the BRAINTREE group

Planning for Disaster Recovery

The Best Practices

Table of Contents

Introduction 1

Acronyms 1

Checklist 1

Disaster Recovery Concepts 2

- Disaster Types 2
- Testing and Maintenance 2
- Roles and Responsibilities 3
- Physical Location 4
- Disaster Recovery Strategy Costs 5
- Criticality Level 5

Production Environment 6

- Network Infrastructure Diagram 6
- List of Servers 7
- List of IT Services 8

IT Disaster Recovery Solutions 9

- Online Backup – for a Cold Site DR Solution 9
- VM Backup in the Cloud – for a Cold Site DR Solution 10
- VM Replication – for a Warm Site DR Solution 11
- Mirroring – for a Hot Site DR Solution 12

Introduction

This document will provide information about how to build your DR plan, including the essential questions you should cover. It offers clues on how to identify the right solution according to your technical requirements. Proper Disaster Recovery planning identifies successful organizations as those which can manage a disaster with minimal cost and effort and maximum speed. The worst organizations are more reactive than proactive and deal with disaster randomly. They don't know how long it will take to recover and how much it will cost. Disaster Recovery planning goes beyond your IT department, so you need to plan for all departments in your organization. This document focuses on IT but also gives tips for your business as a whole.

Acronyms

Here are some acronyms used in this document:

DR	Disaster Recovery	Set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster
RTO	Recovery Time Objective	The targeted time duration and service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity
RPO	Recovery Point Objective	The maximum acceptable amount of data loss measured in time

Checklist

This checklist will help you build your Disaster Recovery Plan. We provide information to answer these questions further in this document.

- Which types of disasters could our company face?
- Where will our employees work if a disaster occurs in our building?
- What will be peoples' roles and responsibilities if a disaster occurs?
- Where will our new server room be located?
- How will we test and update our Disaster Recovery plan to be sure it works the day we need it?
- Which IT services are essential to our company and which ones are not?
- How long can we afford to wait before each of our IT services comes back online?
- How much data can we allow to lose until each of our IT services come back online?
- What is our exact server list?
- On which server(s) are our IT services running?
- Which technology will we use to recover our IT services?
- In what sequence will we execute recovery actions?
- Which people will we contact in case of a disaster?

Disaster Types

There are different types of disasters. Some cause more damage than others. You should prepare an extended list of disaster types that your company may face to ensure your plan covers them all. You may choose to ignore or mitigate some of them. Here are examples of disaster types: equipment failures, connectivity failures, floods, fires, storms, sabotage, terrorism, epidemic illness, power outage...

Testing and Maintenance

A Disaster Recovery plan prepares you to face disasters that could happen any time. To ensure your plan works as expected when a disaster occurs, you have to test it on a regular basis. It's important to add detailed test steps to your Disaster Recovery plan so you're more confident. Don't forget to update your plan every time there is a change in your environment. A test should be run shortly after a change is made to the plan. Here are example of tests you could run:

Walkthroughs: Team members go verbally through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DR supervisor to draw upon an increased pool of knowledge and experience. Staff should be familiar with procedures, equipment, and offsite facilities.

Simulations: A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in the simulation. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Parallel Testing: A parallel test can be performed in conjunction with the checklist or simulation test. In this scenario, historical transactions, such as those on the previous business day, are processed against the preceding day's backup files. This is done at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

Full-Interruption Testing: A full-interruption test activates the total Disaster Recovery plan. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. We cannot overstate the importance of due diligence with respect to previous phases of the Disaster Recovery plan.

Roles and Responsibilities

To elaborate your Disaster Recovery plan, you should identify roles and responsibilities. That way, you will build a Disaster Recovery team that involves all departments, with clear objectives on how to create your plan, update it, and execute it in a timely manner. You need to draw up a list of people and include their names, contact details and an alternate person in case they're not available. Here is an example of the kind of roles and responsibilities you'll need in that team. You could combine roles or adjust them to fit your organization.

DR Supervisor: His responsibility would be to coordinate the efforts of his team's members and ensure an efficient DR plan is in place, up to date, tested and well executed in case of a disaster.

DR Planning Expert: If the CIO or designated project manager is not a DR planning expert, you should retain a firm or consultant to provide expert insight, guidance, suggestions and technical oversight. This helps ensure that industry best practices and compliance requirements are covered, risks are adequately managed and outlays are kept in line with potential losses and exposures. This is an expert advisory role, and necessary only when the team head lacks such expertise.

Business Unit/Operations Stakeholders: Representatives throughout all areas of the company must be included in the recovery team to identify the key systems, services and infrastructure elements they need for recovery. They must also assess recovery testing results to see if such needs are met (and to identify and help correct oversights, omissions, errors and so forth) and to help establish Recovery Time Objectives (RTOs).

Network and Infrastructure Delivery: Key members of IT, voice, networking and infrastructure organization who will be involved in specifying communications and networking capabilities for recovery. They must also be involved in planning, maintaining and testing the business continuity/Disaster Recovery plan and implementation.

IT Systems and Services: Designated system experts who will be responsible for bringing systems and services back into operation during recovery must also participate in planning, maintaining and testing the DR plan.

Other Support Staff as Needed: Trainers, writers and support staff can provide expert help in preparing DR plan documents and training team members in their specific roles. They must also provide the documents, how-to guides and checklists team members will use to guide their work, check their results and document those results for later analysis.

Here is a sample table listing roles and responsibilities:

- The Primary contact column displays the name and phone number of the person playing the role.
- The Role column indicates which role that person is playing in the team.
- The Responsibility column lists the duties linked to the person's role.
- The Backup contact column displays the name and phone number of the alternate person if the primary person cannot be reached.

Primary contact	Role	Responsibility	Backup Contact
Allen Glaton 514-555-4423	DR Supervisor	• Ensures the Disaster Recovery Plan is in place • Ensures the DR PLAN is always up to date • Makes sure the DR PLAN is tested • Coordinates the team during the recovery • Contacts the executives and officials	John Bacon 819-656-7865
Sam Valentine 819-553-1235	Accounting Director	• Ensures the DR PLAN covers the accounting department needs	Paul Yellow 450-321-4445
Todd Winter 450-666-5112	IT systems and services	• Evaluates technologies to be used in the DR plan • Tests the IT systems and services that are part of the DR PLAN • Brings systems and services back, executing the DR PLAN	Michael Felish 819-987-9991

Physical Location

You need to plan where your employees will work if a disaster happens in the office building. You need to determine how they will connect to the environment and with which equipment. If it involves a procedure your employees are not used to, you need to train them how to use servers and data during the disaster. You need to answer the following questions. If users need to work from an alternate location, how will they connect to the DR environment? Do you need to preconfigure a point-to-site VPN access? Do you have an alternate site where you can have a site-to-site VPN already configured? You should know that if your business is already hosting its applications in the cloud with Remote Desktop Services/RemoteApps/Desktop-as-a-Service, etc., it will be less trouble because your employees would be able to access their applications wherever there is an Internet connection. So you might consider hosting your application in a RDS setup in the cloud.

If you need to be in a special physical location to ensure that you are still compliant with your current certifications (like PCI, HIPAA, etc.), you have to make sure the Disaster Recovery supplier for your IT infrastructure is also compliant.

If you need physical access to the datacenter or a special connection on servers, like a USB key for licenses, confirm this beforehand with your Disaster Recovery supplier.

Disaster Recovery Strategy Costs

Different strategies exist for your IT Disaster Recovery plan. Consider these 3 types: cold site, warm site and hot site. In the ideal world, we would always take the strategy that allows all us to restore all services within minutes with no data loss. This is the hot DR site strategy, and it becomes costly to implement especially when you target smaller RTO and RPO for your recovery. In general, you can use a different DR strategy per IT service. That's why you have to evaluate how critical each service is. This will allow you to plan for business continuity with a reasonable budget.

Criticality Level

Here's how you can classify IT services per level of criticality.

Criticality Level	Service Failure in this Class Can Result in the Following:
Mission Critical	• Widespread business stoppage with significant impact on revenue • Risk to human health/environment • Public, wide-spread damage to the organization's reputation
Business Essential	• Direct impact on revenue • Direct negative customer satisfaction • Compliance violation • Non-public damage to organization's reputation
Business Core	• Indirect impact on revenue • Indirect negative customer satisfaction • Significant employee productivity degradation
Business Supporting	• Moderate employee productivity degradation

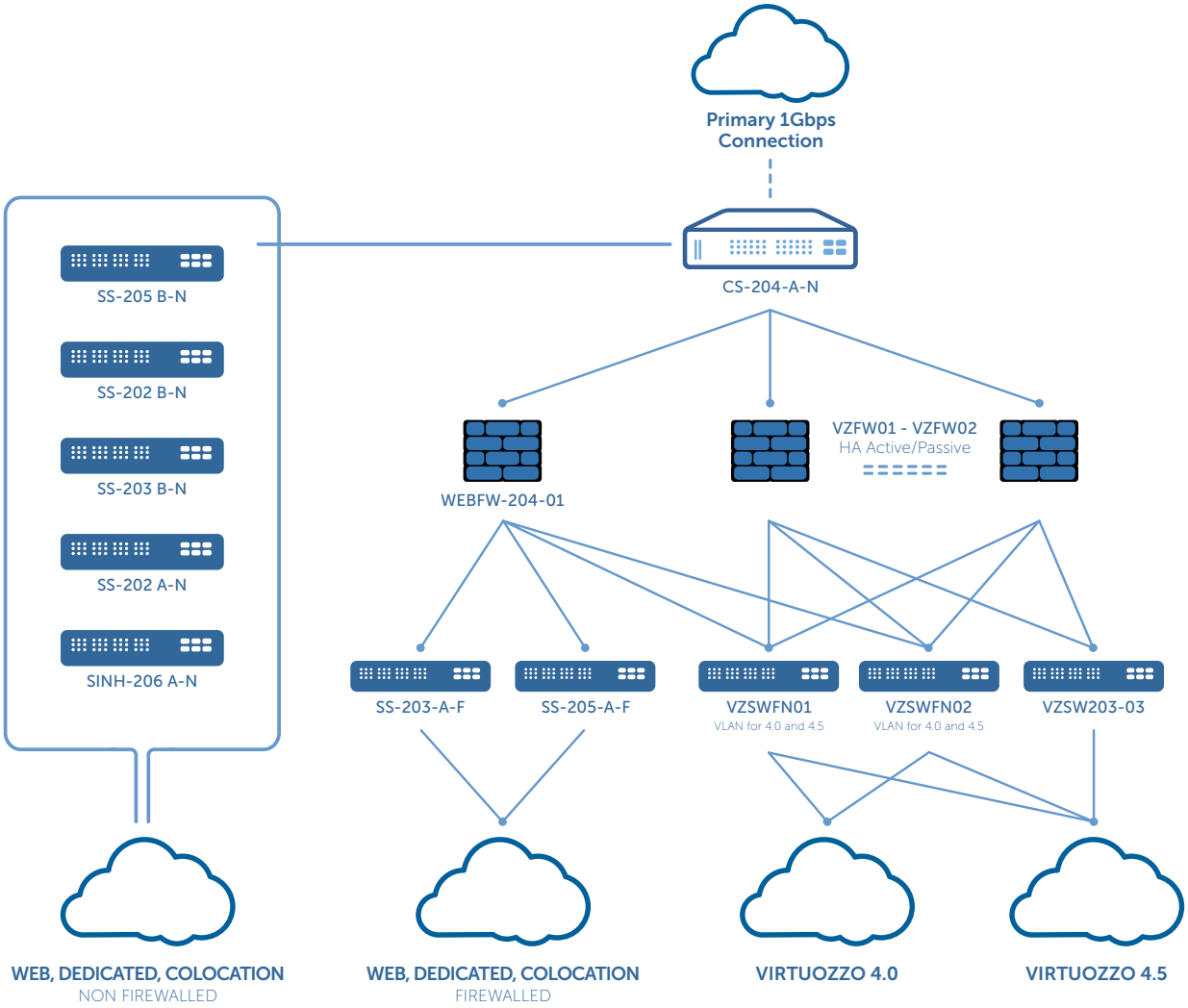
Production Environment

It's important to assess your current production environment. To identify the right DR solution for your business, you need to identify which services are critical to your business and which are less important. We've provided tables in this document to help you do this.

Diagram Of The Network Infrastructure

A diagram of the network infrastructure will help you identify how each server(s)/service(s) interoperate so you can better plan your DR site. That diagram should include IP addresses, network equipment, VLANs, special network configurations, etc.

Here is an example:



Production Environment

List of Servers

An up-to-date list of your servers is essential to your Disaster Recovery plan.

Use the table below as an example.

- The **Server Number** column identifies each server.
- The **Server Type** column specifies if the server is virtual or physical.
- The **Server Specifications** column displays the amount of disk space, memory, CPU, etc. that are allocated to that server.
- The **Host Server Number column** is used only when the server is virtual. It refers to the physical server number running the VM.

Server Number	Server Type	Server Specifications	Host Server Number
P01-PE530-01	Physical	• Dell PowerEdge R530 • S/T: G4G5H • Windows 2012 R2 • 2 CPU quad-core 3.3Ghz • 32GB RAM • 5 x 300GB HD (2xRAID1, 3xRAID5) • 2 x 10Gbps network cards	N/A
V01-2K-01	Virtual	• Windows 2012 R2 • 4 vCPU • 8GB vRAM • 1 vDisk 40GB • 1 vDisk 100GB • 1 vNIC	P01-PE530-01
V01-2K-02	Virtual	• Windows 2012 • 2 vCPU • 4GB vRAM • 1 vDisk 30GB • 1 vNIC	P01-PE530-01

List of IT Services

The up-to-date list of your IT services is the core of your DR plan.

Our example shows a table with 7 columns:

- **Service Name** displays unique names of IT services running in your business.
- **Criticality Level** indicates how critical the service is for your enterprise.
- **RTO** is the maximum delay before the service needs to be restored and ready to process.
- **RPO** is the maximum age of data that can be recovered when the service comes back.
- **Server Number** indicates on which server the service is running (in reference to the previous table).
- **Department** indicates the company department(s) using that service.
- **Contact Person** is the person to refer to about that service.

Service Name	Criticality Level	RTO	RPO	Server Number	Department	Contact Person
Website	Mission critical	15 min	4 hours	3	Computing	Alan Covish
SQL	Mission critical	15 min	15 min	2	Computing	Alan Covish
Acomba	Business core	4 hours	8 hours	3	Accounting	Natasha Brendan
Terminal service (Excel, Word, Outlook)	Business core	2 days	8 hours	2	Sales	Loic Naditu

Once you have completed the list of servers and services, you will know the target RTO/RPO for each service, the type of server hosting it and its criticality. With this information, you should be able to select the best solutions for your needs.

Online Backup – For a Cold Site DR Solution

Type of server: Phisical **RTO:** HIGH **RPO:** MID **Cost:** $

What is it?

Selected files on your servers are backed up to a storage location in a different building. You can restore files from any location with an Internet connection.

Prerequisites

- Subscribe to an online backup solution with your favorite supplier (Braintee Group delivers this service)
- Install the online backup application on the server
- Select all important files or use an application-level backup job (like Exchange or SQL)
- Adjust the bandwidth throttling in the application

How it Works

With the prerequisites completed, an incremental backup process will automatically store your critical data in the cloud. To save bandwidth, you can send a physical hard drive to your supplier with the initial backup of your critical data completed using the online backup application. Once your supplier receives and transfers your initial data, the next backup jobs will only upload changes in the files from your server to the cloud.

If you're running you applications in the cloud and a disaster occurs, bringing a new server up in the cloud involves the creation and installation of a new VM with the same OS as the original, the configuration of the Braintree Group Online Backup application and the restoration of your files.

Pro

- Easy automatic incremental offsite backup
- Backups accessible from anywhere, anytime
- End-to-end encryption

Cons

- Need to configure a new server before the restore
- RTO is really high (could be less if you already have servers ready or VMs in the cloud)

VM Backup In The Cloud – For A Cold Site DR Solution

Type of server: Virtual **RTO:** MID **RPO:** MID **Cost:** $$

What is it?

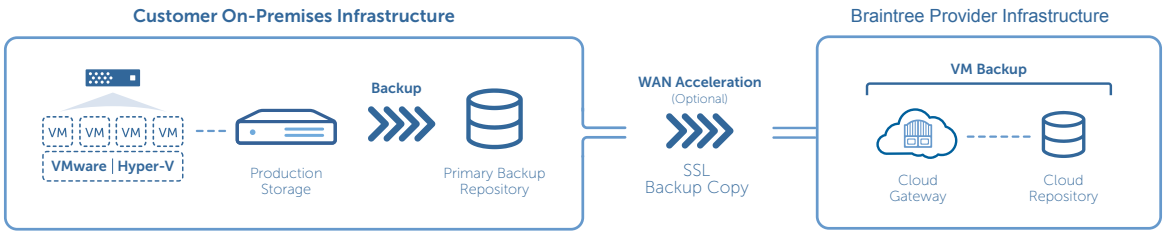
Your entire virtual machine (VM) is backed up as a single file to a storage location in a different building. You'll be able to restore your VM on any server running the same hypervisor (Hyper-V or VMware). After it is restored, your server (VM) will start running the same way it did when you backed it up.

Prerequisites

- Subscribe to the Veeam Cloud Connect service with your favorite service provider (Braintree Group delivers this service)
- Install Veeam Availability Suite, Veeam Backup & Replication or Veeam Backup Essentials
- Create your VM backup jobs to your local repository and your cloud repository

How It Works

With the prerequisites completed, the entire VM is backed up to your local storage then to the cloud repository in your provider's infrastructure.



If a disaster occurs and you cannot use your local facility, you can restore the entire VM in a Private Cloud on your own hardware that is ready for this purpose. However, this is more costly. You could also use the infrastructure of a Service Provider like Braintree Group that offers capacity on-demand. You will only have to set the IP address of your original server and update any configuration related to this IP address.

Pro

- Time for complete restoration involves restoring the backup to the IaaS platform
- No reconfigurations needed as all settings are already in the VM
- Scheduled incremental offsite backups
- End-to-end encryption
- Allows for fairly easy testing of recovery procedure without impacting the environment
- Possibility to restore to the Cloud Service Provider's IaaS, if they offer the service

Cons

- Minimum RPO is equivalent to the time it takes to finish the backup job. It can be high, depending on the VM size and the Internet connection
- Restoring on-premises requires transferring all data. This can be slow depending on the Internet connection
- The hypervisor should be the same on the Cloud Service Provider's infrastructure, in order to successfully restore the VM

VM Replication – For A Warm Site DR Solution

Type of server: Virtual **RTO:** LOW **RPO:** LOW-MID **Cost:** $$$

What is it?

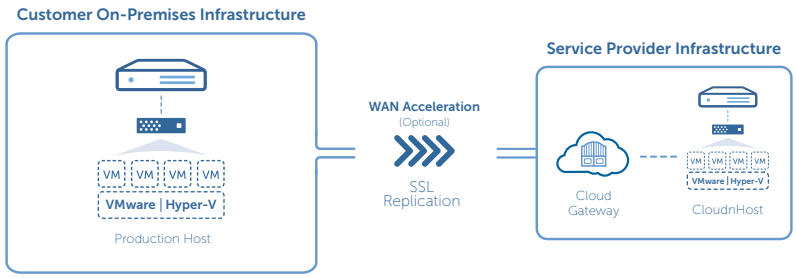
Your entire virtual machine (VM) is replicated to a hypervisor outside your infrastructure. Your replicated VM is ready to be powered up in your cloud service provider's infrastructure.

Prerequisites

- Subscribe to the Veeam Cloud Connect service with your favorite service provider (Braintree Group delivers this service)
- Install the Veeam Availability Suite, Veeam Backup & Replication or Veeam Backup Essentials
- Create your VM replication job with your service provider's infrastructure as the destination

How It Works

With the prerequisites completed, the entire VM is replicated to your Cloud Service Provider's infrastructure. However, it is not up and running. After that, an incremental update of the replicated VM is done each time.



In case of a disaster, you only have to start the VM from your Service Provider's control panel and modify the IP address configuration in the VM.

Pro

- Takes only a couple of minutes to have the replicated VM up and running
- No reconfigurations needed as all settings are already in the VM
- End-to-end encryption
- Allows for fairly easy testing of recovery procedure without impacting the environment
- RPO is lower than with the previous option because only the modified files are uploaded to the replicated VM

Cons

- The hypervisor should be the same on the Cloud Service Provider's infrastructure in order to successfully replicate the VM
- Cost is higher than the other options presented above

Mirroring – For a Hot Site DR Solution

Type of server: Physical or Virtual **RTO:** LOW **RPO:** LOW **Cost:** $$$$

What is it?

The replicated application is configured on two servers (on-premises and in the cloud) and they are both always up and running. The replication process is managed directly by the application. It is important to understand that not all applications have that replication technology. The configuration and the way it works vary from one application to another.

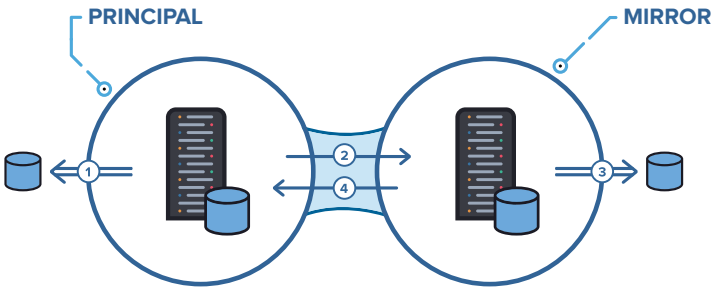
Prerequisites

- Need a server up and running offsite (could be a VM in Performance Cloud)
- Need an application capable of log shipping or mirroring or any replication technology (SQL, Exchange, etc.)
- Need to configure the application to replicate itself to the DR server

How It Works

Once you have the prerequisites, every time something is written in the local application, a replication is done to an external server that is configured to write the data synchronously or asynchronously before the transaction is marked as completed at the local server.

1. Write the data to the transaction log and commit the data
2. Send transaction to mirror
3. Write the data to the transaction log and commit the data
4. Send acknowledgment to principal



In case of a disaster, most of the applications that support mirroring will automatically failover. It is also possible to do a manual failover.

Pro

- Easy automatic failover is almost always available in the application
- Really fast to have the service up and running in the DR site
- No data loss if in synchronous mode or a little data loss in asynchronous mode

Cons

- Need expert to configure the mirroring
- Costly solution because you need to double the number of servers
- Some software is hard to replicate or to keep the replication going