www.sunrisetechnology.it

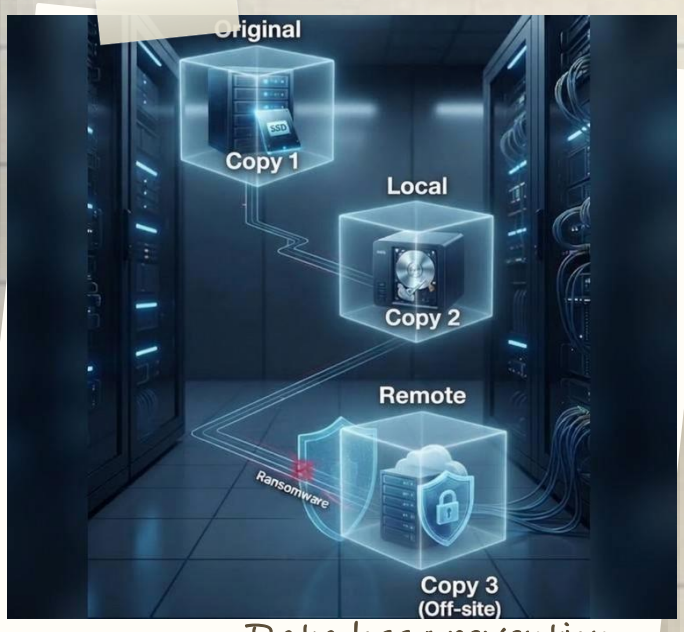
DATA ENGINEERING

The 3-2-1 Rule

3 copies · 2 media · 1 off-site copy · Verify



Resilient backup architecture



Data-loss prevention

AI

Introduction

This document expands on the concepts of the basic guide, providing technical specifications, disaster recovery metrics and advanced architectural considerations to lock down the data infrastructure against any loss vector.

1 · Three copies

The concept of data triplication does not stem from a principle of superfluous redundancy, but from the need to isolate data from heterogeneous risk vectors.



Risk vector analysis

[RISK]

Copy 1

Resides on the main volume and is the everyday working file, subject to potential corruption.

Local copy

Independent medium that mitigates mechanical failures or filesystem crashes of the main volume.

Immutability

Air-gapped or WORM architecture to prevent a cyberattack from compromising remote backups.

Third copy

Definitive isolation to prevent the spread of ransomware and mass-deletion commands.

[LOGICAL ISOLATION]

Fileless malware and silent threats can spread to secondary disks if they remain constantly mounted and writable by the operating system.

Parameters and media

RPO — Recovery Point

Maximum amount of data that can be tolerably lost because of an incident, determined by backup frequency.

RTO — Recovery Time

The time needed to restore operating systems and data after a failure, using high-speed storage.



Media heterogeneity

Storage

SSD NVMe

High-performance internal primary disk for fast handling of daily working data.

NAS

RAID array of NAS-grade mechanical disks to vary the write technology and reduce failures.

Tape / USB — Off-site

External storage system useful for geographic relocation and business continuity.

> ***Rule of thumb: SSD NVMe for daily work, NAS RAID for the local copy, Cloud or external disk for off-site relocation.***

2 · Two media types

Heterogeneity of storage media prevents the risk of a technological single point of failure or one tied to wear over production time.

[ARCHITECTURE]

Hardware

Pairing the internal primary disk with a different type of medium means varying the write technology.

Different file systems

NTFS/APFS for the client and ext4/ZFS on a Linux NAS to protect against logical metadata corruption.

Bit rot

Prevention against silent bit-rot errors and anomalies of the local SATA or NVMe controller.



Diversifying the media

The golden rules of backup

Heterogeneity: *different technologies.*

Separation: *adopt different file systems to prevent logical metadata corruption.*

Relocation: *always keep an off-site copy against fires or physical theft.*

[COMMON MISTAKES IN COMPANIES]

Relying on a single backup copy, keeping backup disks always mounted and accessible, or ignoring the periodic verification of the saved data.

3 · Off-site copy

Geographic relocation is the only bulwark against total physical disasters and perimeter compromises of the company's local infrastructure.

Off-Site Copy

Encrypted cloud storage or an encrypted disk physically rotated to another location.

Continuity

Ensures business continuity in the face of local catastrophic events.



Geographic relocation of the backup copy

[ENVIRONMENTAL RISK MITIGATION]

Events such as fires, catastrophic power surges, physical theft of hardware or floods wipe out local operations and call for a remote strategy.

Fires and floods — Premises

Total destruction of the local hardware and of the primary storage media in the office.

Encrypted Cloud — Off-site

Secure remote storage accessible over the network for fast recovery of critical company data.

Disk Rotation — Backup

Encrypted disks physically transported to another location to guarantee total isolation.

4 · Scripts

Human intervention is statistically the weakest link in any IT security procedure: automation eliminates forgetfulness.

Manual tasks

0%

left to human memory: high risk of errors and omissions.

Scheduled tasks

100%

handled by operating system services and silent incremental scripts.

Exceptions

Notifications and Webhooks

Prompt reporting of failures in task execution, out-of-space conditions or permission errors.

Background daemons

Scheduled execution through Task Scheduler on Windows or cron jobs on Unix/Linux environments to guarantee continuity.

A backup that is not automated is a forgotten backup.

5 · Periodic verification

A backup that has not been tested is, logically speaking, a non-backup. The illusion of safety often leads to discovering the system's ineffectiveness only at the moment of greatest emergency, making a monthly test protocol on a staging environment indispensable.

6 · Test protocol

The verification process must simulate a real restore by extracting significant data samples such as database files, complex accounting archives and system images.



Data restore simulation

INTEGRITY CHECK

You must periodically verify that the backup clients have not stopped synchronizing because of expired tokens.

Expired tokens *— block synchronization.*

Policy changes *— storage variations.*

Disk saturation *— space exhaustion.*

Result: data always restorable in case of emergency.



Data security is a continuous process

Explore more tips and tutorials at
www.sunrisetechnology.it →

Created with the support of AI tools | © Sunrise Technology