › Failback VMware VMs/Hyper-V VMs/EC2 instances
- › Start VMware VMs/Hyper-V VMs/EC2 instances
- › Stop VMware VMs/Hyper-V VMs/EC2 instances
- › Run or stop jobs
- › Run script
- › Attach or detach repositories
- › Send email
- › Wait
- › Check condition

In case your DR workflow includes **Failover** or **Failback** actions, the software may suggest to enable Network Mapping **at step two**. By enabling Network Mapping, you can make sure that VMs are connected to the right network upon failover (or failback). However, if you had Network Mapping enabled during the primary replication job, you can choose existing rules from the list.

**At the third step**, the solution suggests to set Re-IP rules in order to assign new IPs to replicas at the secondary location. Similarly, you can choose Re-IP rules used during the primary failover (or failback) job.

**At step four**, you can select scheduling options for your Site Recovery testing. Virtual infrastructures are prone to frequent changes and updates, making the testing of DR workflows crucial for the actual DR process to be successful. NAKIVO Backup & Replication allows you to test your DR workflows as often as needed in order to be well-equipped in the case of unpredicted events.



**At the final step**, you can set desired RTOs for your Site Recovery jobs, which can give you better understanding on how your workflows perform during tests, and how to improve their efficiency in the future.

## Site Recovery Benefits

The Site Recovery feature introduces multiple benefits – it opens new opportunities and capabilities that were previously unavailable for many SMBs as well as larger organizations.

**Comprehensive Site Recovery workflows:** By using NAKIVO Backup & Replication, users are able to create multiple Site Recovery jobs that can include up to 200 actions. This allows the product to serve different purposes (e.g., monitoring, data center migration, emergency failover, planned failover, failback, etc.) and cover complex disaster recovery scenarios. All of the workflows can be updated and optimized at any time to comply with changes in the infrastructure, or for better DR performance.

**Ease of use:** According to Arcserve<sup>6</sup>, almost 40% of IT professionals believe that DR solutions are too difficult to use. NAKIVO recognizes that complexity of a solution might cause confusion and unnecessary delays in the recovery process. Although being a high-end DR feature, NAKIVO Backup & Replication's Site Recovery merely requires the completion of five simple steps, while offering an intuitive and user-friendly interface, which contributes to faster recovery and requires no effort on the user's part to master the solution.

**Non-disruptive testing:** NAKIVO Backup & Replication allows you to perform regular testing of DR workflows in order to exclude possible weaknesses that could compromise the whole DR procedure in the event of actual disaster. You can verify the validity and efficiency of your Site Recovery jobs before any unexpected event catches you off-guard – and you can make sure that you are able to recover within your RTOs.

**Recovery in one click:** With NAKIVO Backup & Replication in place, the only thing users have to do in a case of disaster is hit a button in order for the selected DR workflow to immediately be put into action. Infrastructures of any scope can be restored in a single click, which helps our users achieve peace of mind and gain confidence in recovery, with minimal losses and the shortest downtimes.

**A one-box solution:** Site Recovery functionality is built into NAKIVO Backup & Replication, augmenting its comprehensive feature set with no additional licensing. This way, aside from features for performing routine data protection tasks, users also get an additional advanced disaster recovery functionality in a single box.

<sup>6</sup>"State of Disaster Recovery 2016", Arcserve (2016)

**Unbeatable pricing:** According to the same survey conducted by Arcserve, 54% of IT pros consider pricing for DR solutions to be too high. With NAKIVO Backup & Replication, having a DR solution is not a luxury but an affordable and wise investment for businesses of any size. By offering flexible and reasonable per-socket pricing, NAKIVO Backup & Replication can dramatically reduce the cost of data protection and site recovery.


## Conclusion


The nature and causes of disasters vary, making any organization a potential victim of unpredicted events – the consequences of which can affect an organization’s financial health and could cost them their reputation as well as their clients. Being under the constant threat of disaster, businesses cannot overlook the importance of having an effective DR strategy, tools, and resources. However, the cost, complexity, and unreliability of modern DR solutions often become the reason for not incorporating them into a business.


NAKIVO has introduced high-end Site Recovery functionality to make DR affordable and effortless for businesses of any scope. By following time-proven DR practices and including NAKIVO Backup & Replication in their recovery strategies, businesses can achieve a significantly higher level of DR preparedness and deliver 24/7 availability of services.


# NAKIVO Backup & Replication at a Glance


NAKIVO Backup & Replication is a fast, reliable, and affordable VM backup solution. The product protects VMware, Hyper-V, and AWS EC2 environments. NAKIVO Backup & Replication offers advanced features that increase backup performance, improve reliability, and speed up recovery.


- 

**Deploy in under 1 minute**  
Pre-configured VMware VA and AWS AMI; 1-click deployment on ASUSTOR, QNAP, Synology, WD NAS, and NETGEAR; 1-click Windows installer, 1-command Linux installer
- 

**Reduce backup size**  
Incremental backups with CBT/RCT, LAN-free data transfer, network acceleration; up to 2X performance when installed on NAS
- 

**Protect VMs**  
Native, agentless, image-based, application-aware backup and replication for VMware, Hyper-V VMs, as well as AWS EC2 instances
- 

**Decrease recovery time**  
Instant recovery of VMs, files, Exchange objects, SQL objects, Active Directory objects; automated Site Recovery
- 

**Increase backup speed**  
Exclusion of swap files and partitions, global backup deduplication, adjustable backup compression
- 

**Ensure recoverability**  
Instant backup verification with screenshots of test-recovered VMs; backup copy offsite/to the cloud

## About NAKIVO

The winner of a “Best of VMworld 2018” and the Gold Award for Data Protection, NAKIVO is a US corporation dedicated to developing the ultimate VM backup and site recovery solution. With 20 consecutive quarters of double-digit growth, 5-star online community reviews, 97.3% customer satisfaction with support, and more than 10,000 deployments worldwide, NAKIVO delivers an unprecedented level of protection for VMware, Hyper-V, and Amazon EC2 environments.

As a unique feature, NAKIVO Backup & Replication runs natively on leading storage systems including QNAP, Synology, ASUSTOR, Western Digital, and NETGEAR to deliver up to 2X performance advantage. The product also offers support for high-end deduplication appliances including Dell/EMC Data Domain and NEC HYDRAsstor. Being one of the fastest-growing data protection software vendors in the industry, NAKIVO provides a data protection solution for major companies such as Coca-Cola, Honda, and China Airlines, as well as works with over 3,000 channel partners in 137 countries worldwide. Learn more at [www.nakivo.com](http://www.nakivo.com)

