Disaster Recovery & Business Continuity

What do we do when something goes wrong?

I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

THIS IS FINE.

Imagine a company...

- Bank with 1 Million accounts, social security numbers, credit cards, loans
- Airline serving 100,000 people on 500 flights daily
- Pharmacy system filling 5 million prescriptions per year
- Factory with 2000 employees producing 200,000 products per day using robots
- Hospital serving 1000s of patients including an emergency room operating 24/7

Imagine a scenario where something fails...

- Server failure
- Disk System failure
- Hacker break-in
- Denial of Service attack
- Extended power failure
- Snow storm
- Spyware
- Malevolent virus or worm
- Earthquake, tornado
- Employee error or Malicious Sabotage

What is Disaster Recovery and Business Continuity?

Business Continuity

The ability of an organization to maintain essential functions during, as well as after, a disaster has occurred

Disaster Recovery

The ability of an organization to re-establish information technology services and data integrity following a disruption

Disaster Recovery is often a large part of Business Continuity

Potential Impact Analysis

Which business processes are of strategic importance?

What disasters could occur?

Is there potential for a cascading failure?

What impact would they have on the organization financially?

- Legally?
- Financially?
- On reputation?
- On human life?

How quickly do you need to be back up and running?

- At what capacity?

Impact Classification

Negligible

No significant cost or damage

Minor

A non-negligible event with no material or financial impact on the business

Major

Impacts one or more departments and may impact outside clients, deliverables, deadlines, etc

Crisis

Has a major material, financial, or legal impact on the business

Impact Classification

Incident	Affected Business Processes	Impact Classification

Impact Classification

Incident	Affected Business Processes	Impact Classification
Fire	Classrooms, Labs	Major/Crisis (If Human life is at risk)
Network Unavailable	Campus Core Network	Crisis (All business units are impacted)
Hacking Breach	MyUB/UB Hub	Major (Legal Liability/Denial of Service)
Server Disk Failure	Timberlake, Metallica, Etc	Minor (If HA using RAID)/Major (Downtime for CSE)
Social Engineering	Financial Aid, Registrar	Major (Legal Liability)

Service Classification

Nonsensitive

Can be performed manually/alternately for an extended period of time with little additional cost and minimal recovery effort

Sensitive

Can be performed manually/alternately for a period of time, but may cost more in staff or time

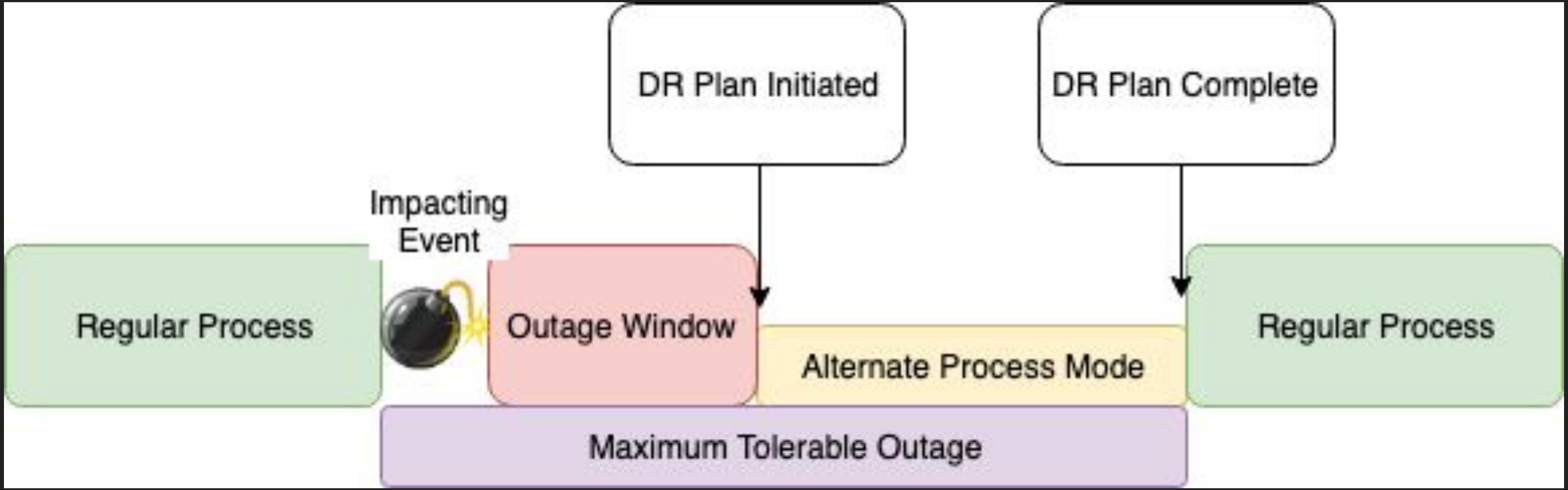
Vital

Can be performed manually/alternately for very short time or with high effort/delays

Critical

Cannot be performed manually/alternately. Tolerance to interruption is very low

Disaster Recovery Timeline



Key Terms

Outage Window

Period of time where services are unavailable or offline

Alternate Process Mode

Service offered by a backup system to provide critical services in the event of a failure (with minimal interruption)

Service Delivery Objective

Level of service in Alternate Mode

Key Terms (Cont)

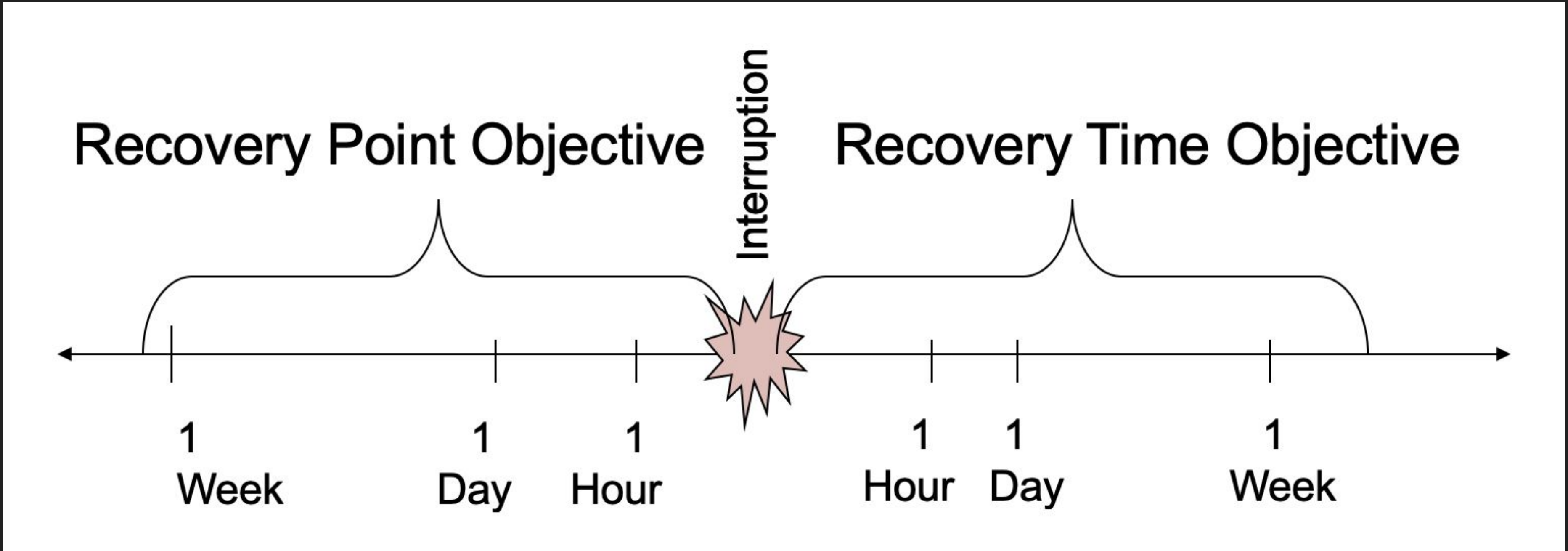
Maximum Tolerable Outage

Maximum time allowed in a Degraded State

Disaster Recovery Plan

How to transition to Alternate Process Mode and then back to Standard Processes

RPO vs RTO


Recovery Point Objective
Interruption
Recovery Time Objective
1 Week
1 Day
1 Hour
1 Hour
1 Day
1 Week

High Availability

Is High Availability the silver bullet for Disaster Recovery?

A Highly Available system is often described as ‘fault tolerant’ or having the ability to ‘fail over’

- A lot of places believe that it is
  - If it’s always online and available, how could services ever be impacted?
  - To a certain extent, this is true
- High Availability reduces the amount of incidents that will cause you to use the Disaster Recovery Plan - however **it is not a replacement for DR**
- **Why?**

HA vs DR

- Disaster recovery includes a focus on re-establishing services and data integrity after an incident not just fail over
- Disaster recovery often includes the use of an alternate site (geographic diversity) not just redundancy at the system or datacenter level
- Disaster recovery addresses multiple failures in a datacenter while high availability typically accounts for singleton predictable failures
- Disaster recovery includes the people and processes necessary to execute recovery while high availability focuses on technology design and implementation

HA vs DR

- Does this mean that High Availability has no place in Disaster Recovery?
  - Of course not
  - DR and HA are often intertwined (and sometimes confused with each-other)

- HA can automatically transition you to Alternate Process Mode where you are running in a degraded (but still functional) state
  - The larger the impacting event the higher your level of HA needs to be
  - For huge corporate entities this often means several Data Centers in multiple geographic locations

- HA usually does not cover the ability to recover lost, corrupted, or destroyed data

Types of High Availability

What levels of High Availability have we covered already?

- Power
    - Both Server PSUs and Services into the Data Center
- Internet Connections
- DNS servers
- Routers and Switches
- Cluster of servers behind a load-balancer

Let’s talk about RAID

- RAID - Redundant Array of Independent Disks
  - Originally - Redundant Array of Inexpensive Disks

- RAID works by placing data on multiple disks at once in a balanced way to either improve performance, or improve data resiliency

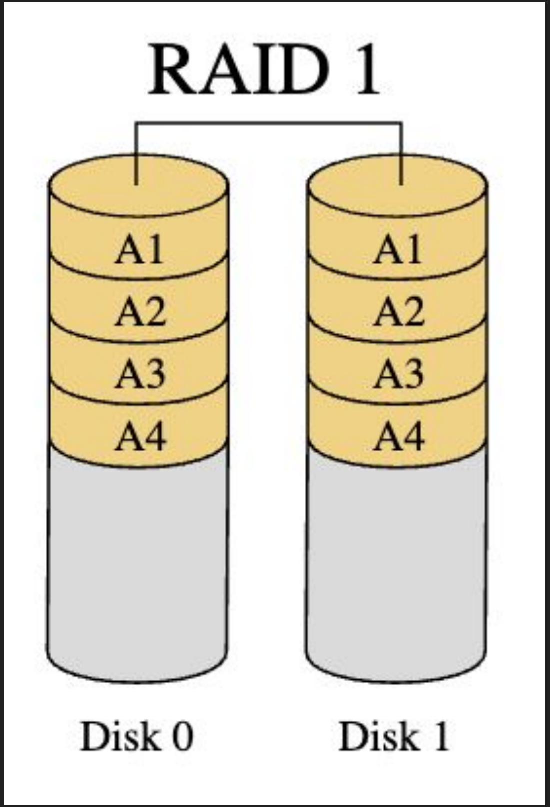
- There are several different “Levels” of RAID, each with advantages and disadvantages

Let’s explore the different options and figure out which is best

RAID 1

Also known as Mirroring

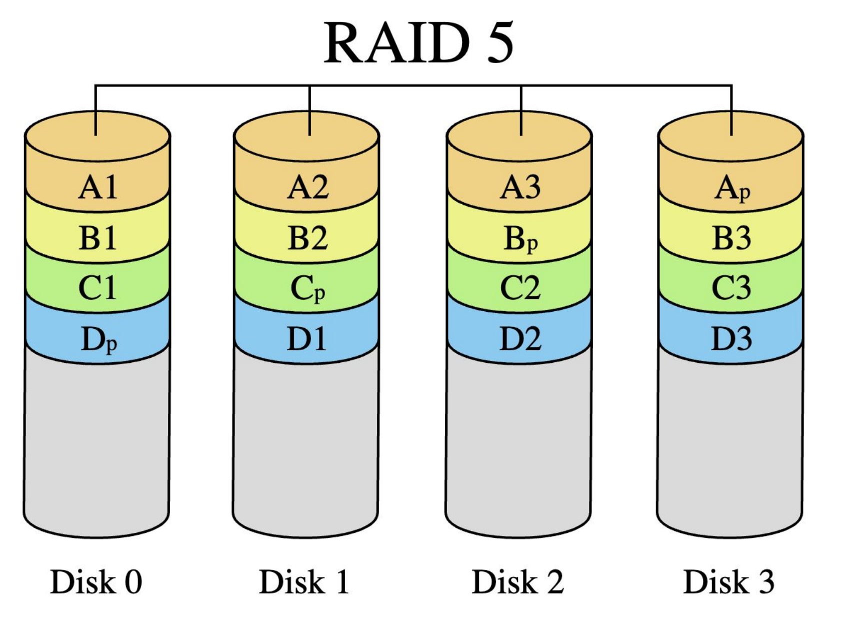
- Any data written to Disk 0 will be written to all N Disks in the array
- Allows for N-1 Disk Failures
- Performance
  - Space Efficiency: 1/N
  - Reads: Faster as information can come from any disk
  - Writes: Slower as information must be written to all disks
  - Requires minimum 2 disks



RAID 5

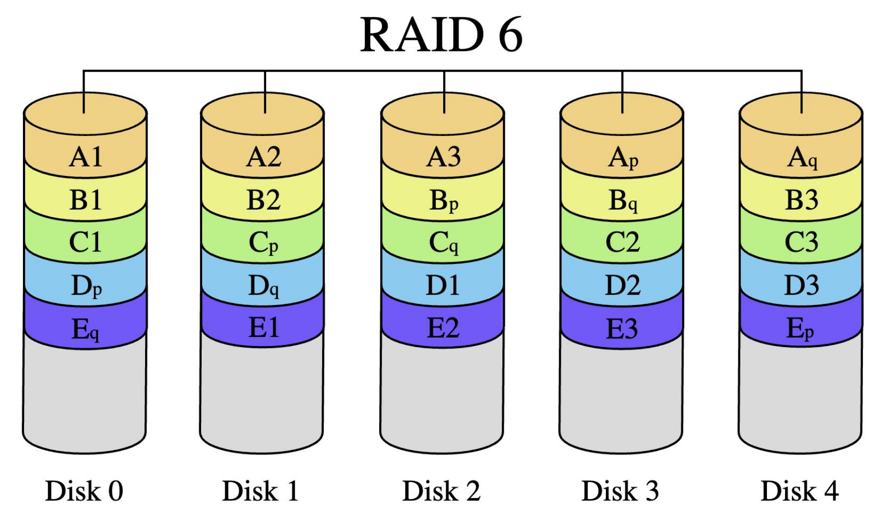
Block-level striping with distributed parity

- Allows for 1 Disk Failure
- Performance
  - Space Efficiency: N-1
  - Reads: Same as 1 drive - worse if in a degraded state (information needs to be calculated from parity)
  - Writes: Slightly slower than a raw disk due to parity computation, but much faster than RAID 1
  - Requires minimum 3 disks



RAID 6

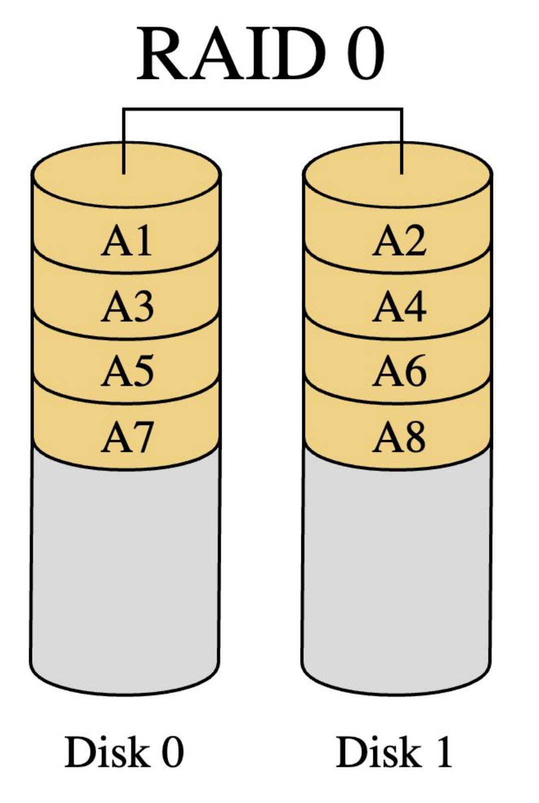
- Same as RAID 5 but with an extra disk of parity
- Allows for 2 Disk Failures
- Performance
  - Space Efficiency: N-2
  - Reads/Writes: Comparable to RAID 5
  - Required minimum 4 disks



Wait a minute, what about RAID 0?

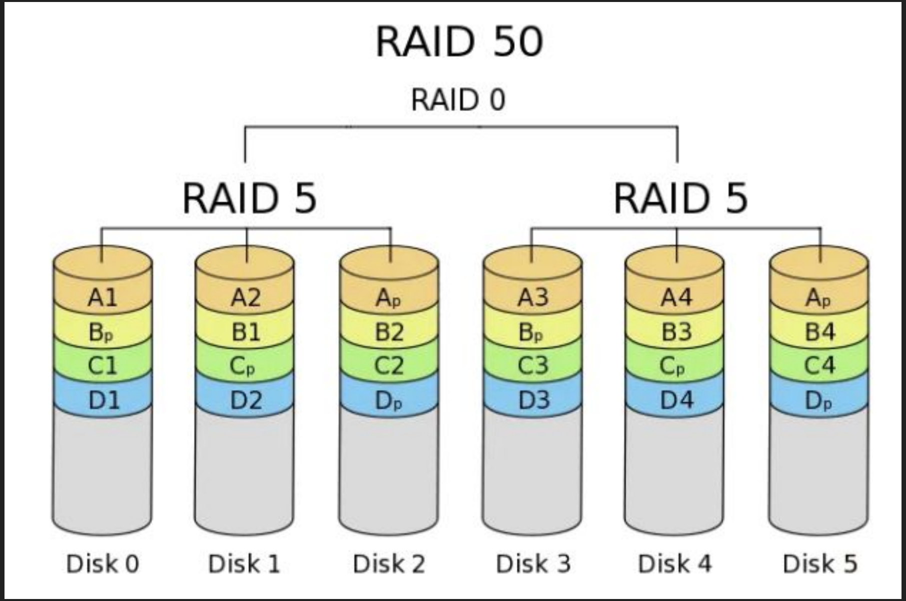
- Each disk stores 1/N of the data written to the array
- Performance
  - Storage Efficiency: **100%**
  - Reads/Writes: **Amazing - All reads and writes are spread across all disks**
- Allows for **ZERO** drive failures!

- **THIS IS NOT RAID**
  - There is NO (R)EDUNDANCY!



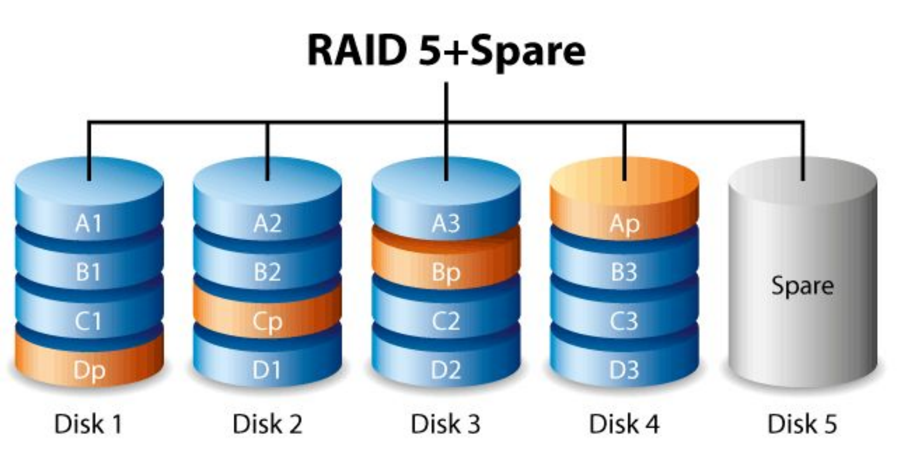
What about Hybrid RAID?

- RAID levels can be ‘combined’ to get the best of both worlds
- Usually always a standard RAID level paired with RAID 0 (striping) for performance
- RAID 50 is usually the best tradeoff between capacity, performance, and reliability and is often used in enterprise SANs



Hot Spares

- Also known as a Hot Standby
- A backup component that can be immediately placed into service when a primary component fails
- In the case of RAID, a Hot Spare lives in the enclosure and upon a drive failure it spins up and begins rebuilding the array
- When the dead disk is replaced it then becomes the hot spare



Cold Spares

- Also known as a Cold Standby
- A component that resides within a computer system but requires manual intervention in case of component failure (might require configuration settings or some other action to engage it)
- Useful for when an architecture cannot support HA/Hot Spare
    - Prevents unnecessary downtime while waiting for new components to be ordered/shipped/etc
    - Can often be pre-configured and ready to swap with the primary to minimize downtime (think network switches)

Applying RAID theory to other HA components

- Do other forms of HA follow the same principles as RAID?
  - i.e. Clustered Servers behind a Load Balancer?
  - What about Power Supplies?

- In the general case, the same concept applies to HA in general
  - HA is often used for redundancy and ‘fail over’
  - However, it is also used for performance and scalability

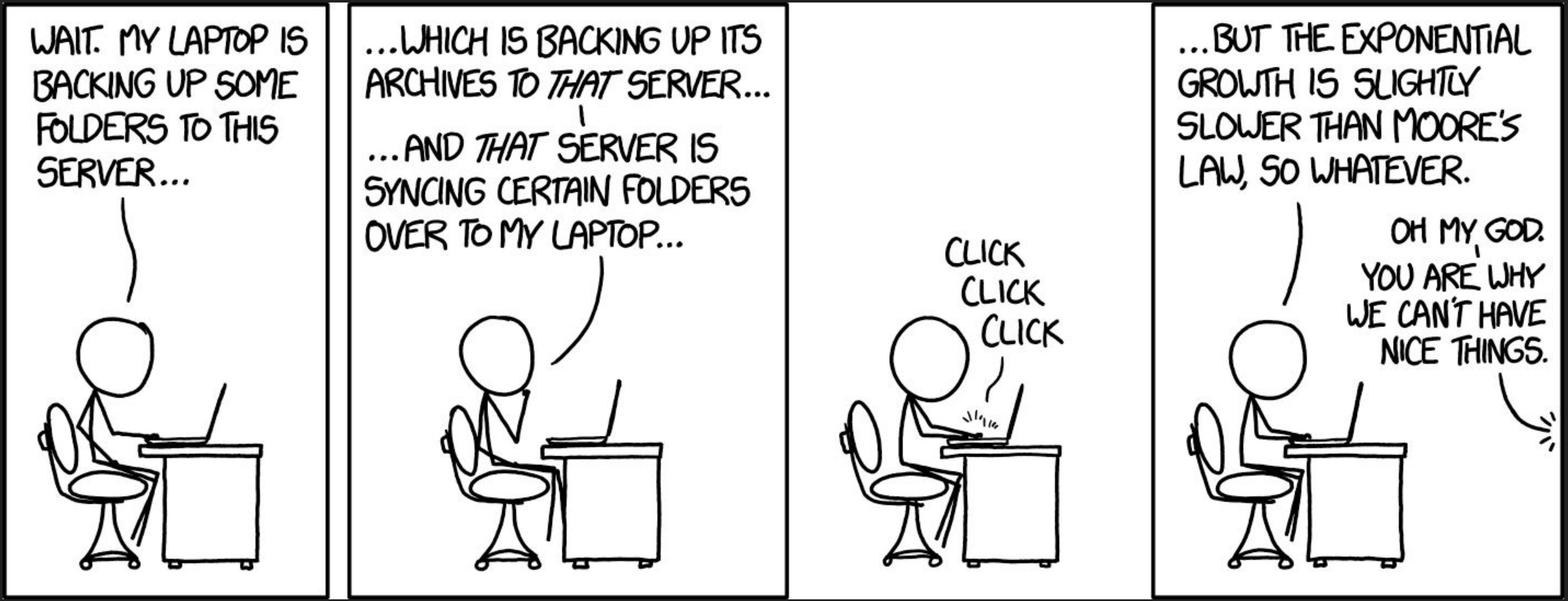
- If you are scaled for pure performance it is the same as RAID 0
  - i.e. You have 2 servers running a web-app behind a LB, both are at 75% capacity
  - If 1 of them fails, not only are you not HA, but the remaining server is at 150% load leading to failure or degraded service to users
  - For HA to truly work it requires additional resources equal to the amount you are consuming at peak load for each failure you want to tolerate

Disaster Recovery

- The vast majority of Disaster Recovery focuses on **Backups**
- What systems do you have backed up?
- How long ago is your latest backup?
- How long will it take to restore that data?

- Is there a backup server, data center, or infrastructure to restore to?
- How long before that is available?
- Is the hardware, operating systems, software, etc on those systems up to date?

Let’s talk about Backups


WAIT. MY LAPTOP IS BACKING UP SOME FOLDERS TO THIS SERVER...
...WHICH IS BACKING UP ITS ARCHIVES TO THAT SERVER...
...AND THAT SERVER IS SYNCING CERTAIN FOLDERS OVER TO MY LAPTOP...
CLICK CLICK CLICK
...BUT THE EXPONENTIAL GROWTH IS SLIGHTLY SLOWER THAN MOORE'S LAW, SO WHATEVER.
OH MY GOD.
YOU ARE WHY WE CAN'T HAVE NICE THINGS.

Let’s talk about Backups

Different Types of Backups

- **Full Backups**
  - The most basic of the backup types
  - Comprehensive backup of all data on a system
- **Incremental Backups**
  - Backs up only the information that has changed since the last backup occurred
- **Differential Backups**
  - Similar to an incremental backup
  - Backs up only data changed since the last full backup every time it is run

These concepts can apply to several types of backups - file system, vm snapshot, database, etc

Backup Types Example

Day of the week	Events	Full Backup	Incremental	Differential
Sunday		Sunday - Full	No Change	No Change
Monday	Change A		Saves A	Saves A
Tuesday	Change B		Saves B	Saves A+B
Wednesday			No Change	Saves A+B
Thursday	Change C		Saves C	Saves A+B+C
Friday			No Change	Saves A+B+C
Saturday	Change D		Saves D	Saves A+B+C+D
Sunday - 2		Sunday - Full	No Change	No Change

Where do we put the backups?

- Ideally, all critical backups should be stored in 2 places
    - One on-site for quick recovery
    - One off-site for larger scale disaster

- Similar to actual data, backups should be stored on a solid storage architecture
    - RAID Arrays
    - SAN/NAS

- Leverage cloud storage for off-site backups
    - Amazon S3/Glacier/Etc
    - Google GCS
    - Azure Blobstore

How long should we keep backups?

Data retention depends on quite a few factors

- Compliance
  - Are you required to keep data for a period of time?
  - HIPAA - 5 years since last patient contact (Up to 30 years in certain circumstances)
- Storage budget
  - How much capacity do you have for backups and how often are you taking backups?
- Business requirements
  - Do you just need the last good copy in the event of a failure?
  - Do you need to go back a quarter, a year, etc in the event something was deleted?

Is is always a good idea to keep the most backups possible?

Calculating Storage Requirements

- Assumptions
  - Retention period of 28 days
  - Initial data size of 100G
  - Daily increase in data of 5G
- Compare size requirements of
  - Full backups daily with full backups weekly and incremental daily
  - Full full backups weekly and incremental daily with full backups weekly and differential daily
- Full Backups daily
  - ∑(100+5i) [i from 0 to 27] = 4690G
- Full backups weekly and incremental daily
  - Full backups: 100 + (100+7*5) + (135+7*5) + (170+7*5) = 610G
  - Incremental: 28 * 5 = 140G
  - Total: 750G

What about security?

- Backups of critical data should be treated with the same severity as the live data

- Encryption! - Both at rest and in transit

- Backups are a target for data exfiltration and destruction and are often less secure in implementation

Defense in depth

If budget allows, have multiple levels of backups for additional protection

- Take a database for example
  - Dump the database
  - Get a filesystem backup of the database VM (configs/database files/etc)
  - Snapshot the database VM itself

- The more levels of redundancy you have the safer you are
  - This also gives you options depending on what the issue is and the level to which you need to restore/rebuild

Testing your backups

A common flaw of a backup system is setting and forgetting it

- Test your backup system often

- If you only try to do a restore when you need to, you may find its been broken for a while and you don’t have the data you thought you did

- Audit your backups
  - What new systems have been introduced? Are the backed up?
  - Are the existing backups covering everything for existing systems?
  - Are the backup windows and retention policies still accurate for those workloads?

References

- CISA® Manual, ISACA
- Certified Information Systems Auditor, Peter H Gregory, McGraw-Hill
- Business Continuity & Disaster Recovery Planning, Cybrary.it
- Business Continuity & Disaster Recovery, Javaid
- RAID Diagrams/Explanations - en.wikipedia.org/wiki/Standard_RAID_levels
- SolarWinds - Backup and Recovery Whitepapers