Stop Fearing a Disaster by Preparing a Disaster Recovery Strategy

by Alan Alvarez

INTRODUCTION

Are you responsible for making sure your operational systems are always online? Are you worried about what would happen if your main customer transaction system goes down? So, you already have a DR strategy to protect you against a system failure, but are you convinced it will work as expected when the time comes?

These are fair questions to ask yourself. This means you are cautious and want to understand the steps necessary to make sure you have a robust environment.

The first thing to understand is what is the consequence or the cost of a disaster, then the type of disaster that you need to prepare for, and finally identify the systems that need to be replicated. Once you gathered the necessary risk information, then you can begin planning for a robust disaster recovery strategy. This brief article along with its accompanied white paper will help you navigate and build a solid disaster recovery strategy.

What is the cost of a disaster and what are the types of disasters?

There are many different types of disasters and most of them fit into 3 categories. Disasters can be natural, man-made, or human-error. Each disaster can be covered by different strategies, or the same strategy can prevent all types. DR strategies will be covered later in the paper

Natural Disasters

A natural disaster is an event resulting from earth's natural hazards. Examples of natural disasters are floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, draughts, meteoroid strikes, and landslides

Man-Made

Man-made disasters are the consequence of technological or human hazards. Examples include riots, terrorist attacks, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation, and acts of war.

Human Error

Human Error disasters result from the intentional or un-intentional disruption of a system. Examples of human errors are shut down of servers, corruption of operating systems, hacking, deletion of applications or data, and changes to infrastructure that result in an outage.

GETTING STARTED

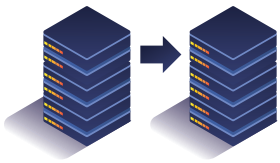
There are many factors to consider when planning and designing a DR Strategy. First you need to identify the risk of a system failure and what is the impact of that failure. Then you need to identify what are the pieces that need to be replicated and restored. You will need to choose your DR location strategy, what technology to use, how to orchestrate all environments, and how to return to normal.

A disruption of service can include a failure of a server node, corruption of an operational system, or a complete loss of a data center. During the assessment, a full analysis will run of your organization's existing infrastructure and recommend the most cost effective and robust backup solution. Next, the consultant will walk you through many factors to consider when planning and designing a DR strategy.

1. Identify the risk of a system failure and what is the impact of that failure.
2. Identify what are the pieces that need to be replicated and restored.
3. Choose your DR location strategy, what technology to use and how to orchestrate all environments.
4. Return to your normal operations.

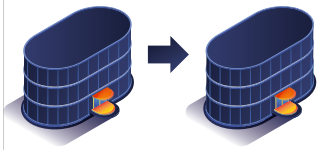
By using industry leading disaster recovery tools and best practices in the market and matching it up to your IT system requirements will ensure that your DR environment matches your RTOs, RPOs and SLAs.

Disaster Recovery Target Locations



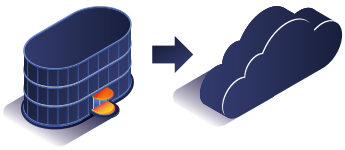
Server to Server

- Node
- Rack
- Partial Data Center
- Partial Network Components



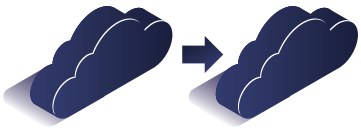
Data Center to Data Center

- Node
- Rack
- Partial Data Center
- Partial Network Components
- Data Center Network
- Complete Data Center



Data Center to Cloud

- Node
- Rack
- Partial Data Center
- Partial Network Components
- Data Center Network
- Complete Data Center
- Multiple areas of availability
- Manage-less DR
- More cost effective



Server to Server

- Node
- Rack
- Partial Data Center
- Partial Network Components
- Data Center Network
- Complete Data Center
- Multiple areas of availability
- Manage-less DR
- More cost effective
- Region

This graphic represents the type of target locations of a DR strategy. Depending on the risk/cost evaluation, a DR site can be within the same data center, separate data center, or a public/private cloud.

Disaster Recovery Target Types

Active - Passive Cold

- Target system is off
- Data is restored from backup
- Single Licensing might be an option
- Longest RTO
- Longest RPO

Active - Passive Warm

- Target system is on
- Data is restored from backup or is stored in target file system
- DR licensing might be an option
- Longer RTO
- Longer RPO

Active - Active

- Target system is on
- Data is replicated to target application
- Mirror production licensing
- Shortest RTO
- Shortest RPO
- Load Balancing optional

This graphic represents the different types of DR target strategies, where the recovery target can be a resource that is either non-existent that can be commissioned on demand, it can be a stand-by system, or it can be a complete replicate of the production environment.

KEY FACTORS IN MAKING YOUR DECISION

There are more than just technical considerations when designing a DR strategy. The main key factors when making your decision is easily broken down by the following factors.

Price

DR services will help you not only measure the cost of operational downtime, but also the cost of the overall solution. Does the cost of downtime justify the cost of the solution? We can help you answer that question. DR experienced architects will take cost into consideration when helping you design your DR strategy

Environment

Where should I host my DR site? What is my DR Strategy type? What tools will I use? These are questions that an IT consultant who specializes in DR can assist you.

Orchestration

Data between environments needs to be moved from location to location and be up to date as possible. When a disaster occurs your DR site needs to have up to date data and operations need to continue while the original system is brought back on-line.

Testing

To ensure that your DR environment is responsive and behaving as expected, planned and un-planned tests need to happen periodically

Recovery Speed

How long will it take for your DR site to take over operations? How long will it take to remediate the original environment, and how long can you return to normal operations?

Support

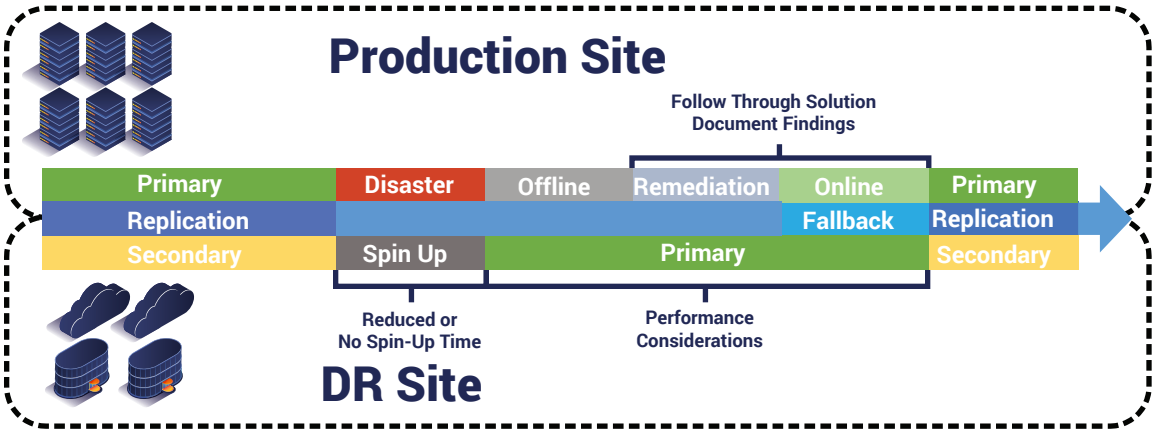
This is an important point for a DR strategy, who will monitor, manage, and remediate your infrastructure during a disaster?

Failback

Once the failed system is recovered, how will you restore it to normal operations?t

Astadia DRaaS Monitoring and Management

Astadia™ DRaaS
Where Enterprise Meets Clouds



This graphic represents the DR process and how Astadia Managed Services can monitor and manage your DR strategy

The DRaaS Approach

Disaster Recovery can be resolved by using a comprehensive portfolio of services that enable business operations to continue to function in the event of any disruption of service. A disruption of service can include a failure of a server node, corruption of an operational system, or a complete loss of a data center.

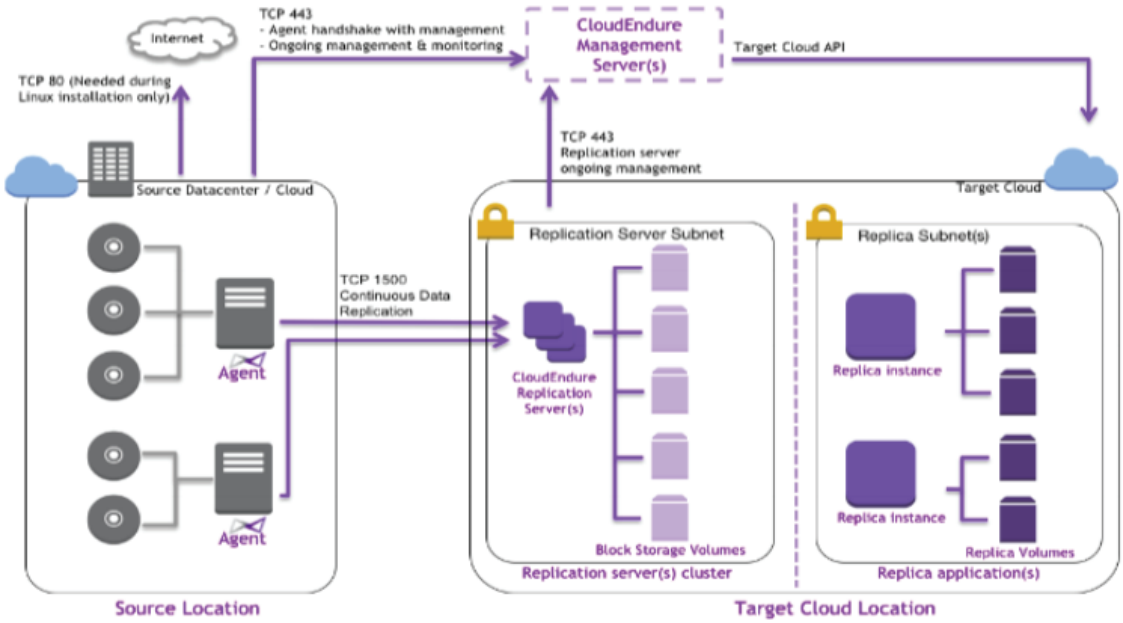
Operational downtime can severally impact a company's finances, loss of opportunities, and even loss of market share, so it is important to not overlook the importance of a Disaster Recovery strategy.

You should explore these critical factors to determine how they may apply to your own Disaster Recovery plan as well as IT infrastructure. Please email us any comments or questions at info@astadia.com and check out our blog at CloudGPS.Astadia.com for ongoing discussion and updates.

CloudEndure Partnershipt

Powered by CloudEndure Disaster Recovery allows you to use your cloud environment as an enterprise-grade business continuity/ disaster recovery (BC/DR) solution for your applications, commonly reducing total cost of ownership (TCO) by 80%+ compared to traditional Disaster Recovery as a Service (DRaaS) solutions, while improving recovery objectives.

CloudEndure maintains ongoing replication into a low-cost “staging area” located in a target region of choice, which reduces your compute, storage, and software licensing footprint to a minimum. In the event of a disaster, CloudEndure triggers an automated large-scale orchestration and system conversion process (p2c/v2c/c2c), recovering your database applications in minutes.



REMOTE MONITORING AND MANAGEMENT

The teams that manage the IT infrastructure and support all of your customers will use a set of defined and well tested industry processes and tools. These Managed Services ensure that customer IT infrastructure, databases and applications are designed, managed and operated on a 24 X 7 basis, ensuring a highly available and secure environment for business transactions. The managed services leverage IT Infrastructure Library (ITIL) based best practices providing services through integrated sets of processes and technologies. These are proven methodologies and should be supported by a strong Program Management Office and a dedicated Account Management team.

These teams continually strive to gain insight to your processes, and applies that knowledge to develop repeatable standardized and optimized support processes that reduce inefficiencies. This effective model allows you to realize cost savings through a continual focus on improvement.

DISASTER RECOVERY SERVICES

DR Consulting Services

Disaster Recovery 101

Business Value of a DR Solution
DR Strategy Design
Respond to alerts
Risk of Downtime Assessment

TCO of DR solution

Risk vs TCO comparison

Identify operational systems for DR

DR Design, Implement, and Test Services

DR Requirement Gathering

DR Strategy Design

TCO of DR Analysis

DR Implementation Services

Disaster simulation and recovery testing

DR strategy optimization services

DR Manage and Monitor

24x7 Monitoring and Management

Respond to alerts

Document causes of failure

Assist with remediation process

Failback to normal operations after remediation

CONCLUSION

If you haven't begun your journey with Disaster Recovery just yet, chances are that a cloud adoption project is in your near future. While the cloud has come a long way in a relatively short period of time, the services they offer continue to expand and offer new capabilities at an astonishing rate.

There are many success factors for cloud adoption that help ensure you achieve maximum return on your investment and we're glad to have shared several with you through this whitepaper. You have a long journey ahead of you and we'd encourage you to share it with travel companions from your community of customers, partners and employees.

Please feel free to reach out with any questions, comments or feedback to info@Astadia.com.

ABOUT ASTADIA

Astadia is a premier technology consultancy focused on maximizing the impact and minimizing the risks of today's blended enterprise and cloud ecosystem.

Our focus areas include:

- **Cloud Migrations** – Moving enterprise workloads to target cloud environments to optimize costs, improve reliability and free-up resources to focus on innovation.
- **Legacy Modernization** – Assess, identify and modernize mainframe-based applications and databases, whether through reuse, rewrite or replace.
- **Managed Services** – 7/24 visibility and support for the blended IT ecosystem, including enterprise, cloud and end users.
- **Cloud Development** – Design, build, test, secure and deliver great software for today's elastic, hyper-scale world.

Clients choose Astadia for our 25+ years of experience, our agility and our emphasis on delivering results that matter.

How can we help? We'd love to hear about your IT journey. Email us at Info@Astadia.com.