Acronis

A Cloud **Disaster Recovery Use Case**

New Generation Data Protection

This use case describes a disaster recovery scenario affecting a mid-size company. It includes a systematic recovery timeline demonstrating how the company's IT department restored their data center leveraging Acronis Disaster Recovery Service.

USECASE

August 2015

Introduction

Data is your organization's lifeline. If you lose it, it can be more than an inconvenience.

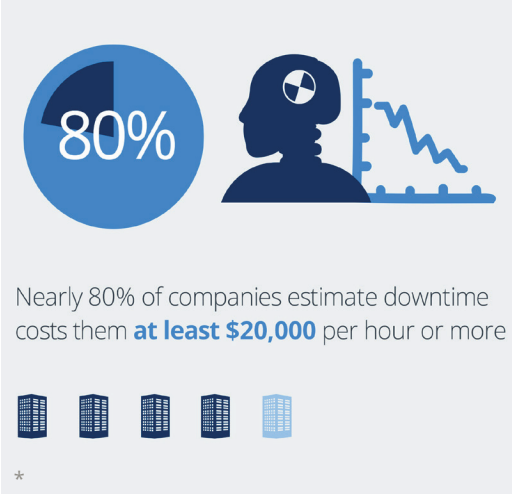
Lost data can result in a shutdown of internal business processes, impacting employee productivity, revenues, and brand reputation. Lost data can also result in contract penalties and stiff fines for non-compliance.

The most significant consequence of lost data can occur when a full disaster strikes. According to **the Institute for Business and Home Safety**, an estimated 25 percent of businesses do not reopen following a major disaster. If you do not have data protection, your company can be a statistic.

This document is a use case that describes a DR scenario affecting a mid-size company. The scenario: a disaster destroys the company's production data center and the IT team must recover the data center within the Recovery Time Objective.

The use case describes the company's IT environment, the backup, storage and DR policy, the DR plan, and provides a systematic recovery timeline demonstrating how the IT department restored the data center leveraging Acronis Disaster Recovery Service.

This use case is appropriate reading for CIOs, CTOs, and IT directors / managers in medium-sized organizations and IT workload specialists in enterprise companies.



*Source: *"Complexity and Data Growth Driving Small and Medium-Sized Environments Toward a New Generation of Data Protection"*, IDC, June 2014. Sample: 401 SMB Businesses, <1000 employees

The Company's Production Data Center

The company has one primary data center that is located in the same building as the rest of the company's operations. The data center hosts all the production servers, storage, and the network infrastructure. Desktops, laptops, and mobile devices are connected via a wired and wireless infrastructure.

The Production Servers

The company has a hybrid IT environment – a mixture of physical and virtual servers that run different workloads and provide services to all departments.

- There are ten physical servers running two primary Microsoft® Active Directory® (AD) Domain Controllers (DCs), production ERP software, and legacy applications. IT is in the final stages of virtualizing the physical servers. A few physical servers will remain because some of the vendors cannot virtualize their applications.
- The majority of the workloads are on virtual machines running the VMware vSphere® Enterprise Edition suite. There are 15 ESXi hosts running 100 virtual machines; all controlled by a single VMware vCenter™ server.
- VMware vSphere has 16TB SAN storage for centralized production, which houses most of the VMs. Logically, vSphere is split into two segments – production and R&D / QA; both are implemented with vCenter, vSphere networking, and VMware vSphere® Distributed Switch™ (VDS).
- The virtual environment runs the majority of applications – Microsoft Exchange, a few Microsoft SQL Servers, custom applications developed by R&D, and a CRM system powered by an Oracle® database server running on a Windows® host.

The Production Network

The company has a 1Gbit, flat structure network, running on mid-level network switches. The throughput is acceptable. Logically, the data center network has three major subnets:

- A physical segment housing physical servers, the ERP system, and primary DCs
- A production virtual segment defined and managed by vSphere VDS
- A R&D / QA virtual segment also handled by vSphere VDS

The Disaster Recovery Service

- As part of the overall disaster recovery plan, IT contracted Acronis to provide a Cloud Disaster Recovery in one of Acronis' DR Data Centers.
- Acronis has enough CPU, Disk and RAM resources to start all protected systems if disaster happens. Acronis guarantees servers to be up and running within 15 minutes from the time of the request to being operational. These 15 minutes do not include the time for non-server DR operations.
- As part of the Acronis Disaster Recovery Service, Acronis also runs the Active Directory Domain Controller in Acronis DR Cloud – so the Active Directory is always up-to-date, and would not require failover.

The Production and Backup Storage

As described above, production storage is a centralized 16TB SAN, used by VMware vSphere.

The backups are stored to three separate Acronis Disaster Recovery Local Cloud appliances, which combine the backup management, local backup storage, local failover and replication to Acronis DR Cloud:

- LCA-1 is for protection of physical servers. It is connected to the same network switch with most of the other physical servers through a 1GBit connection.
- LCA-2 is connected through a dedicated small network switch to the production ESXi servers.
- LCA-3 (R&D/QA) is connected to the R&D / QA virtual hosts.
- IT has separated the Acronis local cloud appliances so that they can more easily manage protection in different network zones and concentrate backup data flow within specific subnets.

The Company's IT Disaster Recovery Policy

The company's IT Disaster Recovery policy is a subset of the overall DR plan. It describes the required IT equipment and a business continuity strategy that addresses all company operations – communication, business and banking, financial, audit and compliance, logistics, human resources, and so on.

Business Continuity Objectives

A planning committee developed the backup and DR policy, which the executive management team approved. The first objective of the plan describes the company's Recovery Time Objective (RTO) and Recovery Point Objective (RPO). When deciding RTO and RPO, you need to consider your available budget. A shorter RTO and RPO are more expensive and require more resources. For example, a zero RPO and RTO require you to implement long-distance fault tolerance systems. A RPO / RTO of seconds require a long-distance high availability solution. This company cannot afford fault-tolerant systems or a high availability solution.

To determine the maximum amount of time that the company can operate without critical systems, the committee analyzes the business processes, operations, downtime costs and available budget. They then map this time back to the RTO. The committee determines that the company's RTO for complete recovery and return to normal business operations is 8 hours.

Based on this, the RTO for the production data center is 4 hours. The RTO for any single server is 1 hour. With RTO, the subcomponents of the DR plan are always shorter than the company's RTO. Next, the DR plan describes the company's Recovery Point Objective (RPO). The RPO is the maximum, tolerable period of time that assets can be lost. While all organizations want to preserve 100 percent of their assets, it is not economically feasible to do so.

Instead, the company must decide how many assets it can afford to lose to determine the RPO; the length of time before the DR event, up to the moment an event occurs, specified in seconds, minutes, hours, or days.

On average,
51% of high priority applications
have a downtime tolerance
of **less than one hour**

* *ESG Research Study, The Evolving Business Continuity and Disaster Recovery Landscape*

The committee determines that the organization's RPO is 3 hours. That means that the company is willing to lose products, assets, and data generated within the last 3 hours prior to a disaster. A RPO of 3 hours for the company's data means that IT should run data backups at least every 3 hours. The RPO of the subcomponents of an overall DR plan can be the same as or shorter than the company's overall RPO. Some organizations tier the production workloads and set different RPOs based on the value of generated data.

The Company's IT Disaster Recovery Solution

The company uses Acronis Disaster Recovery Service to protect its production data center. Acronis Disaster Recovery Service delivers unified data protection and disaster recovery for multi-system environments. Based on an organization's business needs, it can protect individual workloads or protect an entire data center.

The company chose Acronis Disaster Recovery Service because the suite of products provides:

- Data protection for the company's physical and virtual systems
- A easy-to use web console to configure, install, and maintain the service
- Disk and VM image backup so IT can capture a complete image of a disk or volume on a physical or virtual machine
- Single pass backup for Microsoft SQL Server and SharePoint, which lets IT capture both application and operating system data at one time
- Support for multiple hypervisors including VMware and Hyper-V
- Seamless P2V and V2V migration to support the disaster recovery of physical or virtual servers to virtual machines

Protected Systems

The company uses Acronis Disaster Recovery Service to back up and failover all production workloads - the production and R&D / QA physical servers and VMs. Full backups capture approximately 8TB of uncompressed data. Differential and incremental backups generate significantly less data because only the difference is stored.

The company's average daily data change is about 1.5 percent; daily incremental backups capture 120GB of data, while weekly differentials capture 600GB of data.

With Acronis Disaster Recovery Service, the company does not need to use synthetic or consolidation backups because the single-pass recovery automatically reconstructs the data from the backup points.

The Backup Storage Policy

The Acronis Disaster Recovery Service initially backs up all Company systems to Acronis Local Cloud Appliances and then replicates the backup copies to Acronis Cloud.

With a local copy, IT can quickly restart individual workloads without failing over to the cloud. The copies stored in Acronis Cloud are for major disaster recovery.

This approach mirrors Acronis' recommended 3-2-1 backup strategy: maintain all data in three locations (production systems, backup on LCA, and backup in Acronis Cloud), on two types of media (disk and cloud), and one copy of backup data stored offsite.

The Backup Schedule

With the RPO, RTO, protected systems, and backup storage policy defined, it is easy for IT to define the protection schedule.

Acronis Disaster Recovery Service has backup retention features to fit the company's needs. The company decides to run backups every 3 hours to meet RPO requirements.

IT does not have to define the blackout period for the backup window. Acronis uses snapshot technologies on both virtual and physical systems so operations are not affected. Acronis's disk-imaging technology also backs up all the data consistently – even if the files are open.

Backup Duration

Production servers hold 2TB of data and the LCA-1 can ingest 80MB of data per second. With an average compression ratio of 3:1, a full backup (1TB) of the production servers takes two to three hours. The differential backups take 25 minutes, and incremental backups complete within ten minutes.

Production virtual servers hold 4TB of data, and LCA-2 performance is similar to LCA-1. Full backups take 8 hours, differentials complete within one hour, and incremental backups complete in less than 25 minutes.

The duration of backups for the R&D / QA teams is similar to the production physical server because LCA-3 performance is on par with its counterparts.

The Disaster Recovery Plan

Natural disasters are common in certain geographies. For example, the U.S. reports more than 1,200 tornadoes every year. Earthquakes and tsunamis, floods, forest fires, hurricanes, mudslides, and avalanches can destroy a data center, sometimes without warning. Many natural disasters can affect an entire area, which is why you must store one backup copy a reasonable distance from the original location. Being prepared is the key to ensuring that your organization's operations continue.

War, terrorism, and sabotage are all man-made disasters. In many cases, man-made disasters are not intentional. Regardless, a fire caused by negligence or human error can destroy an entire data center.

While some man-made disasters can be prevented, no organization is 100 percent protected. The DR plan must cover any incident that causes company operations to cease or data to be lost.

The company creates a high-level DR plan, and the IT team develops a plan for the data center. The IT team plans, documents, and tests every step of the DR process.

IT does not need to follow their DR plan manually. Acronis Disaster Recovery Service includes advanced DR automation and graphical editor for DR Runbooks – so the IT team simply applies the DR plan into the Acronis service. During a disaster, the high-level plan is activated with runbooks already prepared for IT infrastructure.

Acronis Disaster Recovery Service allows the IT team to test their DR plan on a regular basis so that every engineer understands their objectives and tasks.

A Disaster Happens

The disaster happens and company management invokes the DR plan. The IT team begins to recover the data center. Here is the timeline.

Date	Time	Action/Event	Details
Day 1	0:00mn	The disaster happens.	The data center is destroyed.
	0:10am	Company management invokes the DR plan.	
	0:11am	IT opens Acronis DR Console on the inter-net-connected device (even tablet).	Note, that Active Directory replica is already operational, as it is constantly running.
	0:15am	IT starts DR Runbook execution in Acronis Disaster Recovery Service	IT can perform this execution from any device, even the tablet through wireless connection.
	1:02am	The Runbook execution is complete	All company servers are now operational in Acronis Data Center.
	1:05am	IT starts tests of all production workloads	This involves testing e-mail flow, CRM and ERP operations, SQL database operation, etc
	3:12am	Tests are complete	
	3:15am	The data center restoration is complete	Total Duration: **3 hours 15 minutes**

The data center is operational, well below the RTO. However, the DR plan for the company is not fully executed yet. Other pieces of the plan are still in process – the relocation of employees and manufacturing facilities, connecting laptops and new desktops to the DR data center, and so on.

Summary

A disaster destroys the company's data center but the company is prepared. The IT team developed a disaster recovery plan that included the Recovery Point Objective, Recovery Time Objective, protected systems, backup storage policy and backup schedule. The management team approved the disaster recovery plan.

IT exercises the plan on a regular basis using different scenarios.

The timeline of actions clearly lays out the steps the IT engineers took to recover the data center and restore operations.

Using Acronis Disaster Recovery Service, the IT team achieved all of the business objectives set forth in the DR plan and restored all data center operations in 3 hours 15 minutes, well below the RTO of 4 hours.

Acronis Disaster Recovery Service is powered by the Acronis AnyData Engine, which combines backup, bare metal restore and system recovery to protect data whether it resides on premise, in the cloud, or in remote offices. With Acronis Disaster Recovery Service, the company simplified backup and disaster recovery, significantly reducing the IT time and effort to recover their data center

> "Due to the client-facing nature of our business, email service, DMS, time and billing management are absolutely critical to us.
>
> The **solution provides us** with the bullet-proof **assurance** that our apps are always available, no matter what."
>
> *Matt Beland,Director, IT and Security, Davis Wright Tremaine, LLP*

Acronis Disaster Recovery

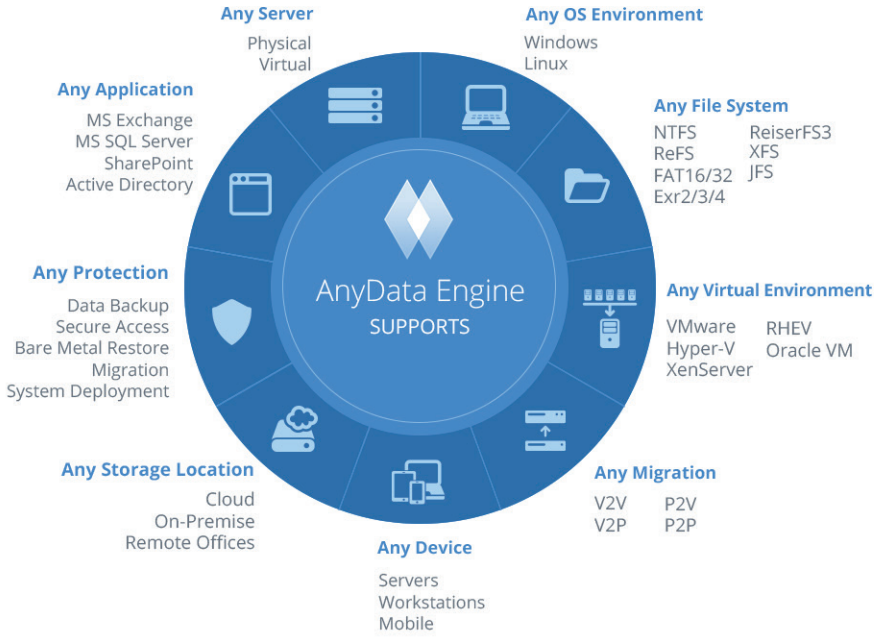
Acronis Disaster Recovery Service is a complete IT business continuity solution that backs up and replicates systems into an on-site appliance and Acronis cloud data center, and can recover and restart customer's systems with a guaranteed SLA in the event of an outage. Acronis Disaster Recovery Service can protect any physical or virtual system in any environment and in any location — it is powered by the Acronis AnyData Engine, a set of unique, deep, and powerful new generation data protection technologies that capture, store, recover, and manage data in virtual, physical, and cloud environments.

Acronis provides a trusted all-in-one disaster recovery solution with push-button recovery of any IT services, system and data in any environment at any location. Acronis enables business continuity by protecting data, servers and entire data centers with a robust hybrid cloud DR solution. Acronis is trusted by organizations of all sizes, who have low tolerance for IT disruptions, data loss or services downtime.

The Acronis AnyData Engine

The Acronis AnyData Engine is the core suite of technology that powers all Acronis new generation data protection products to capture, store, recover, control, and access data in virtual, physical, cloud, and mobile environments.

Fueled by over 100 patents it lets you easily protect of all the data across multiple systems. System administrators have the ability to define and manage consistent data protection policies and still get highly efficient, granular control. Whether your data resides on-premise, in the cloud, or in remote offices, the AnyData Engine combines disaster recovery, data backup, bare metal restore, migration, system deployment, recovery, and enterprise file sync and share.



Top 5 Reasons to Choose Acronis Disaster Recovery Service

1. **Enable** business continuity with 15 minute RTO and guaranteed SLAs
2. **Reduce** downtime from days to minutes and seconds
3. **Simplify** data protection with professional-grade backup and cloud disaster recovery in one solution
4. **Eliminate** risks with periodic DR testing, and 24x7x365 white-glove support
5. **Protect** the entire infrastructure with broad platform support

> “**We really liked the Acronis model** and their focus on **security**, **availability** and **technical** functionality. Our i**mproved ability to test the failover** and recovery allows my team to sleep better at night”
>
> *Philip Wood,*
> *Head of IT,*
> *Bristows LLP*

Useful Links

Acronis Website

Acronis Disaster Recovery Service

ABOUT ACRONIS

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products were named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com.** Follow Acronis on Twitter: **http://twitter.com/acronis.**

Acronis

For additional information, please visit http://www.acronis.com

To purchase products, please visit http://www.acronis.com/en-us/company/contacts.html#international to find an Acronis office or authorized dealer.