Applied Virtual Networks

COMP 4912

Instructor: **Dawood Sajjadi**

PhD, SMIEEE, CISSP

ssajjaditorshizi@bcit.ca

Winter-Spring 2025

Week #9

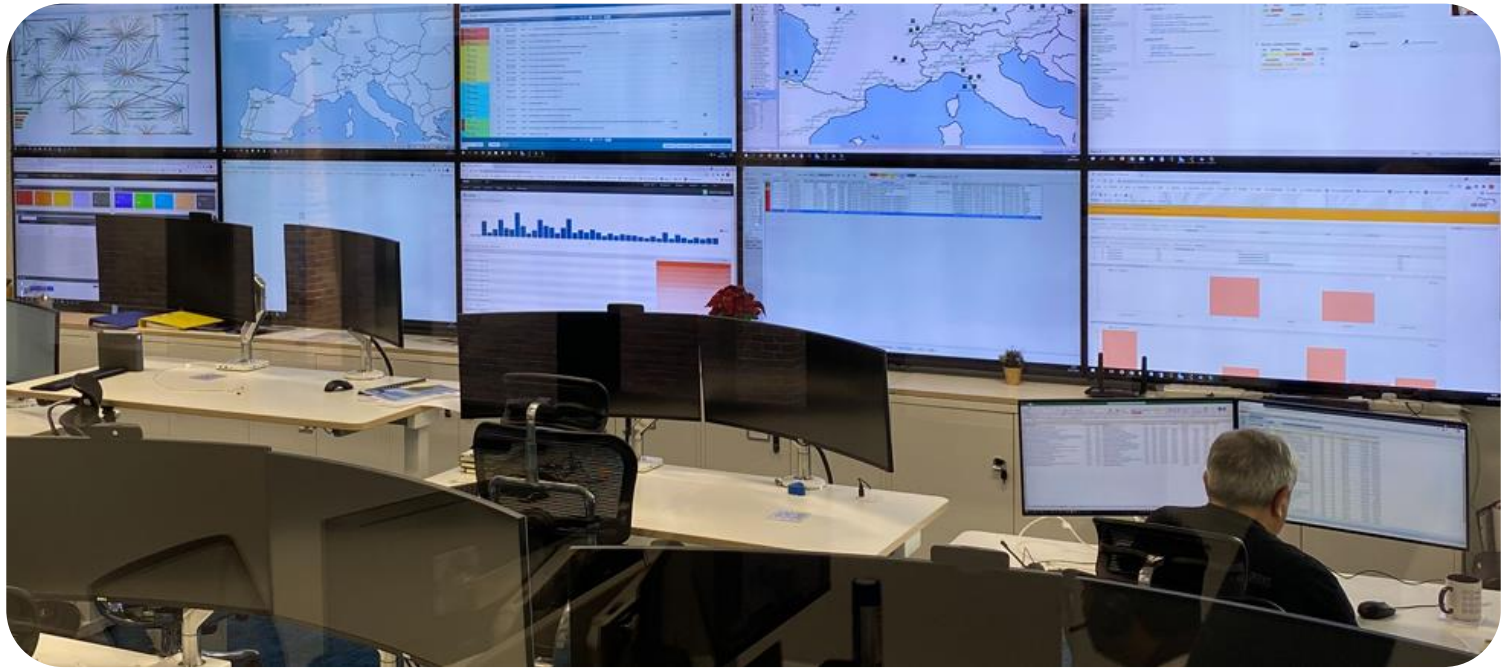
BCIT™

Monitoring an IT Infrastructure

RECAP

- **Ensure System Reliability** – Detect and prevent failures before they impact operations.
- **Performance Optimization** – Identify bottlenecks and optimize resource utilization.
- **Early Threat Detection** – Spot security vulnerabilities and respond to anomalies in real time.
- **Cost Efficiency** – Reduce downtime and optimize IT spending by identifying inefficiencies.
- **Minimize Downtime** – Proactive monitoring helps avoid costly service disruptions.
- **Compliance & Auditing** – Maintain logs and reports to meet regulatory requirements.
- **Capacity Planning** – Predict future growth and scale infrastructure accordingly.
- **Root Cause Analysis** – Quickly identify and troubleshoot system issues.

Network
Operation
Center



Security
Operation
Center

BCIT™

Metrics for Service Monitoring

RECAP

There are several known metrics that help to define service **Reliability, Availability, and Disaster Recovery strategies.**

SLO (Service Level Objective)

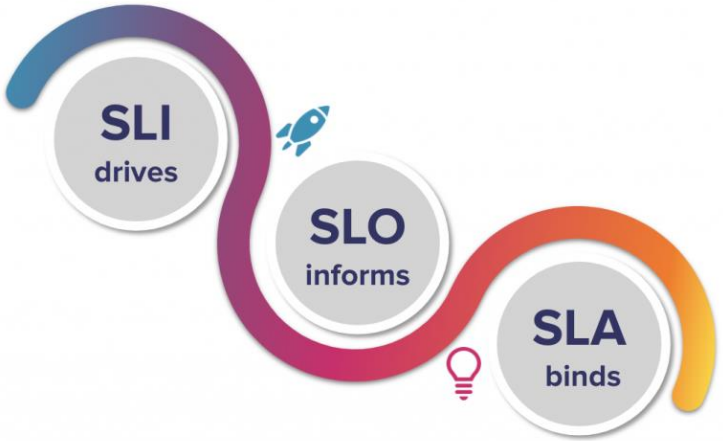
- ✓ A **targeted performance goal** used internally by service teams.
- ✓ Defines desired service levels (Latency < 100ms, or Uptime > 99.95%).

SLA (Service Level Agreement)

- ✓ A **formal contract** between a service provider and a customer.
- ✓ Defines **minimum service guarantees** (e.g., 99.99% uptime).
- ✓ Includes **penalties** if the provider fails to meet commitments.

SLI	SLO	SLA
service level **indicator**: a well-defined measure of 'successful enough'	service level **objective**: a top-line target for fraction of successful interactions	service level **agreement**: consequences
• *used to specify SLO/SLA*	• *specifies goals (SLI + goal)*	• *SLA = (SLO + margin) + consequences = SLI + goal + consequences*
• *Func(metric) < threshold*		

- ✓ **SLI:** current measured API latency is **160ms**
- ✓ **SLO:** **internal target latency < 150ms**
- ✓ **SLA:** guaranteed max latency to customer is **< 170ms**
  There will be a penalty & legal action for breach of SLA



BCIT™

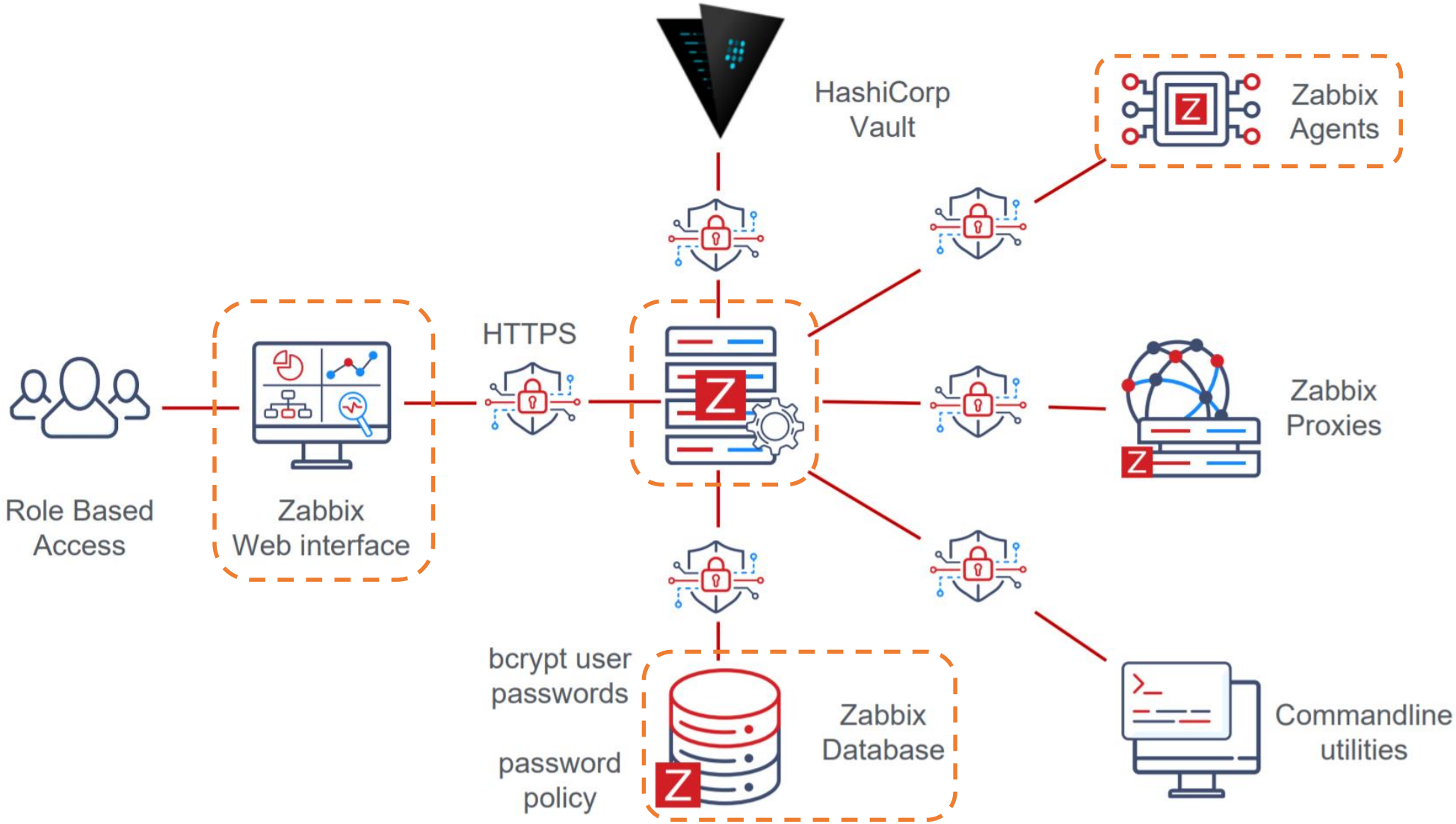
Monitoring an IT Infrastructure

RECAP

ZABBIX

https://www.zabbix.com

Zabbix Structure



BCIT™

SNMP Versions

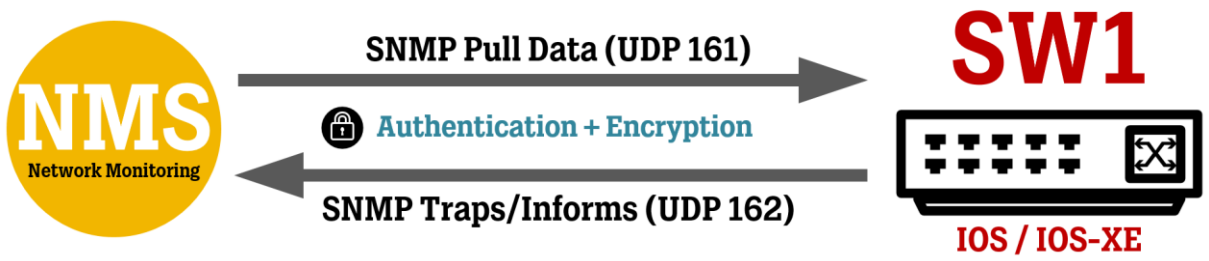
RECAP

- SNMP comes in three versions: SNMPv1, SNMPv2c, and SNMPv3.
- SNMPv3 is the most Secure version.

SNMPv1: Basic functionality, no security.

SNMPv2c: Improved performance, still uses community strings.

SNMPv3: Security enhancements (Authentication & Encryption).



SNMPv1	SNMPv2c	SNMPv3
Easy to set up	Easy to set up	Hard to set up
Less Efficient	Less Efficient	More Efficient
Supports 32 bits counters	Supports 64 bits counters	Supports 64 bits counters with security
Plain-text community string	Improved error handlingand SET commands	Adds encryption and authentication
Packet Types: • Get-Request • Get-Next-Request • Set Request • Get Response	Packet Types: • Get-Request • Get-Bulk-Request • Get-Next-Request • Set Request • Inform-Response • SNMP v2 Trap	Basic functions are like v1 & v2 New packet types for SNMPv3

BCIT™

Syslog

RECAP

- ✓ **Syslog** is a standard protocol for **Logging System Messages**.
- ✓ It allows **Applications** and **Systems** to send logs to a **Centralized Location**.
- ✓ Used for **Monitoring**, **Troubleshooting**, and **Security** analysis.

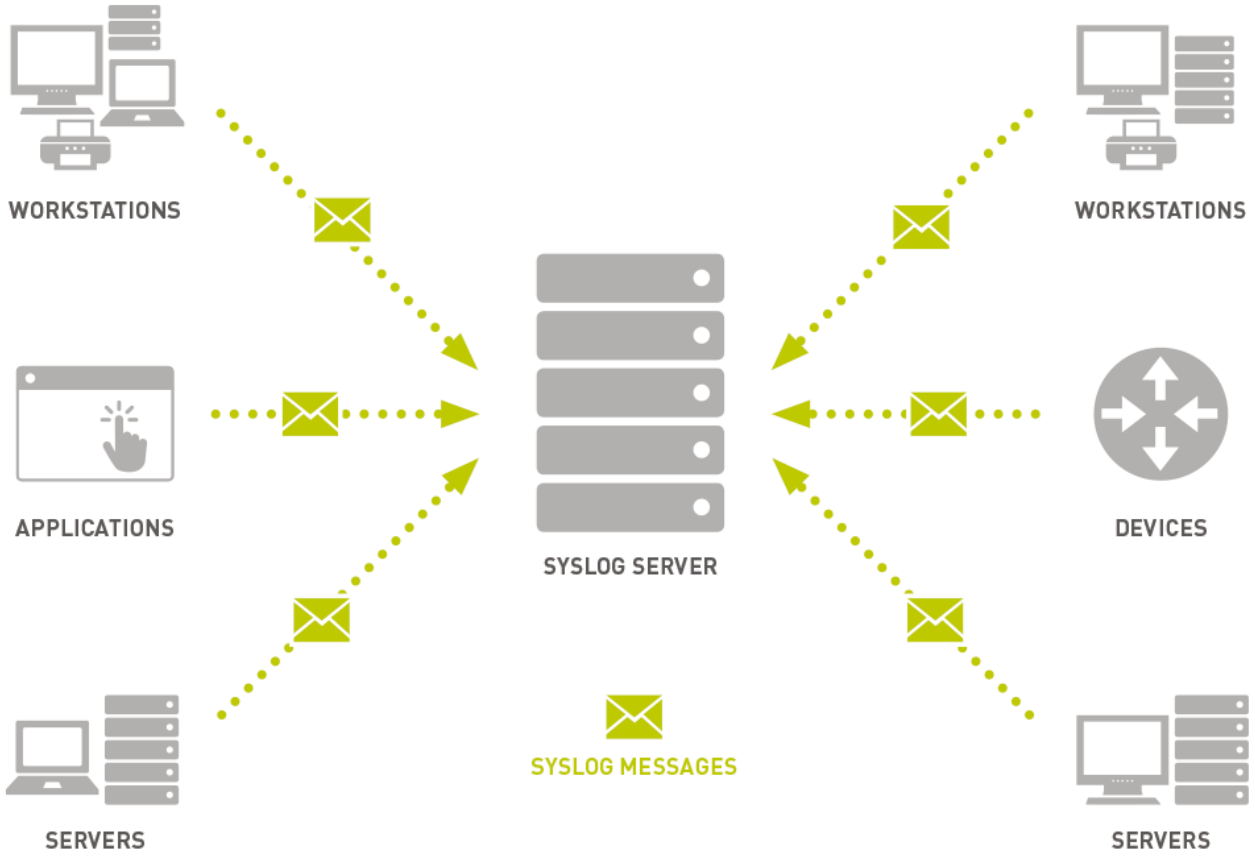
Components of Syslog

Log Generators – Applications/System processes that create logs.
Syslog Daemon - Manages log processing and forwarding .
Log Storage/Server - Collects and stores logs centrally for analysis.

Syslog Message Format

Priority (PRI) - Severity and facility level.
Timestamp - When the log was generated.
Hostname - The system that sent the log.
Application name - Source of the message.
Message Content - The actual log details.

<34> Mar 8 10:15:22 myserver sshd[1234]: Failed login attempt



BCIT™

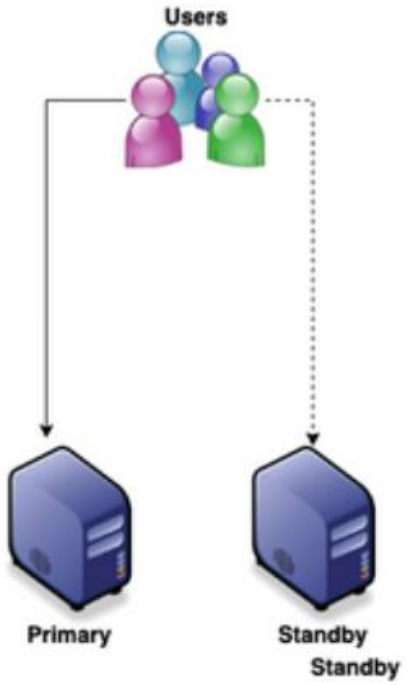
Learning Outcomes of Week #9

1. Understand the core concepts of Disaster Recovery (DR).
2. Exploring different options to provide Redundancy for Internet services.
3. Delineating Hardware/Software requirements for having High Availability.
4. Understanding Business Continuity and RPO/RTO/RSL concepts.
5. Describing Backup technologies and mechanisms.
6. Explaining roles of LB/Network protocols in providing service availability.

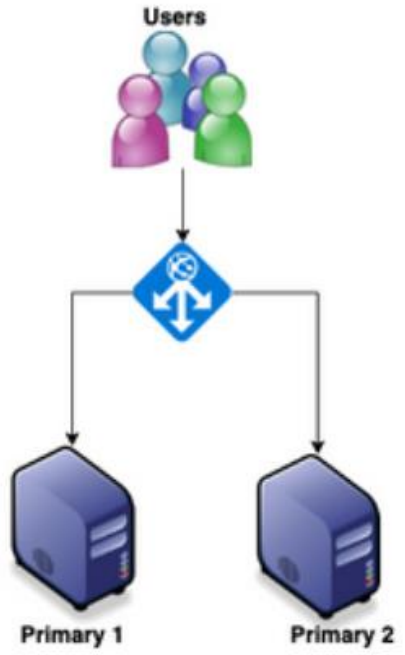
BCIT™

HA vs. FT vs. DR

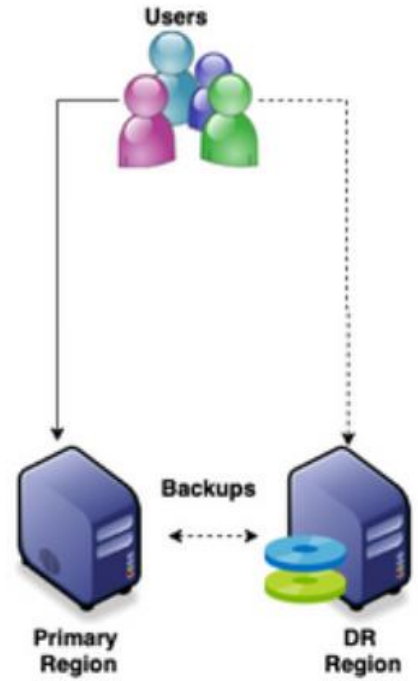
High Availability



Fault Tolererance



Disaster Recovery



BCIT™

HA vs. FT vs. DR

What is High Availability (HA)?

It is defined as a characteristic of a system which aims to **ensure an agreed level of operational performance**, usually Uptime, for a **higher than normal** period. High Availability does not mean that the systems will not have failure and downtime. An Highly Available system can have downtime but the systems should be designed to be up and running with minimal efforts in case of a failure. These efforts can be manual or automated.

What is Fault Tolerance (FT)?

It is the property that enables a system to continue operating properly in the event of the failure of one or more faults within some of its components. A **Fault-Tolerant Design** enables a system to continue its intended operation, possibly at a reduced level, rather than failing completely, when some part of the system fails.

What is Disaster Recovery (DR)?

It is a set of **policies, tools and procedures** to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. **Disaster Recovery** assumes that the primary site is not recoverable (at least for some time) and represents a process of restoring data and services to a secondary survived site, which is opposite to the process of restoring back to its original place.

BCIT™

HA vs. FT vs. DR

Feature	High Availability (HA)	Fault Tolerance (FT)	Disaster Recovery (DR)
Focus	Minimize downtime	Prevent downtime completely	Recover from major outages
Scope	Individual component failures	Individual component failures	Large-scale disruptions
Examples	Redundancy, failover	Data replication, locking	Backups, DR plans
Goal	"Five nines" uptime	Continuous operation	Restore critical functions

BCIT™

Types of Redundancy

Hardware Redundancy: Duplicate physical components (e.g., servers, storage, network, power).

Software Redundancy: Clustering and failover mechanisms.

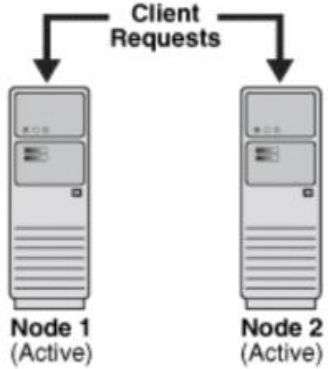
Network Redundancy: Practice of implementing backup links/devices to ensure continuous network availability.

Geographic Redundancy: Multiple sites/data centers across geographical regions.

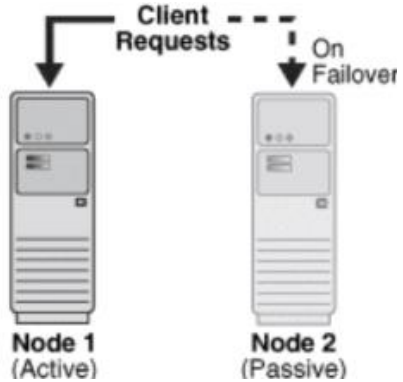
Category	Technology	Purpose	Common Use Cases
Network	HSRP/VRRP	Router failover for uninterrupted gateway connectivity	Enterprise gateway redundancy
Network	BGP Multi-Homing	Using multiple ISPs for internet redundancy	Cloud providers, ISPs, large enterprises
Network	SD-WAN	Dynamic WAN failover across multiple connections	Hybrid cloud, remote offices
Server	Failover Clustering	Automatic failover between clustered servers	Databases, file servers, enterprise apps
Server	Virtualization HA	Ensures VM continuity if a host fails	VMware HA, Hyper-V, Proxmox
Server	Database Replication	Replicates database data across multiple servers	SQL & NoSQL databases
Application	Load Balancers	Distributes traffic to multiple application servers	Web applications, microservices
Application	Kubernetes Auto-Healing	Automatically restarts failed containers	Cloud-native applications
Application	Multi-Region Deployment	Deploys services in multiple geographic locations for DR	Disaster recovery, content delivery
Hardware	Redundant Power Supply (PSU)	Prevents power failures by having dual power inputs	Enterprise data centers
Hardware	Power Distribution Units (PDU)	Distributes electrical load and prevents failures	Server racks, Power management
Hardware	RAID Storage	Protects against disk failures in storage systems	Storage arrays, cloud storage

Core HA Concepts

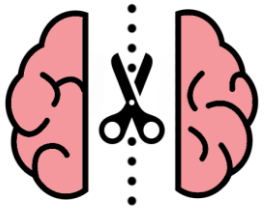
- ✓ Identify Single Points of Failure.
- ✓ Add Redundancy to eliminate Failures.
- ✓ Need Policy for how to interface with Redundant Systems.



Active/Active:
Both redundant components used in normal operation; symmetric design.
- ✓ Higher utilization and capacity/performance
- ✓ Capacity/performance is reduced on failure



Active/Passive (Primary/Secondary):
A Primary and Secondary system; secondary only does work if primary fails; asymmetric design.
- ✓ Failures don't affect capacity/performance
- ✓ Half the hardware is idle most of its life (low utilization)

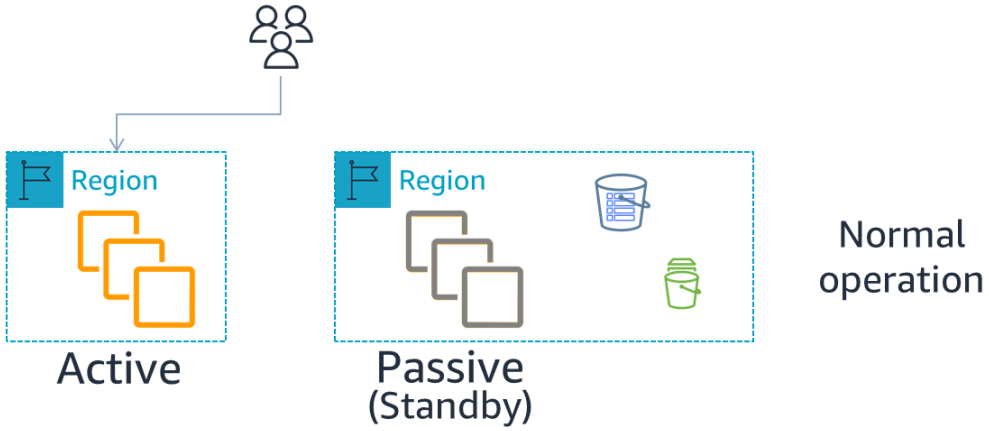


Imagine an **Active/Passive** system.
What if the two redundant systems lose contact with each other, and each thinks its time to "take over"?
Both are serving traffic and issuing commands, which lead to chaos!
Redundant computer systems must have protocol to govern takeover.

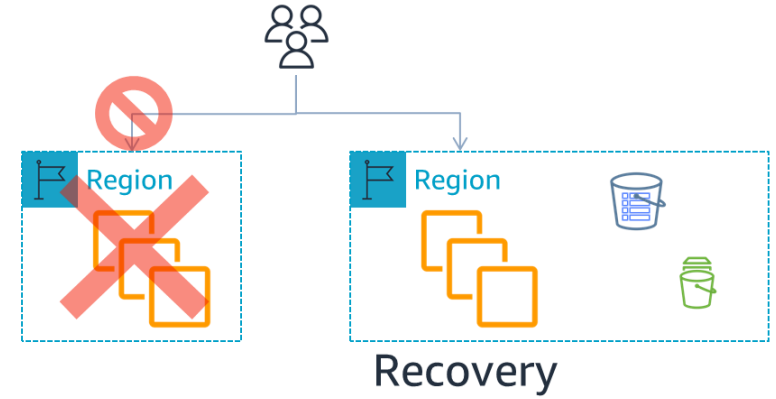
BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

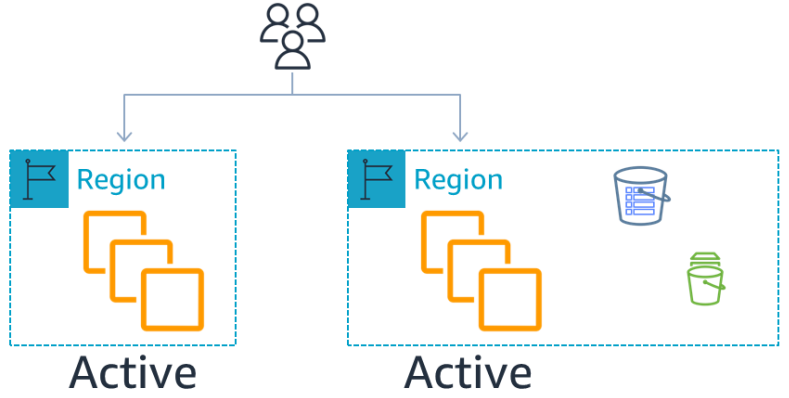
Active/Active & Active/Passive DR Strategies



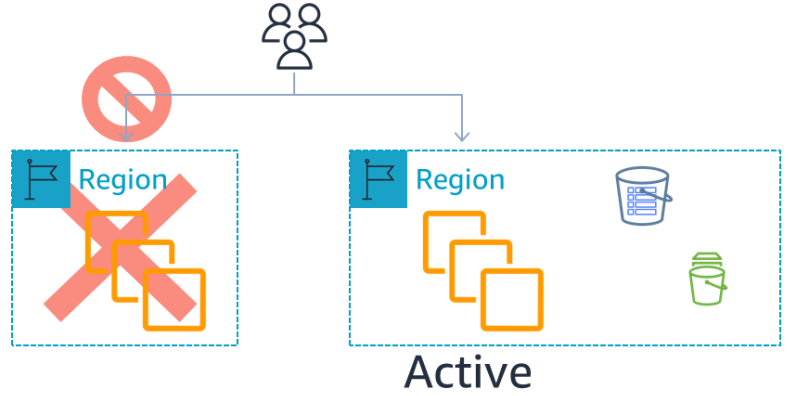
Normal operation



After a disaster event



Normal operation



After a disaster event

BCIT™

https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

Metrics for Service Monitoring

There are several known metrics that help to define service **Reliability, Availability, and Disaster Recovery strategies.**

SLO (Service Level Objective)

- ✓ A **targeted performance goal** used internally by service teams.
- ✓ Defines desired service levels (Latency < 100ms, or Uptime > 99.95%).

SLA (Service Level Agreement)

- ✓ A **formal contract** between a service provider and a customer.
- ✓ Defines **minimum service guarantees** (e.g., 99.99% uptime).
- ✓ Includes **penalties** if the provider fails to meet commitments.

RPO (Recovery Point Objective)

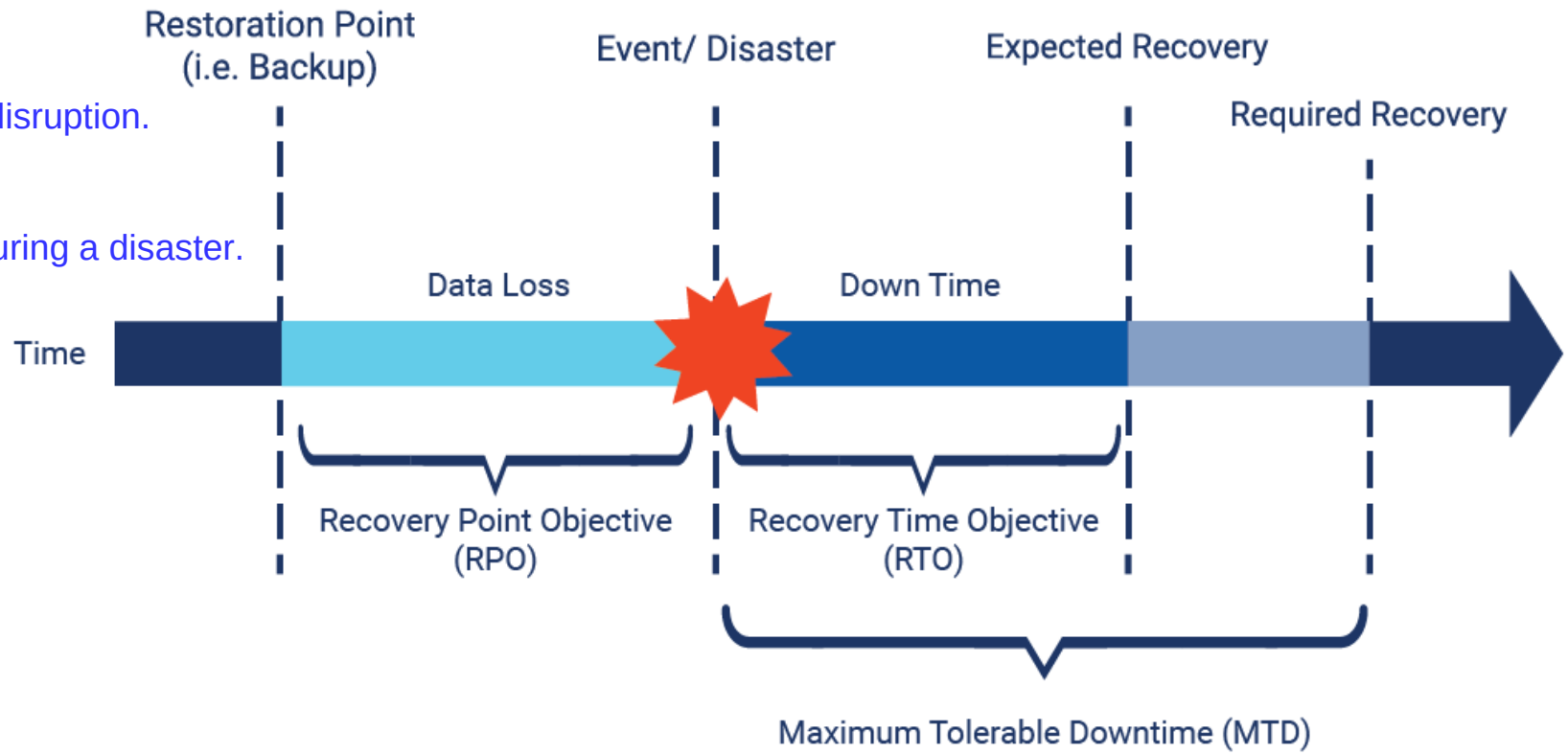
Maximum amount of data loss a company can tolerate.

RTO (Recovery Time Objective)

Maximum time allowed to restore operations after a disruption.

RSL (Recovery Service Level)

The percentage of a service that must be available during a disaster.

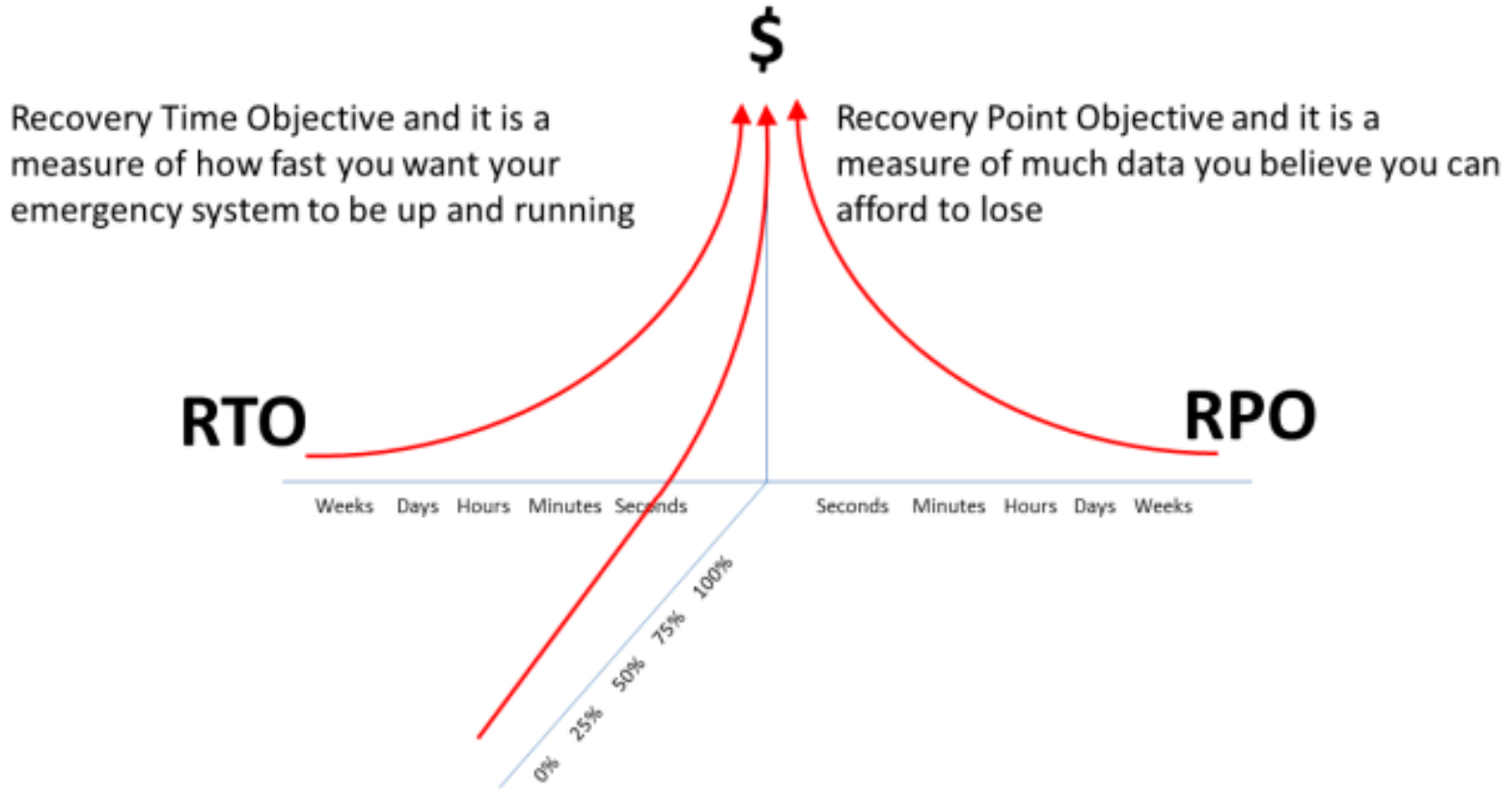


BCIT™

RPO/RTO/RSL vs. Cost

Sample Values for Selected Services

Service	RPO (hour)	RTO (hour)	RSL (%)
LDAP	15 minutes	1 hour	99.90%
DNS	5 minutes	30 minutes	99.99%
Email	30 minutes	2 hours	99.50%
Database	10 minutes	1 hour	99.95%
File Server	1 hour	3 hours	99%
Web Server	10 minutes	45 minutes	99.90%

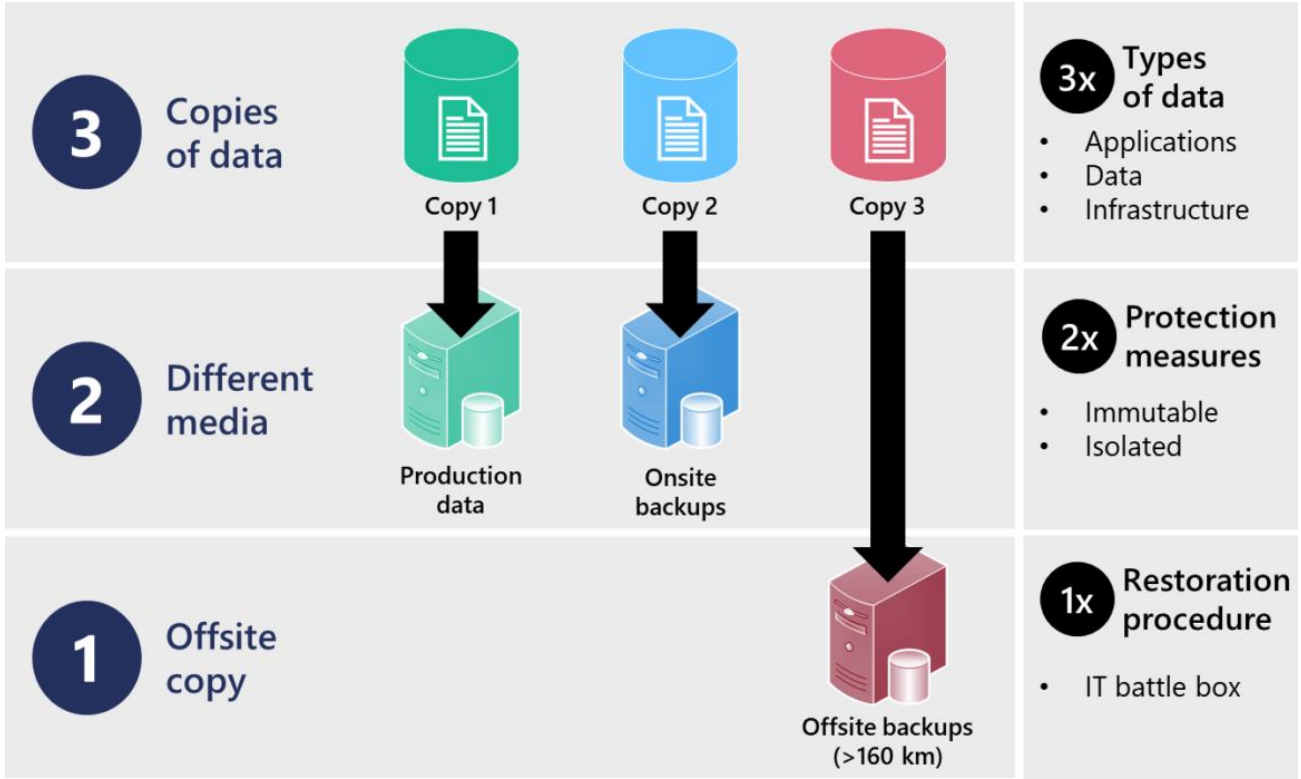


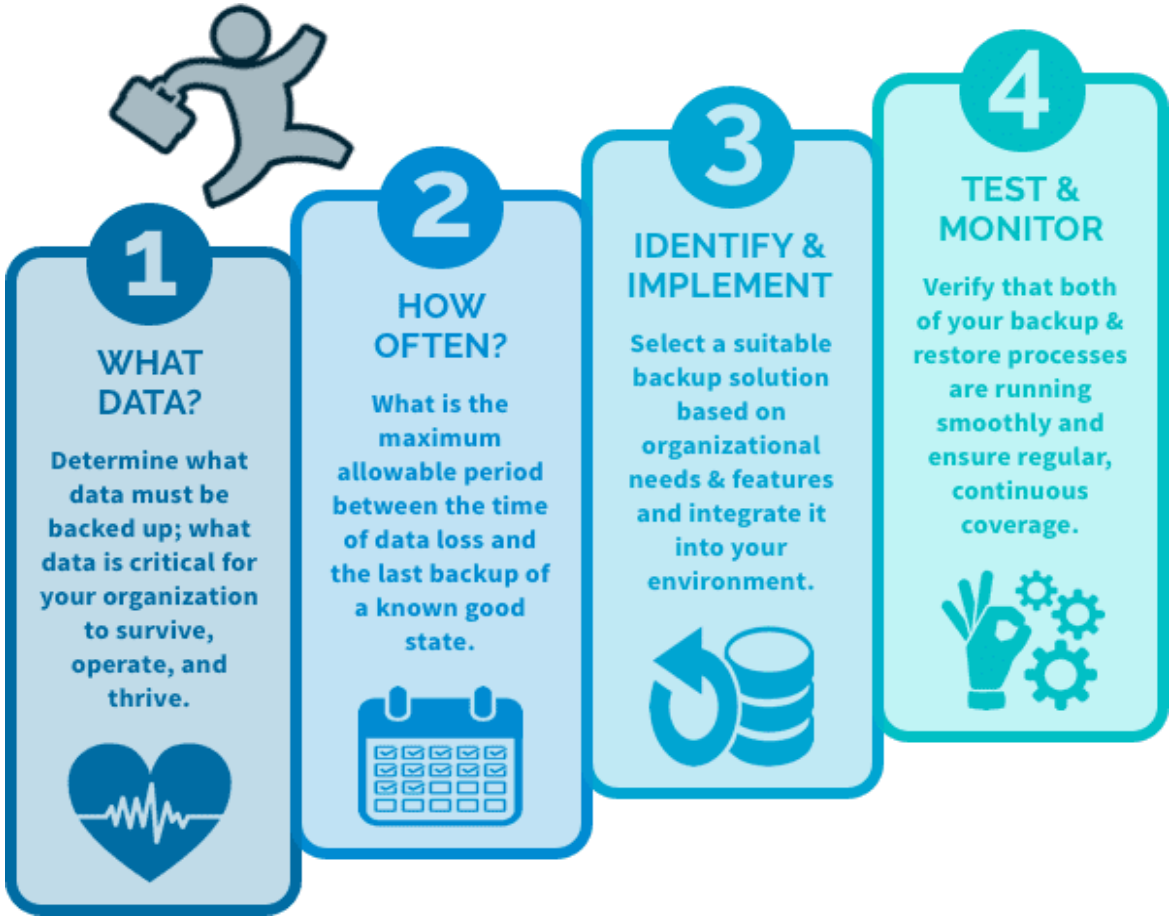
RSL Recovery Service Level and it is a measure of how what kind of computing needs are required in an emergency situation

BCIT™

Backup Strategies

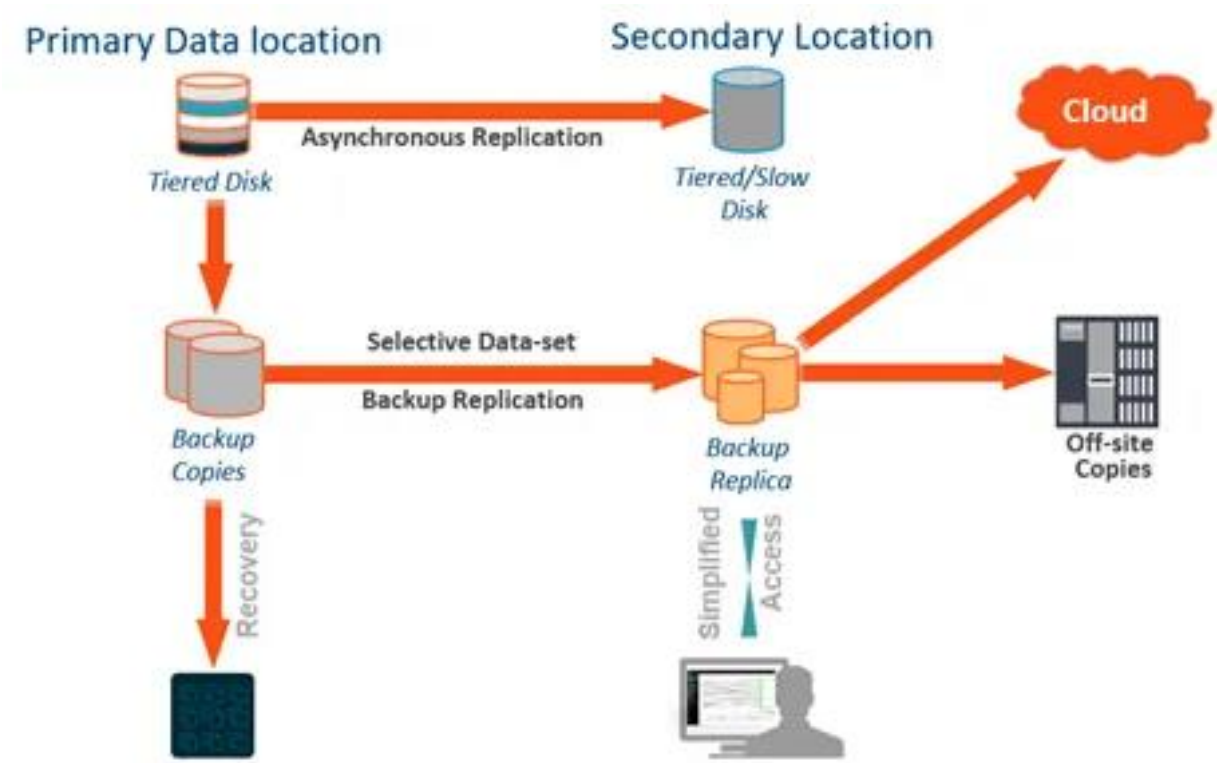
3-2-1 Backup Rule

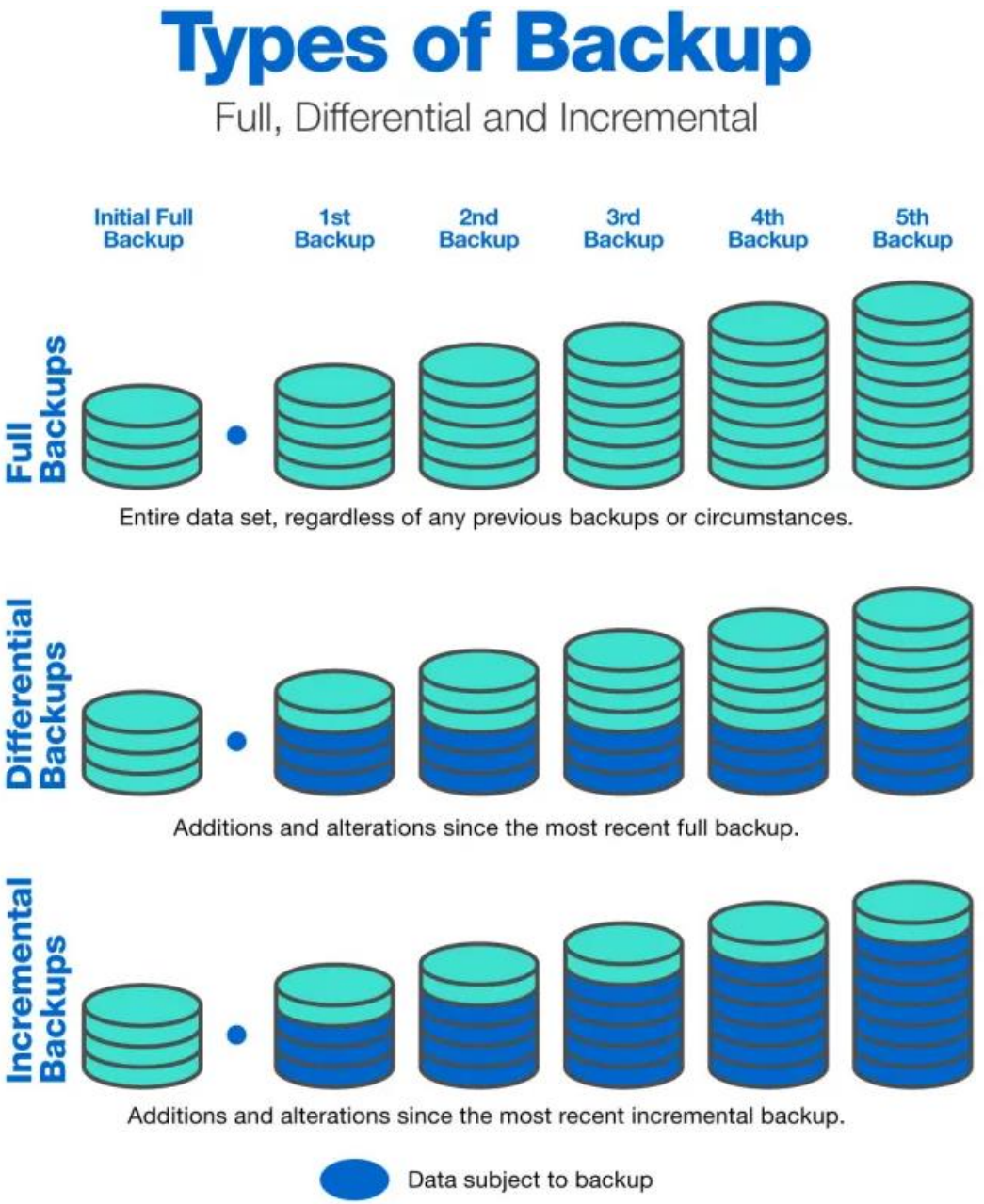




BCIT™

Backup Types



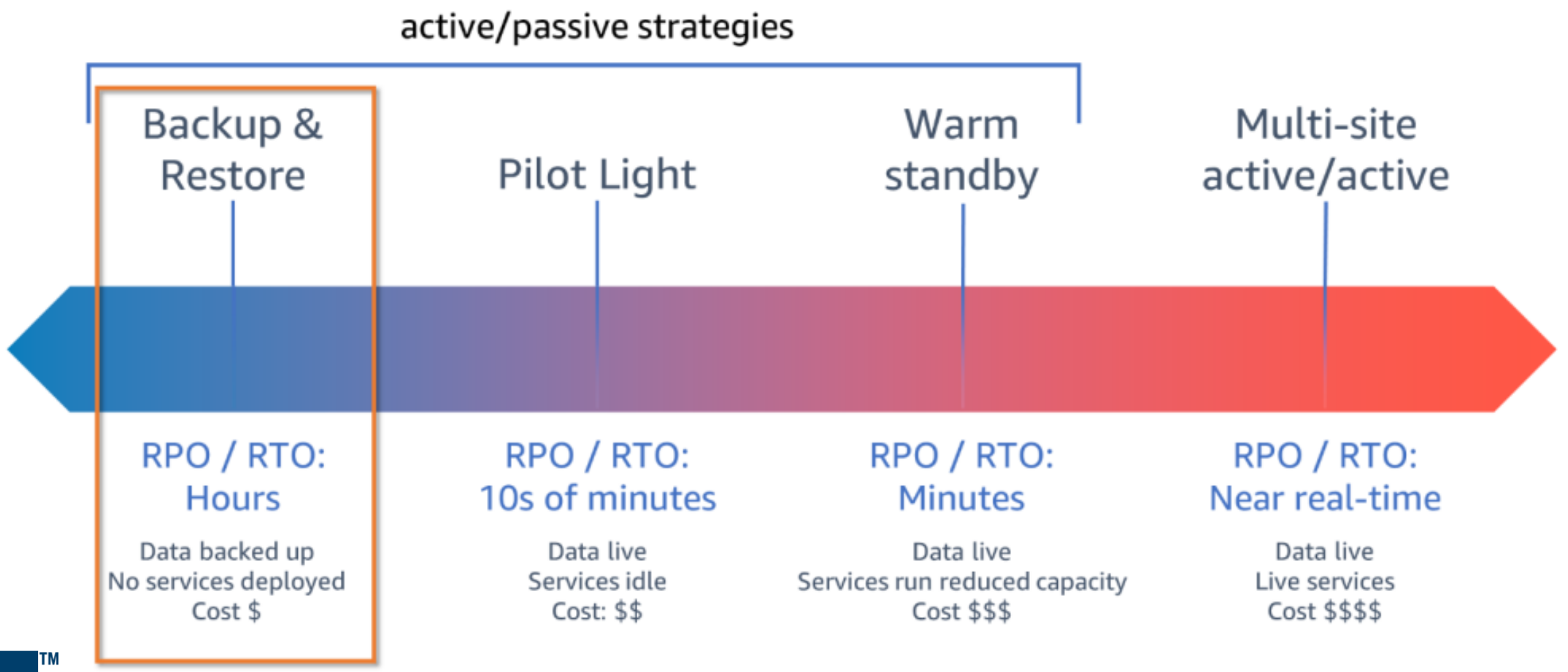


BCIT™

https://blog.quest.com/7-steps-for-creating-a-data-backup-strategy/

https://www.exabytes.my/blog/compare-incremental-full-differential-backup/

RPO/RTO/RSL vs. Cost



BCIT™

https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

Five-Nine SLA (99.999%)

MTBF (Mean Time Between Failures)

- ✓ The **average time a system runs before experiencing a failure**.
- ✓ A higher MTBF means **fewer failures**, increasing overall uptime.
- ✓ Example: If a server has an **MTBF of 200,000 hours**, it fails less frequently.

$$\text{Availability (\%)} = \left(\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \right) \times 100$$

Higher MTBF → Fewer failures → Better uptime
Lower MTTR → Faster recovery → Better uptime

MTTR (Mean Time To Repair)

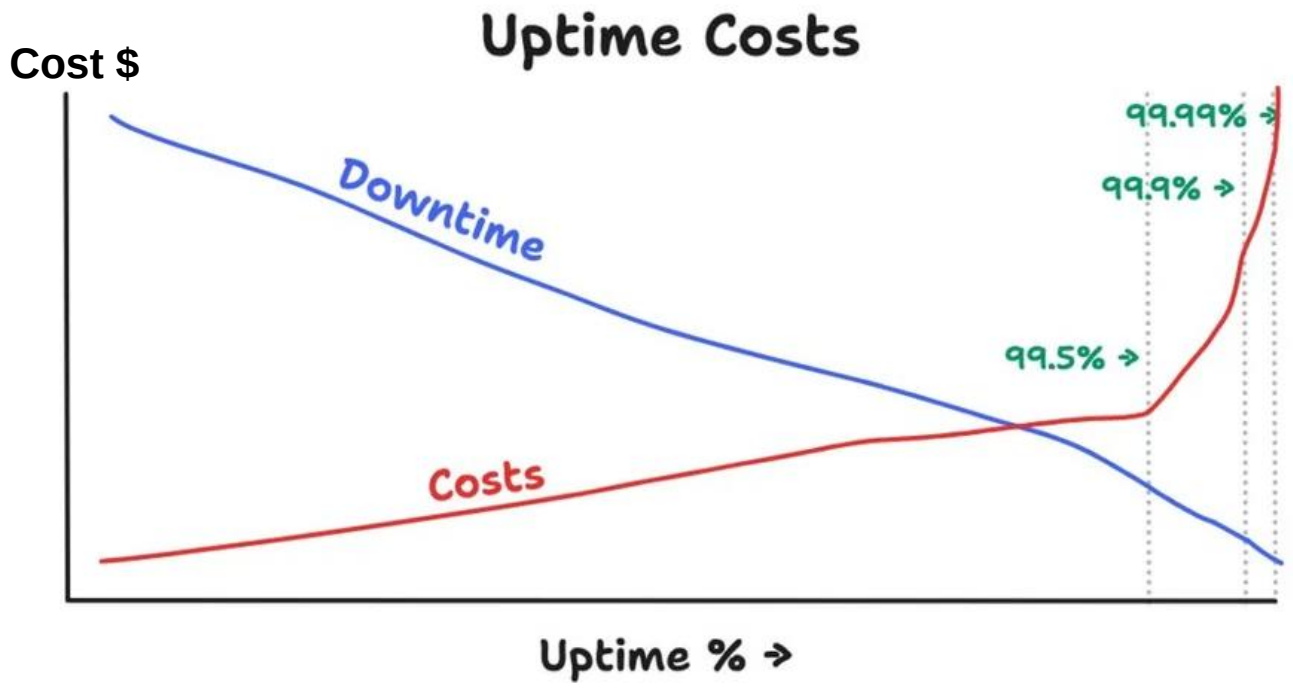
- ✓ The **average time taken to repair and restore service after a failure**.
- ✓ A lower MTTR **reduces downtime**, improving availability.
- ✓ Example: If an incident occurs and the service is restored in **5 minutes**, it helps maintain high uptime.

	Availability	Downtime / Year	Downtime / Month	Downtime / Week	Downtime / Day
5 nine →	99.999%	5.256 Minutes	0.438 Minutes	0.101 Minutes	0.014 Minutes
	99.995%	26.28 Minutes	2.19 Minutes	0.505 Minutes	0.072 Minutes
4 nine →	99.990%	52.56 Minutes	4.38 Minutes	1.011 Minutes	0.144 Minutes
	99.950%	4.38 Hours	21.9 Minutes	5.054 Minutes	0.72 Minutes
3 nine →	99.900%	8.76 Hours	43.8 Minutes	10.108 Minutes	1.44 Minutes
	99.500%	43.8 Hours	3.65 Hours	50.538 Minutes	7.2 Minutes
	99.250%	65.7 Hours	5.475 Hours	75.808 Minutes	10.8 Minutes
2 nine →	99.000%	87.6 Hours	7.3 Hours	101.077 Minutes	14.4 Minutes

BCIT™

https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/

Five-Nine SLA



	Availability	Downtime / Year	Downtime / Month	Downtime / Week	Downtime / Day
5 nine →	99.999%	5.256 Minutes	0.438 Minutes	0.101 Minutes	0.014 Minutes
	99.995%	26.28 Minutes	2.19 Minutes	0.505 Minutes	0.072 Minutes
4 nine →	99.990%	52.56 Minutes	4.38 Minutes	1.011 Minutes	0.144 Minutes
	99.950%	4.38 Hours	21.9 Minutes	5.054 Minutes	0.72 Minutes
3 nine →	99.900%	8.76 Hours	43.8 Minutes	10.108 Minutes	1.44 Minutes
	99.500%	43.8 Hours	3.65 Hours	50.538 Minutes	7.2 Minutes
	99.250%	65.7 Hours	5.475 Hours	75.808 Minutes	10.8 Minutes
2 nine →	99.000%	87.6 Hours	7.3 Hours	101.077 Minutes	14.4 Minutes

BCIT™

https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/

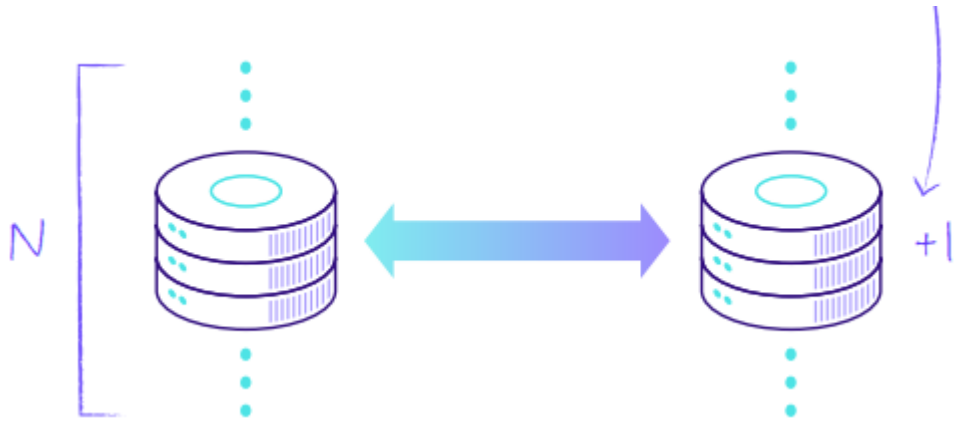
Data Centers, Engines of the Internet

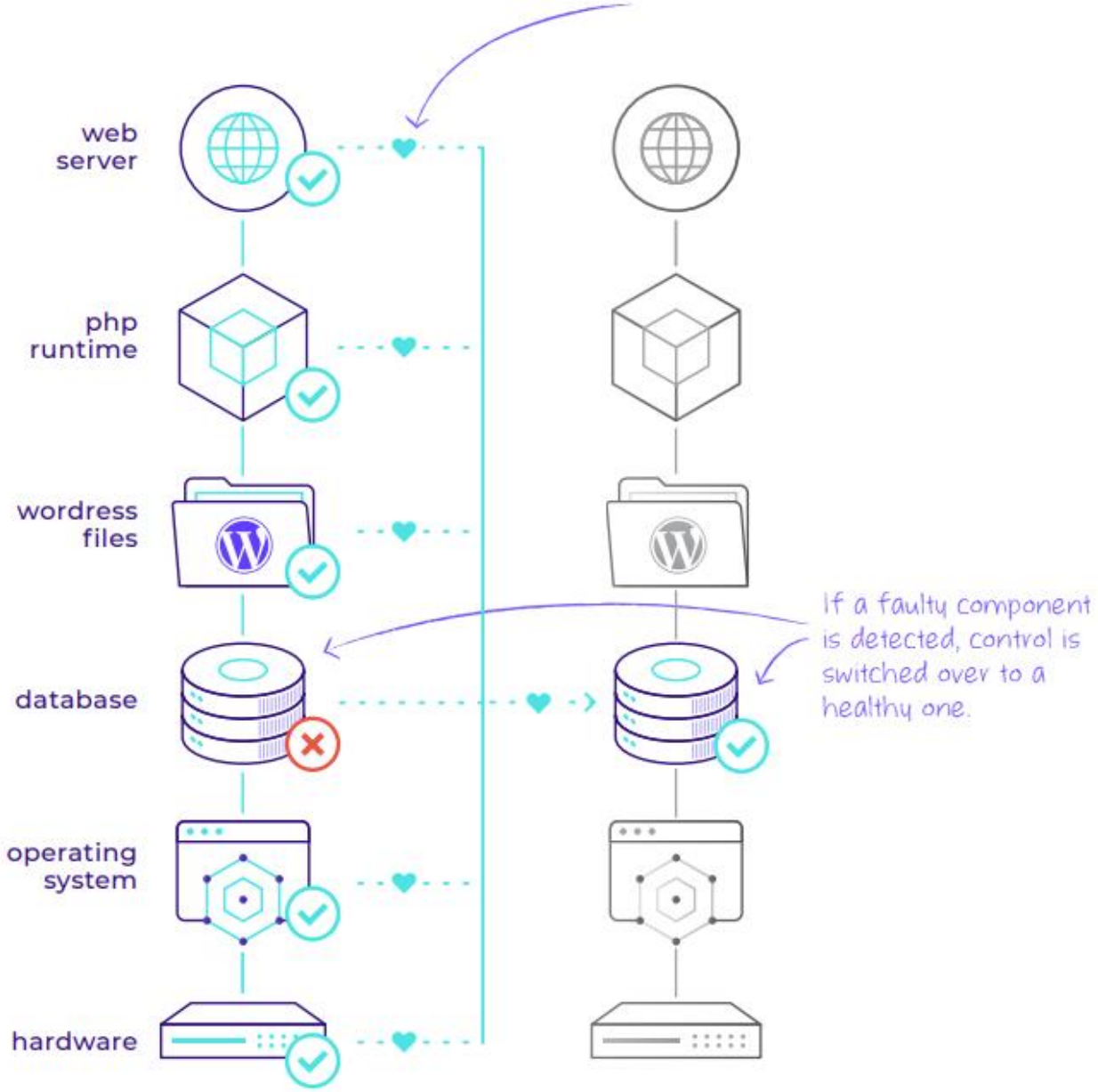
Let’s Watch https://www.youtube.com/watch?v=80aK2_iwMOs

BCIT™

Different Layers to Apply Redundancy

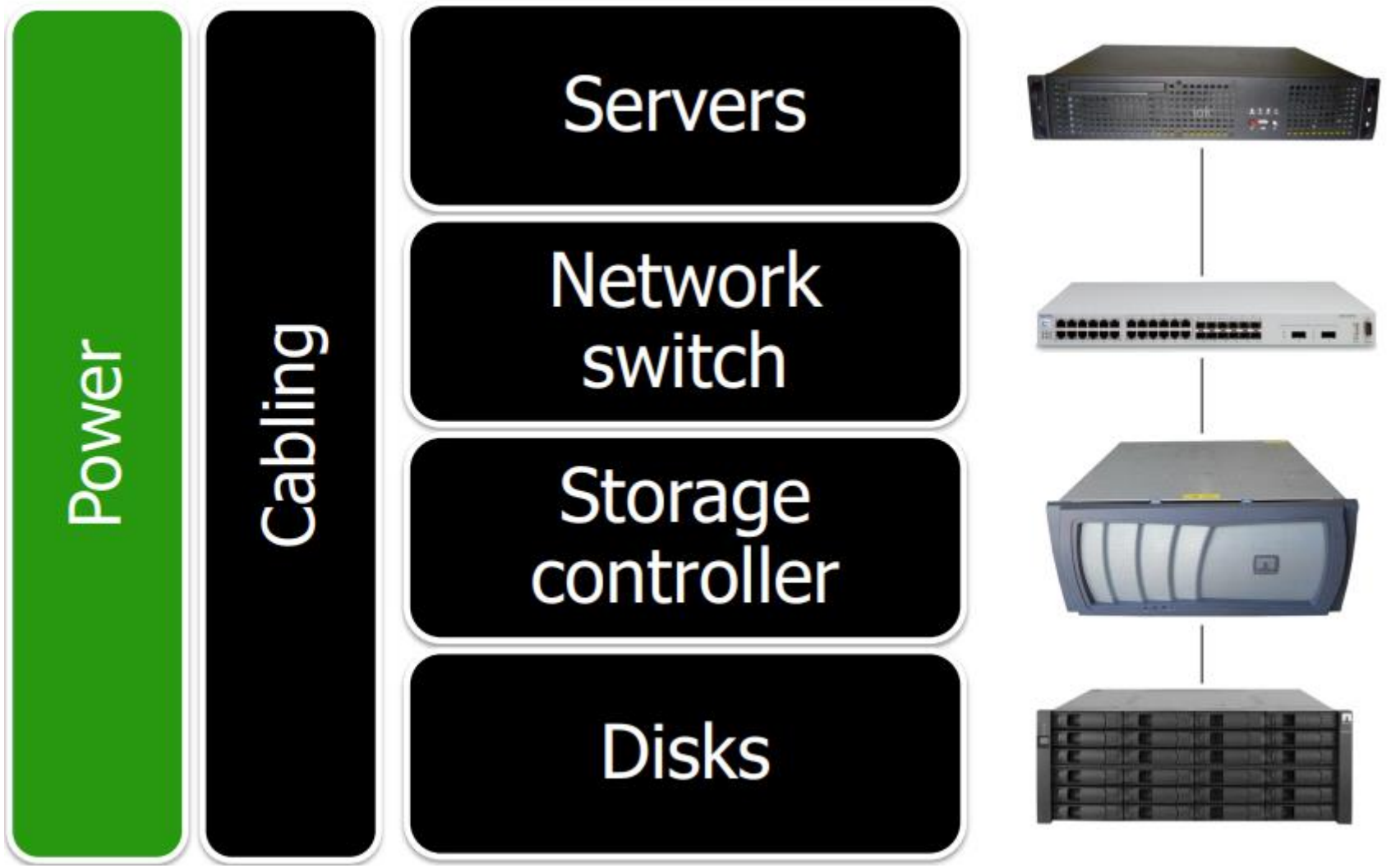
For every component, there is always one extra.
This is called **N+1** redundancy.





BCIT™

Different Layers to Apply Redundancy



https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Power)

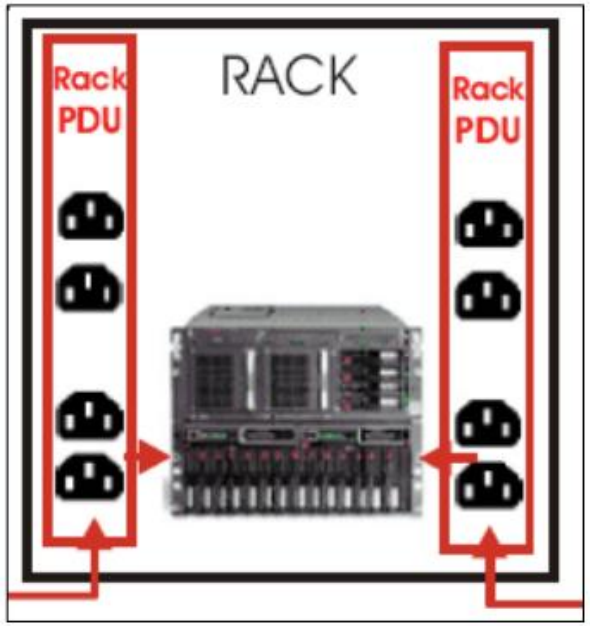
Everything has 2+ power supplies

- ✓ Equipment can survive with half its power supplies dead
- ✓ This protects against power supply failure

Power comes from Power Distribution Units (PDUs), rackmount power bars

- ✓ HA power: Racks have two PDUs
- ✓ PDU 1 hooked to “left” power supply
- ✓ PDU 2 hooked to “right” power supply

Power supplies usually hot-swappable (replaceable without downtime)

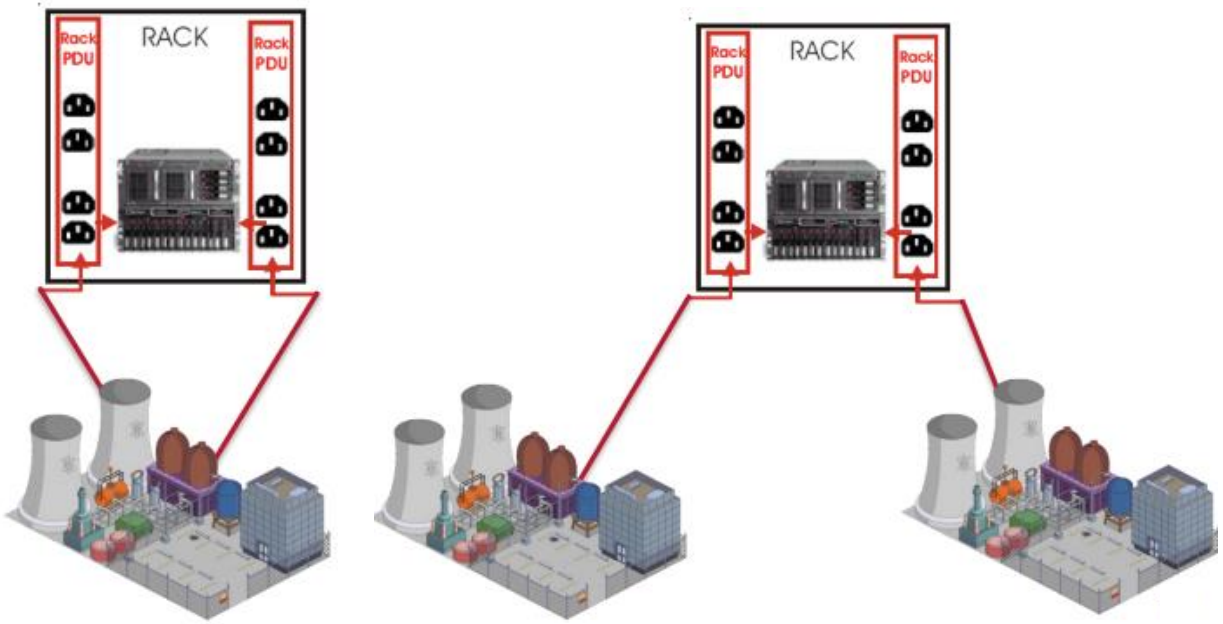


BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Power)

Utility Power (Single/Double Feed)

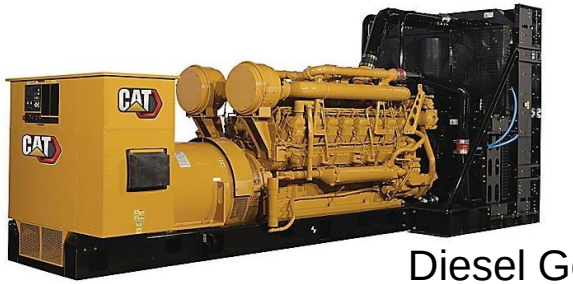


UPS: Uninterruptable Power Supply

- ✓ Takes AC power in, gives AC power out.
- ✓ Keeps a big battery array charged.
- ✓ If AC power-in fails, AC power-out comes from battery (w/o interruption).
- ✓ DC power from batteries must be converted to AC with an inverter.
- ✓ Keep things running long enough to start a gasoline/diesel generator.
- ✓ If not, keep things running, long enough for graceful shutdown.

Rackmount UPS

Building-scale battery array

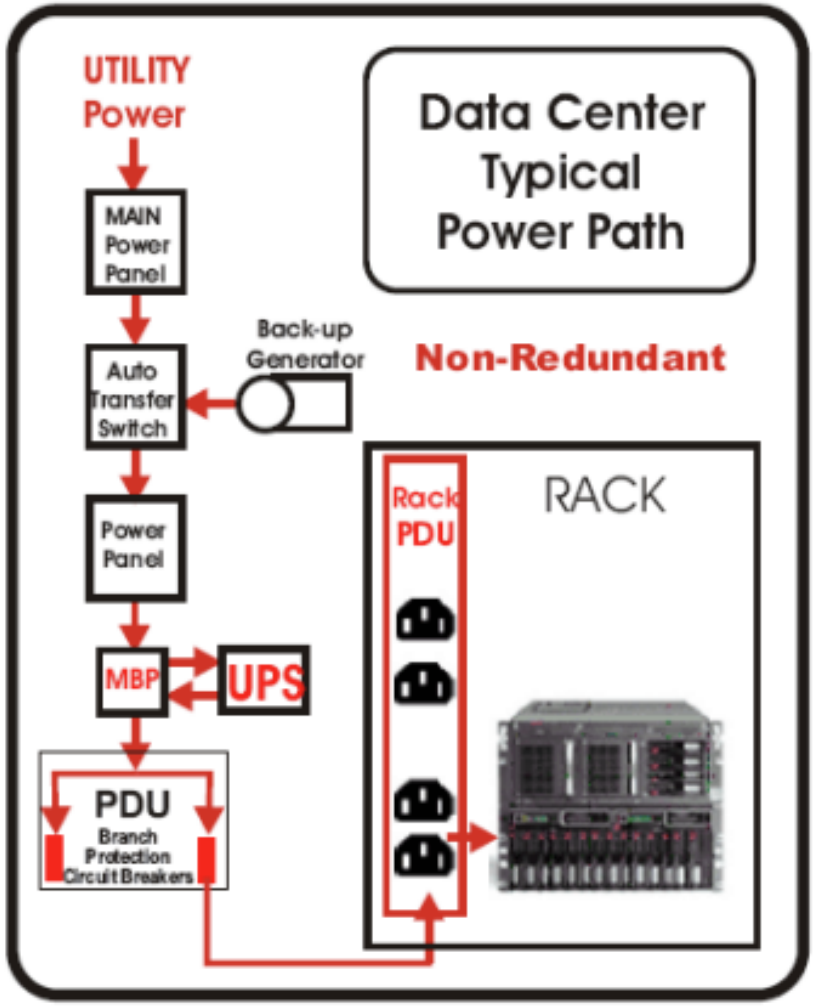


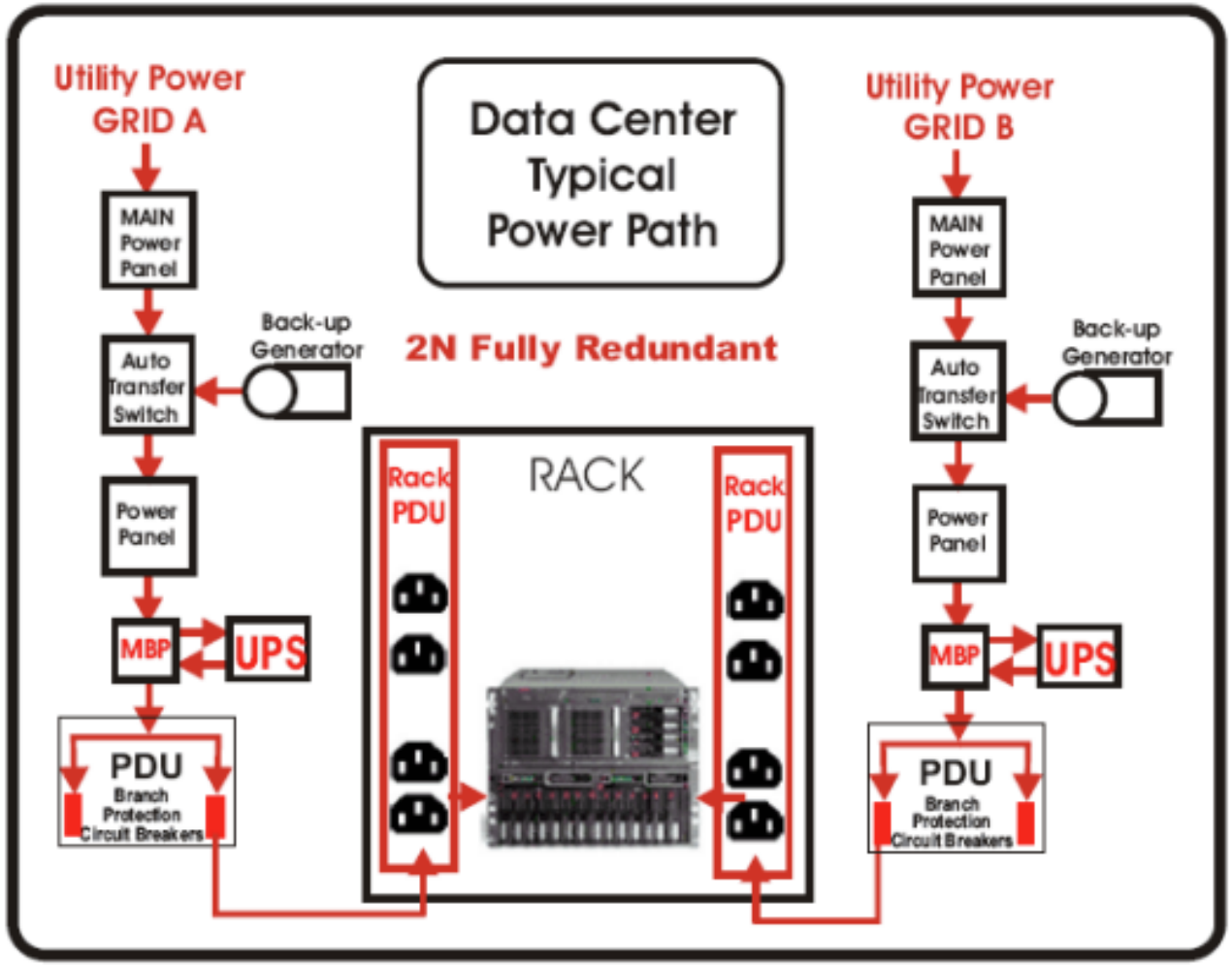
Diesel Generator

BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Power)

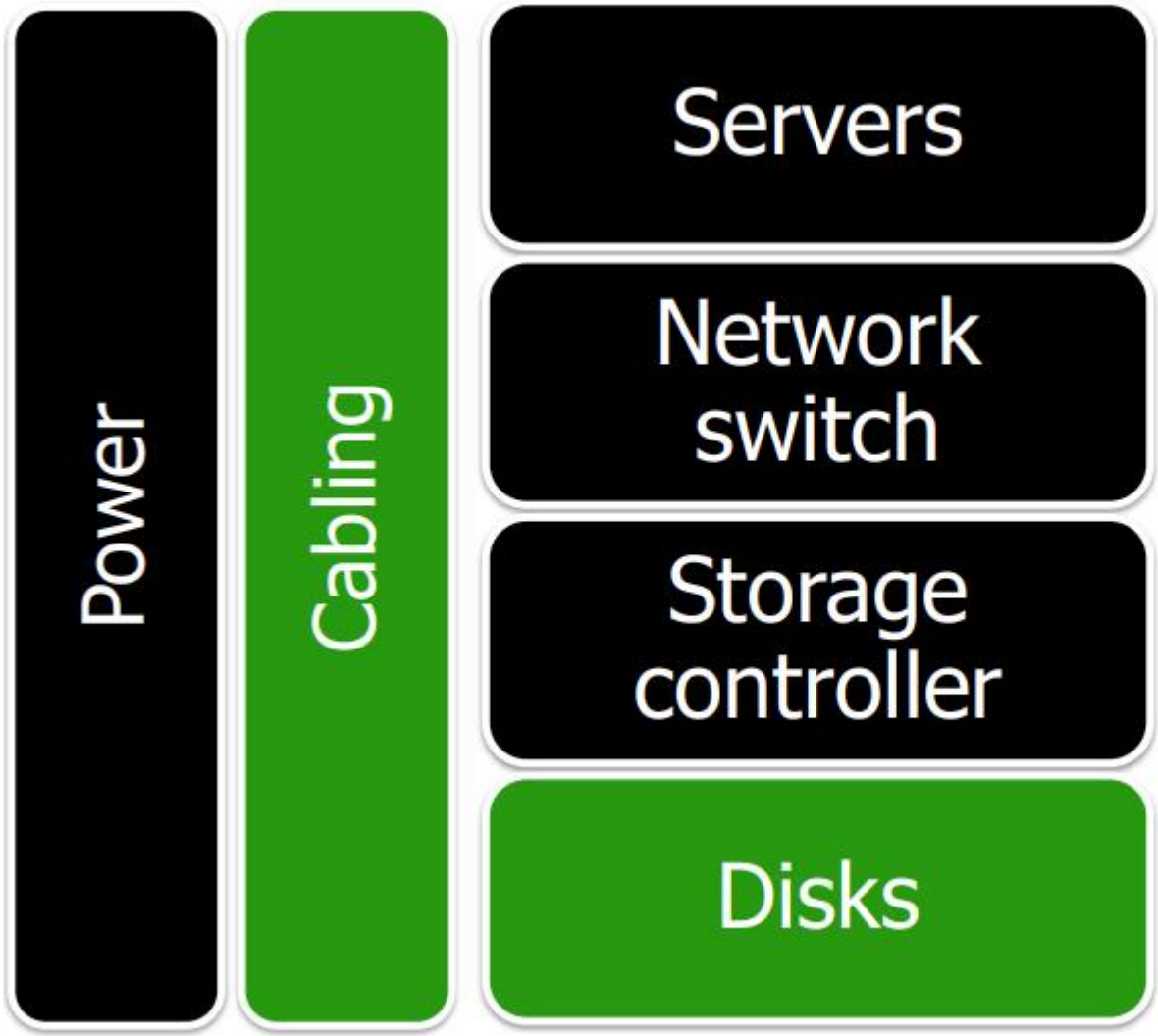




BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

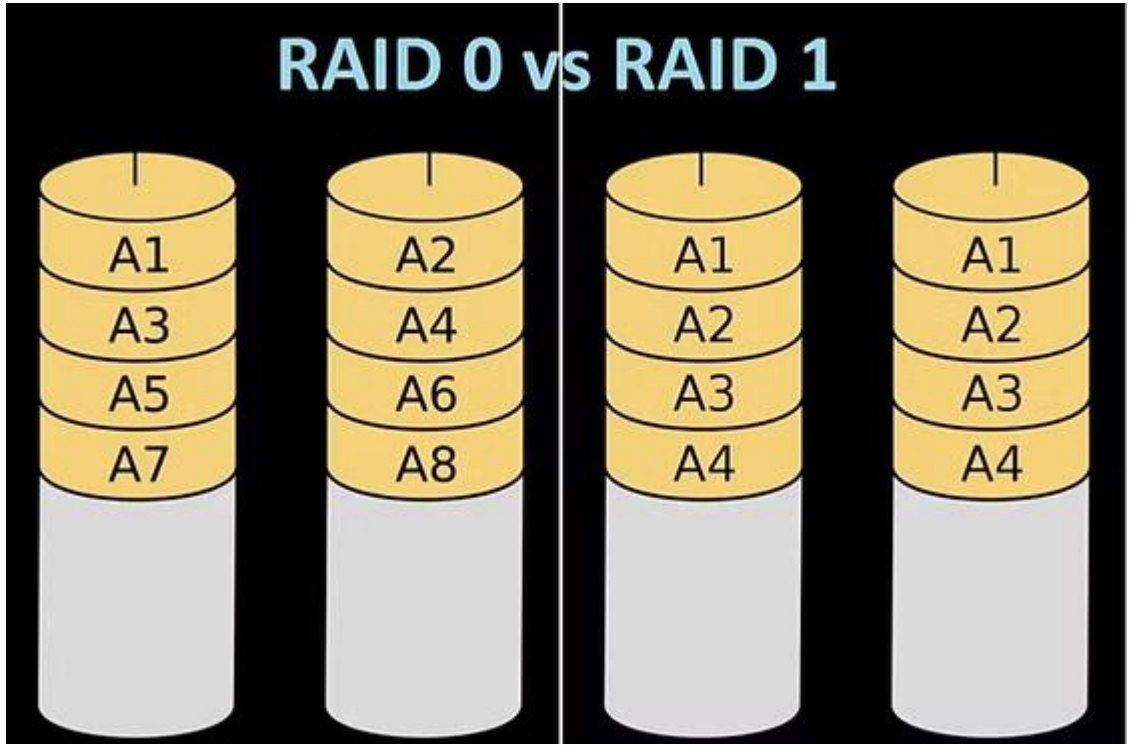
Different Layers to Apply Redundancy

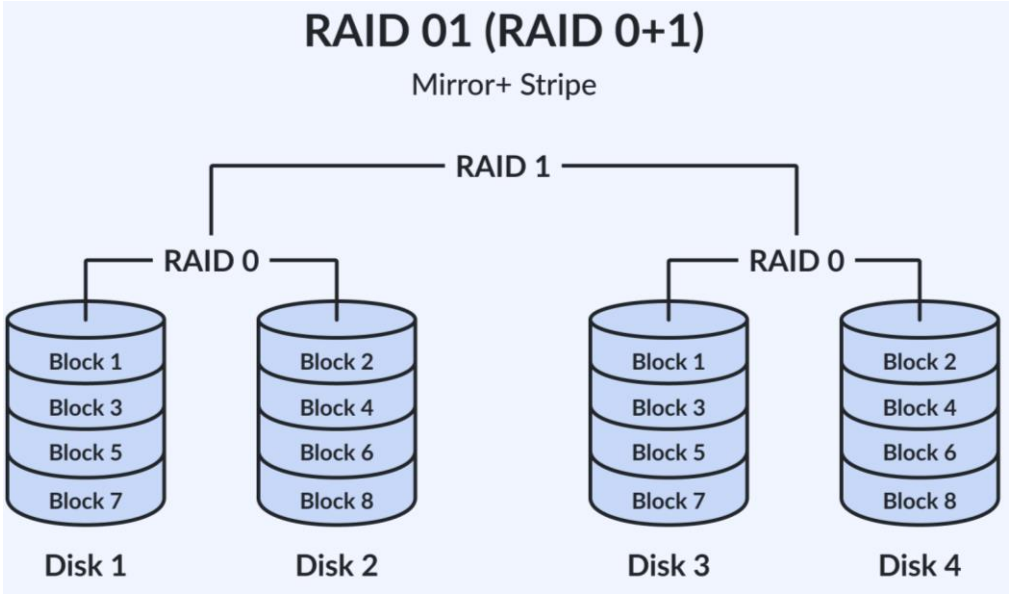


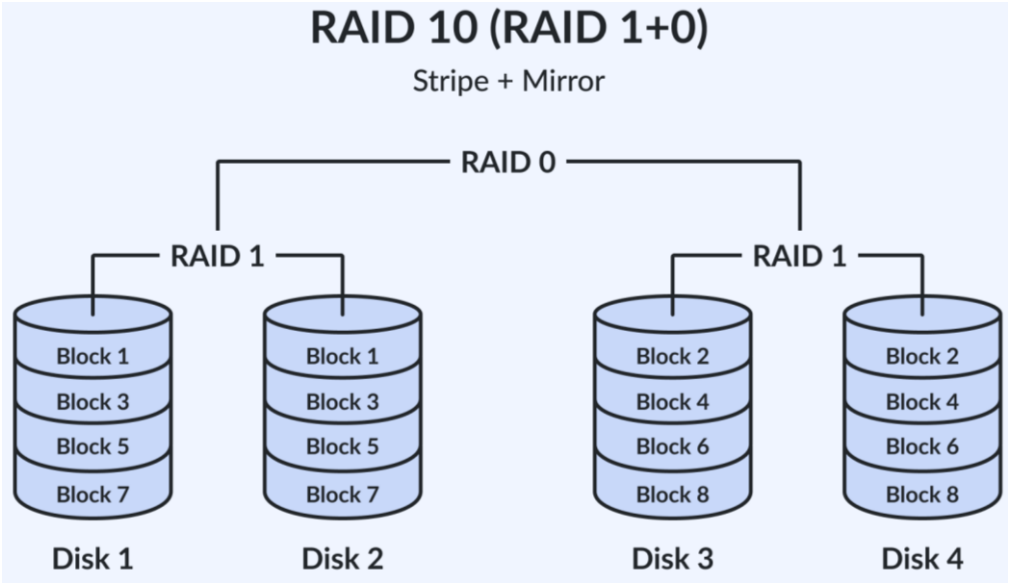
BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Disks)



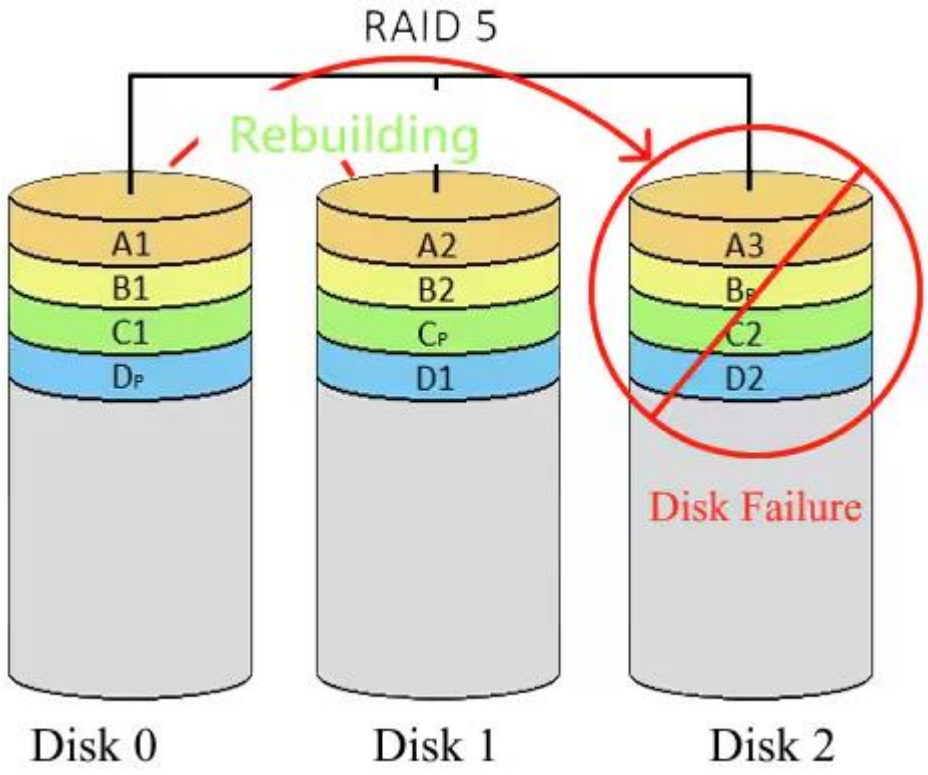


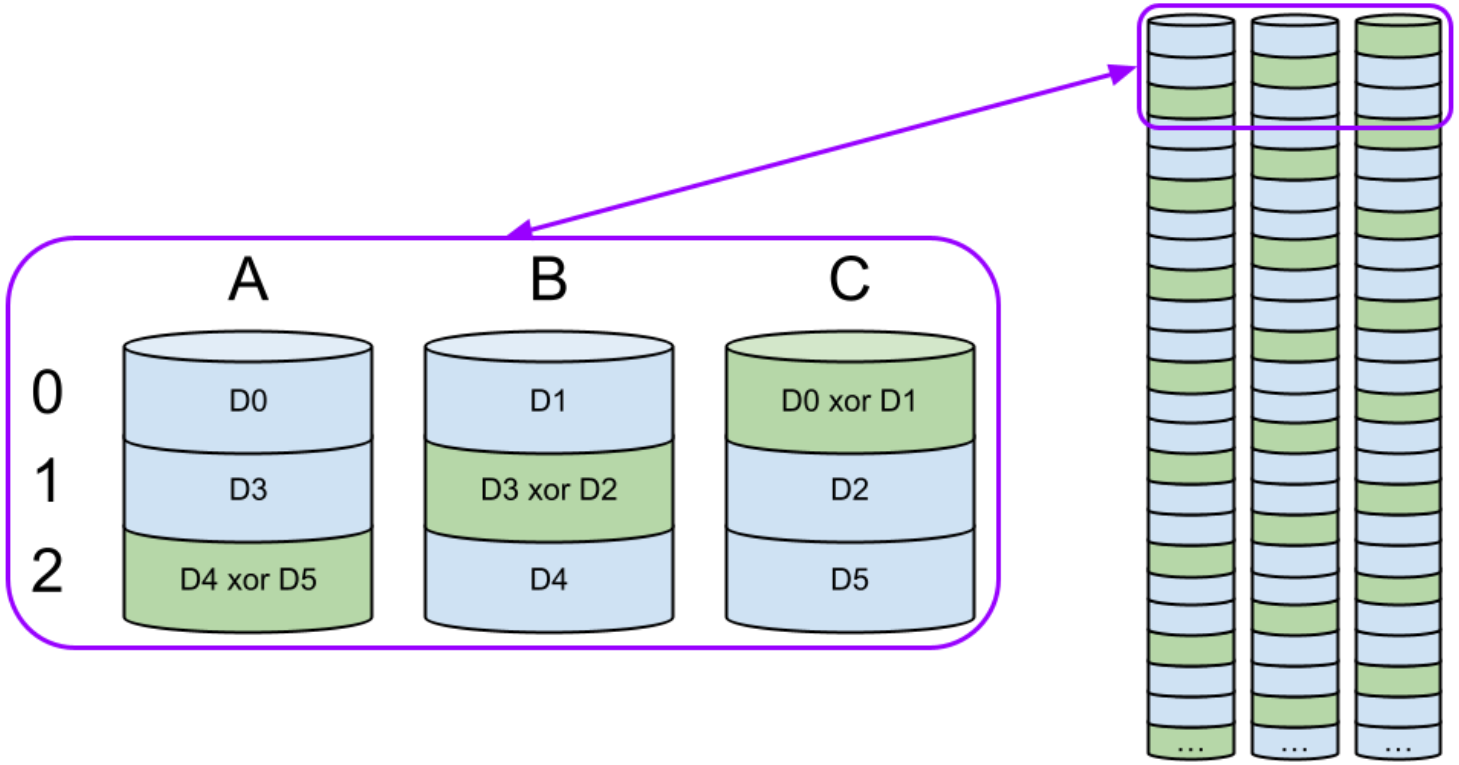


BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Disks)



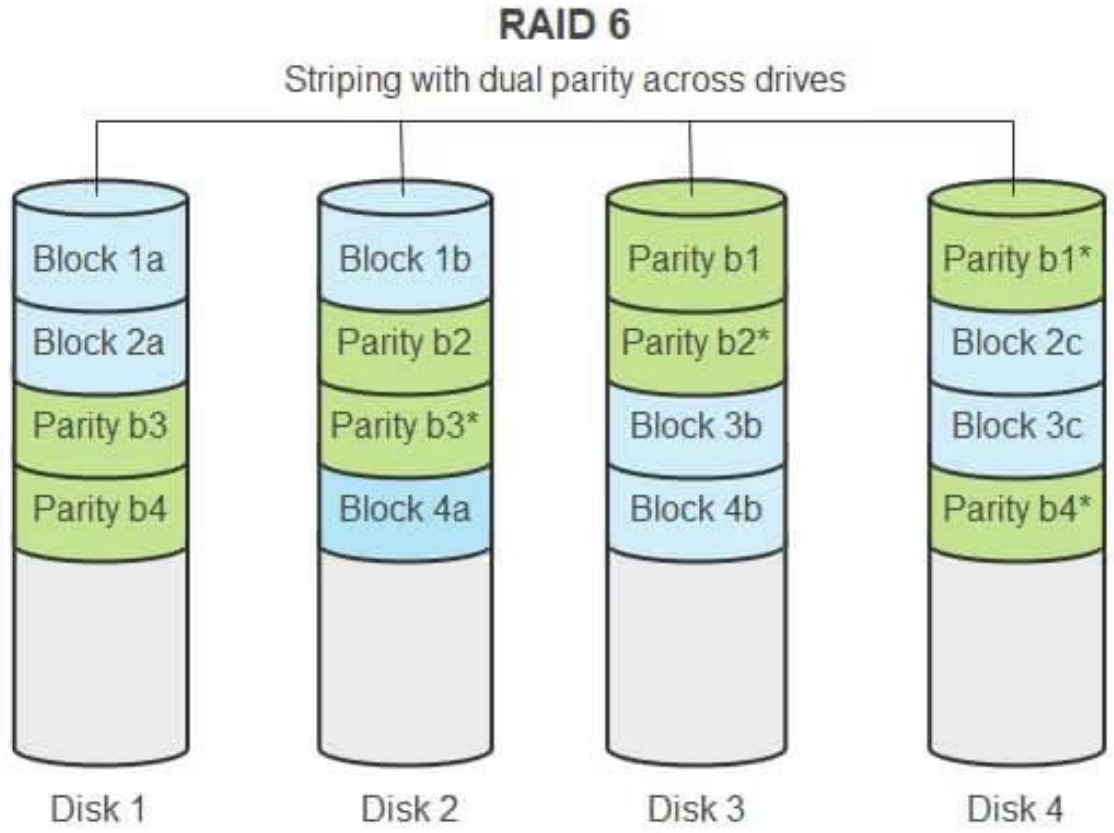


https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Disks)

RAID 5
uses a single parity stripe, which is distributed across all disks.
Needs at least 3 disks, and can tolerate only 1 disk failure.

RAID 6
uses two parity stripes, distributed across all disks, offers greater fault-tolerance.
Needs at least 4 disks, and can tolerate up to 2 disks failure.



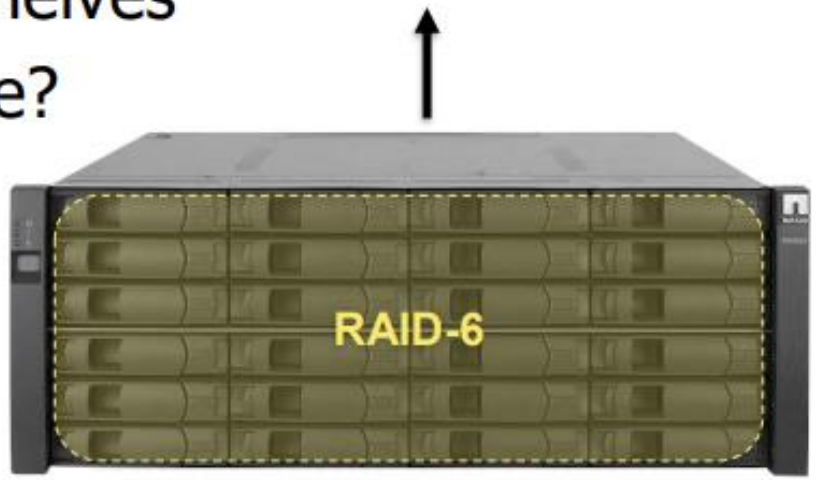
RAID Type	Minimum # of Drives	Space Lost to Redundancy	Read/Write Performance	Data Safety
RAID 0	2	None	Excellent	Poor
RAID 1	2	50%	Average	Good
RAID 0+1	4	50%	Good	Good
RAID 10	4	50%	Good	Good
RAID 5	3	1 Drive	Good	Good
RAID 6	4	2 Drives	Good	Excellent

BCIT™

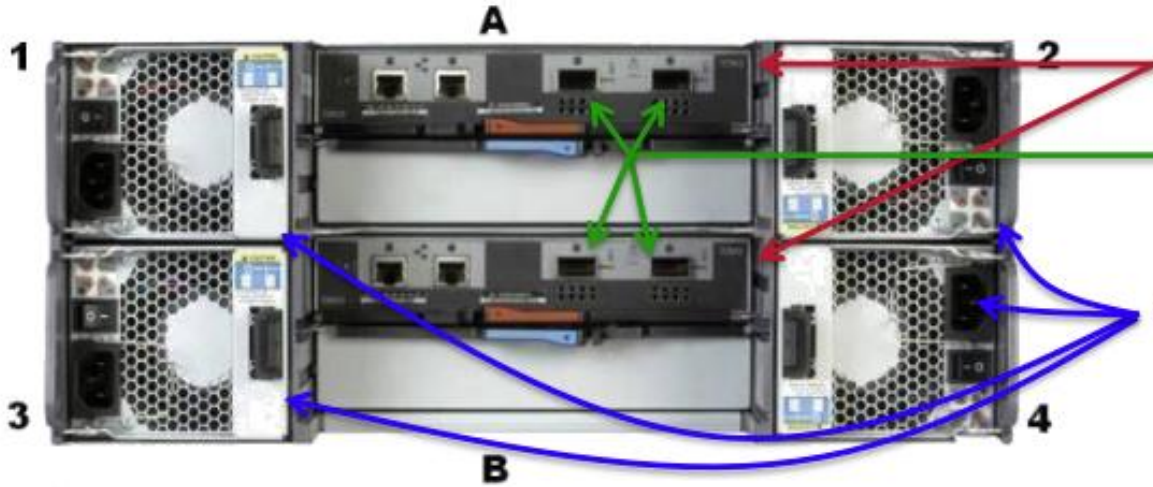
https://www.pugetsystems.com/labs/articles/raid-explained-24/

Hardware Redundancy (Disks)

- Disks physically installed into disk shelves
- Is there a single point of failure here?
  - Yes, the uplink!



- Actual back of this shelf:



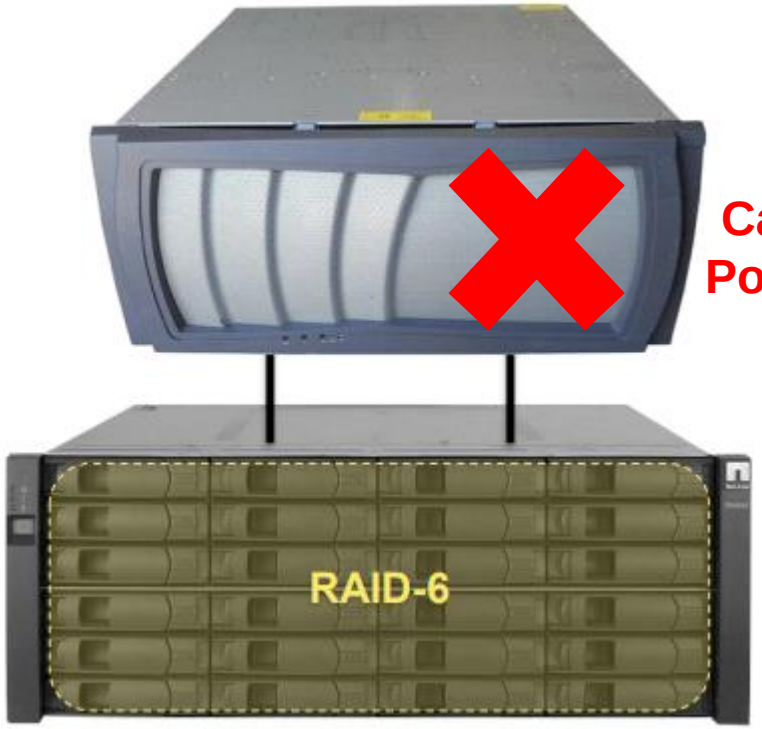
- Two IO Modules
  - Each with two SAS ports
- Also two power supplies per IOM

BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

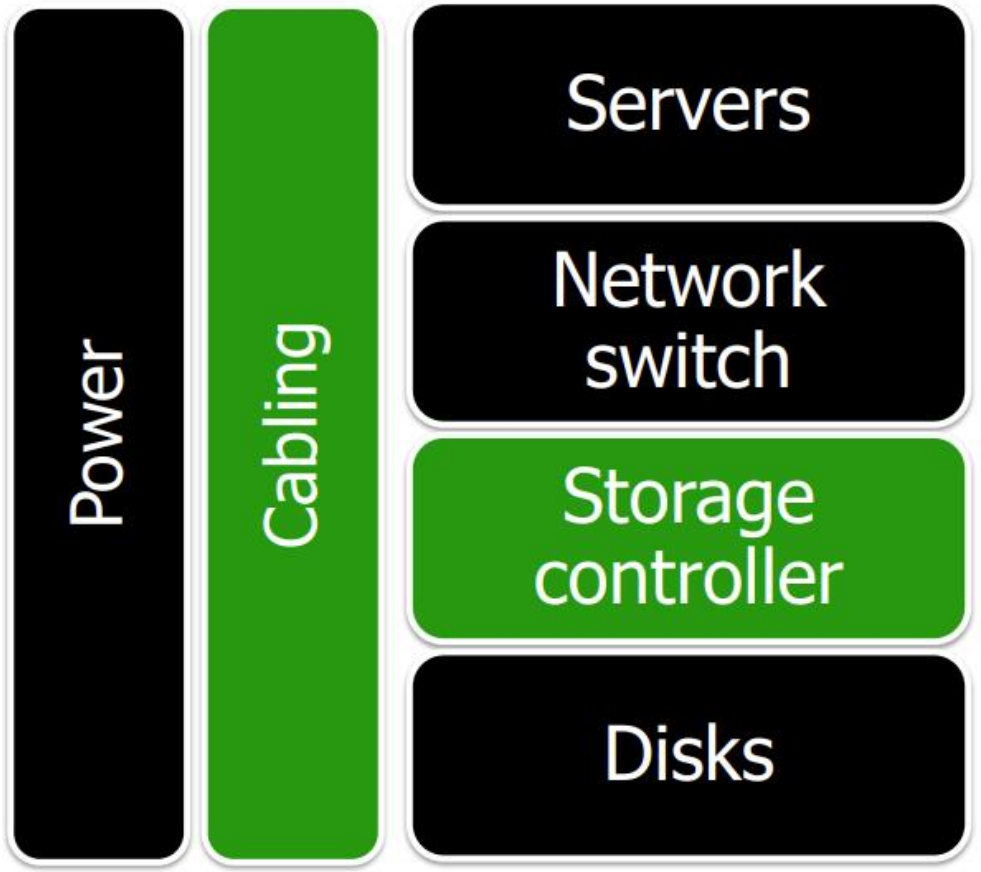
Hardware Redundancy (Disks)

Controller Module



Storage

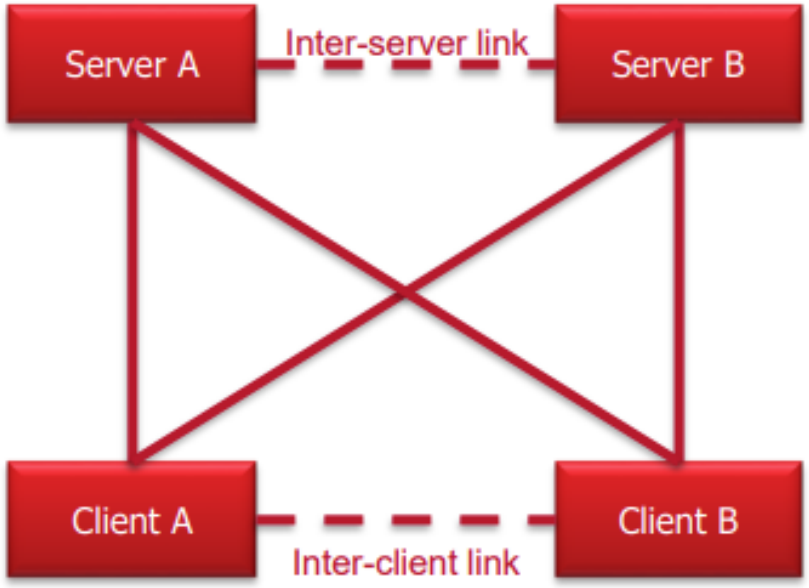
Can be Single Point of Failure

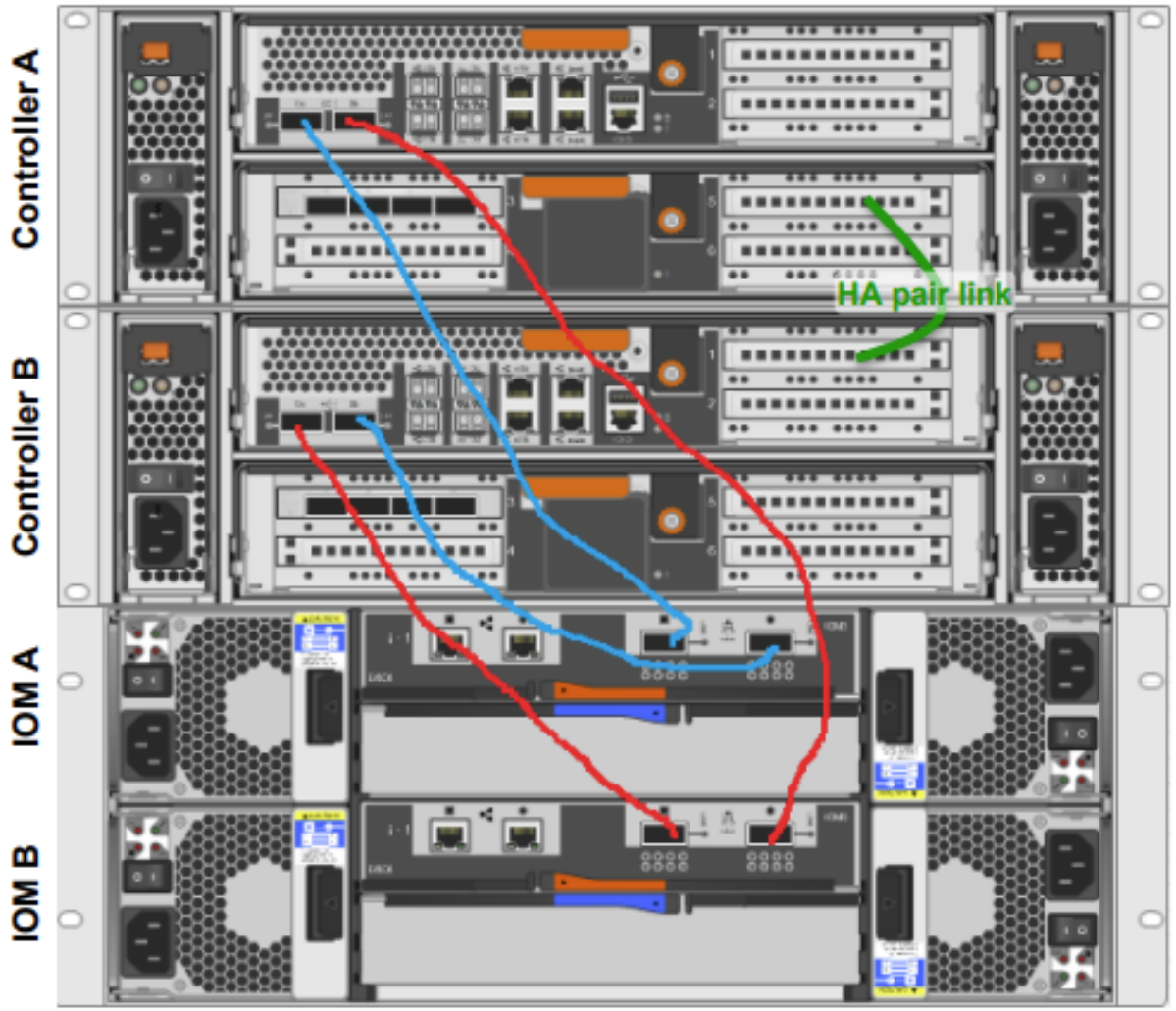


BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Hardware Redundancy (Disks)

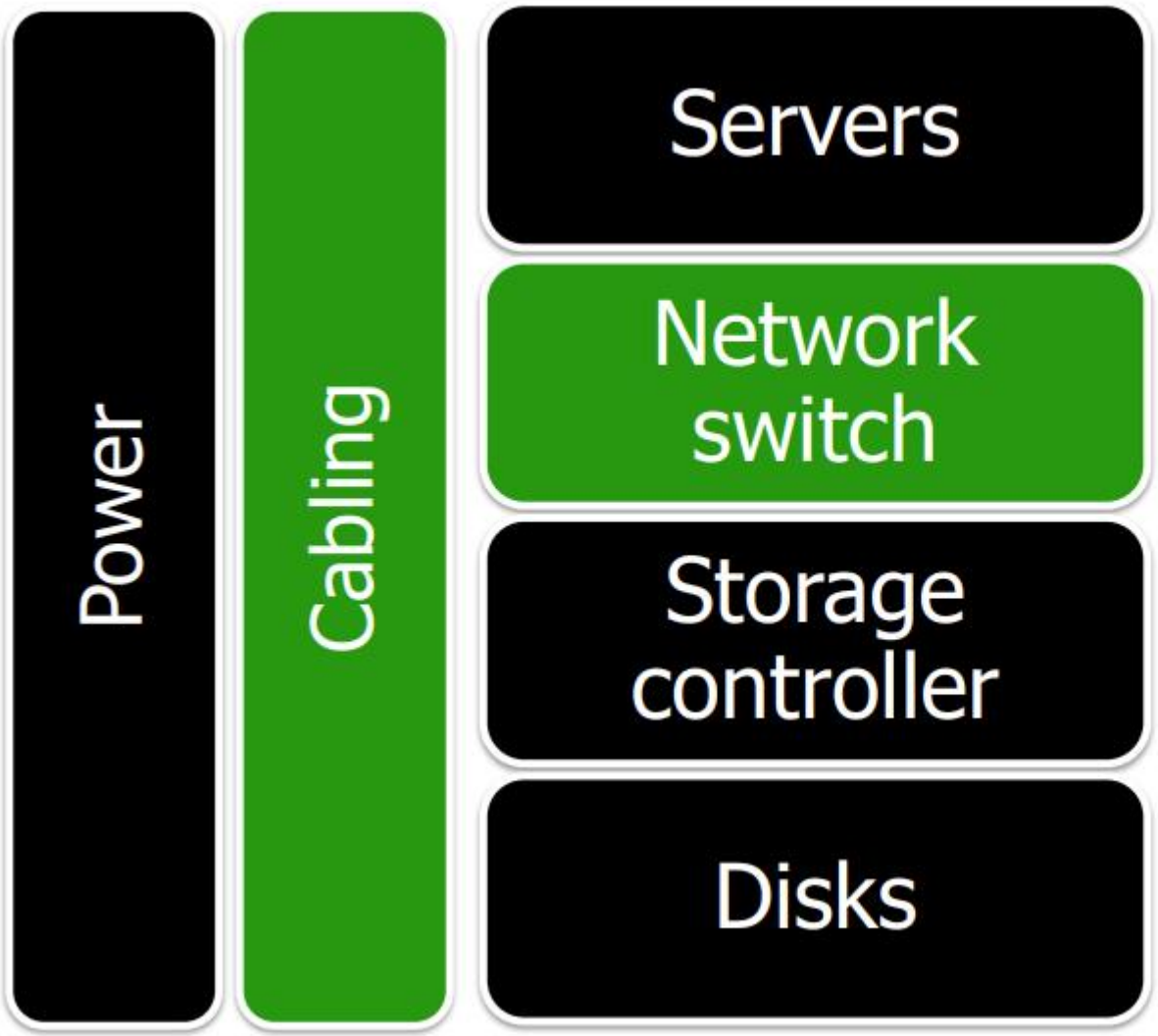


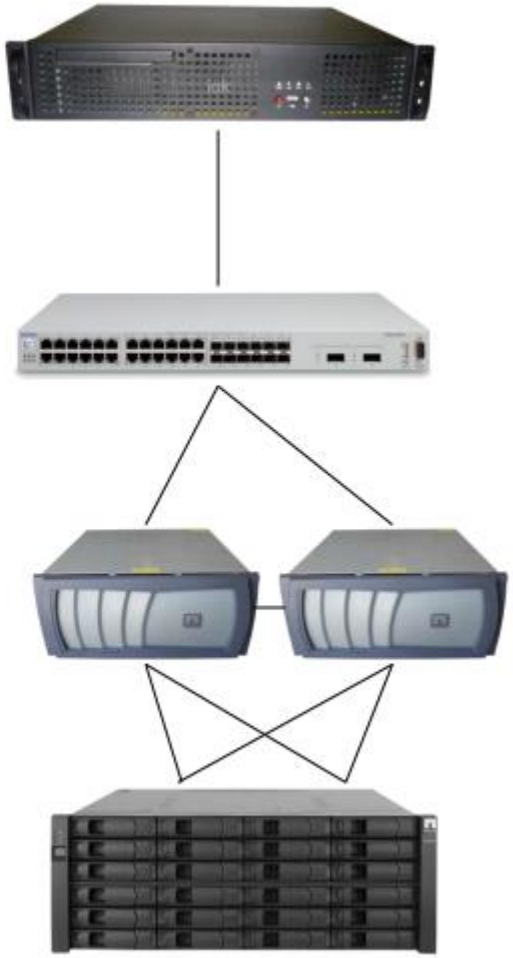


BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

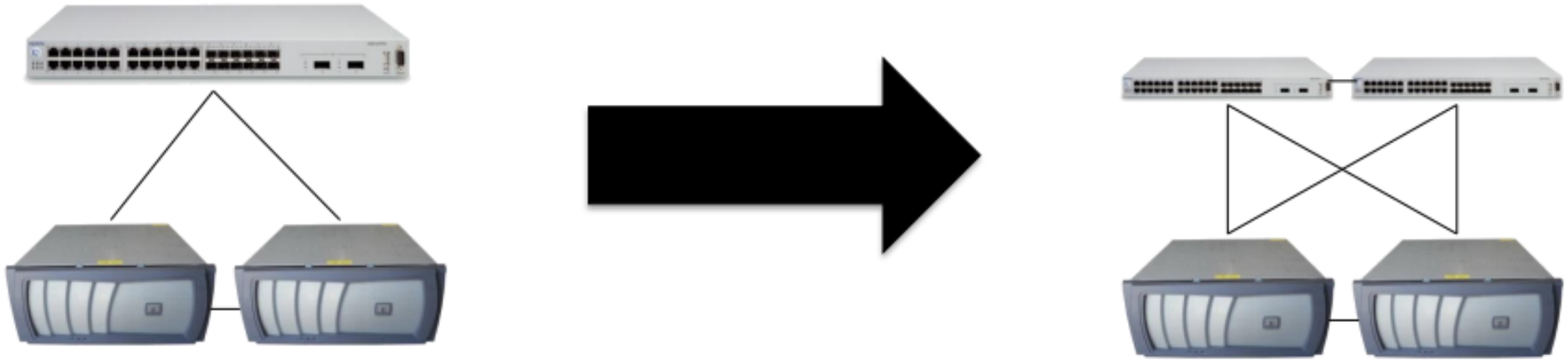
Network Redundancy





https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Network Redundancy



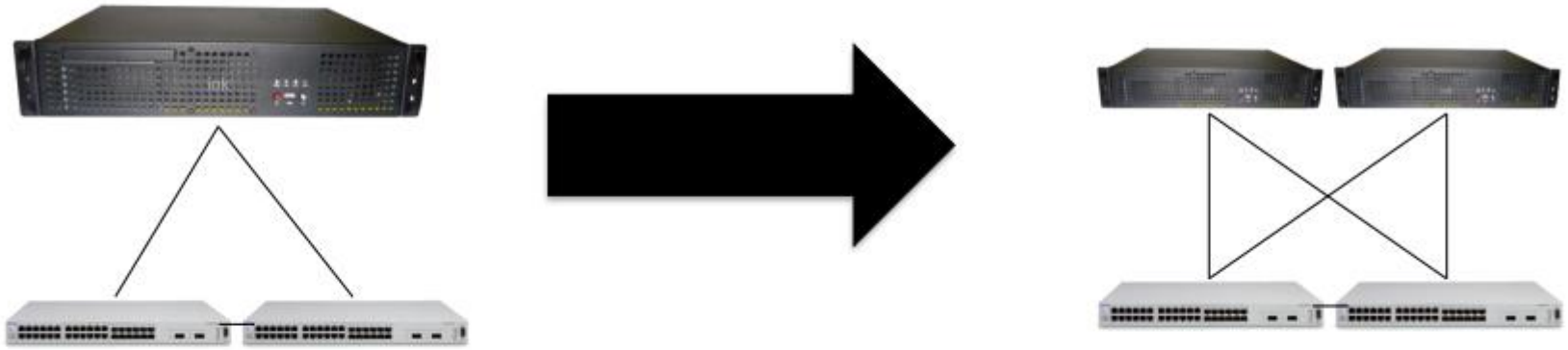
- In networking, this is known as **multipathing**
- Can be applied to Ethernet or Fibre Channel (FCP)

BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Network Redundancy

- Apply the Universal HA topology 

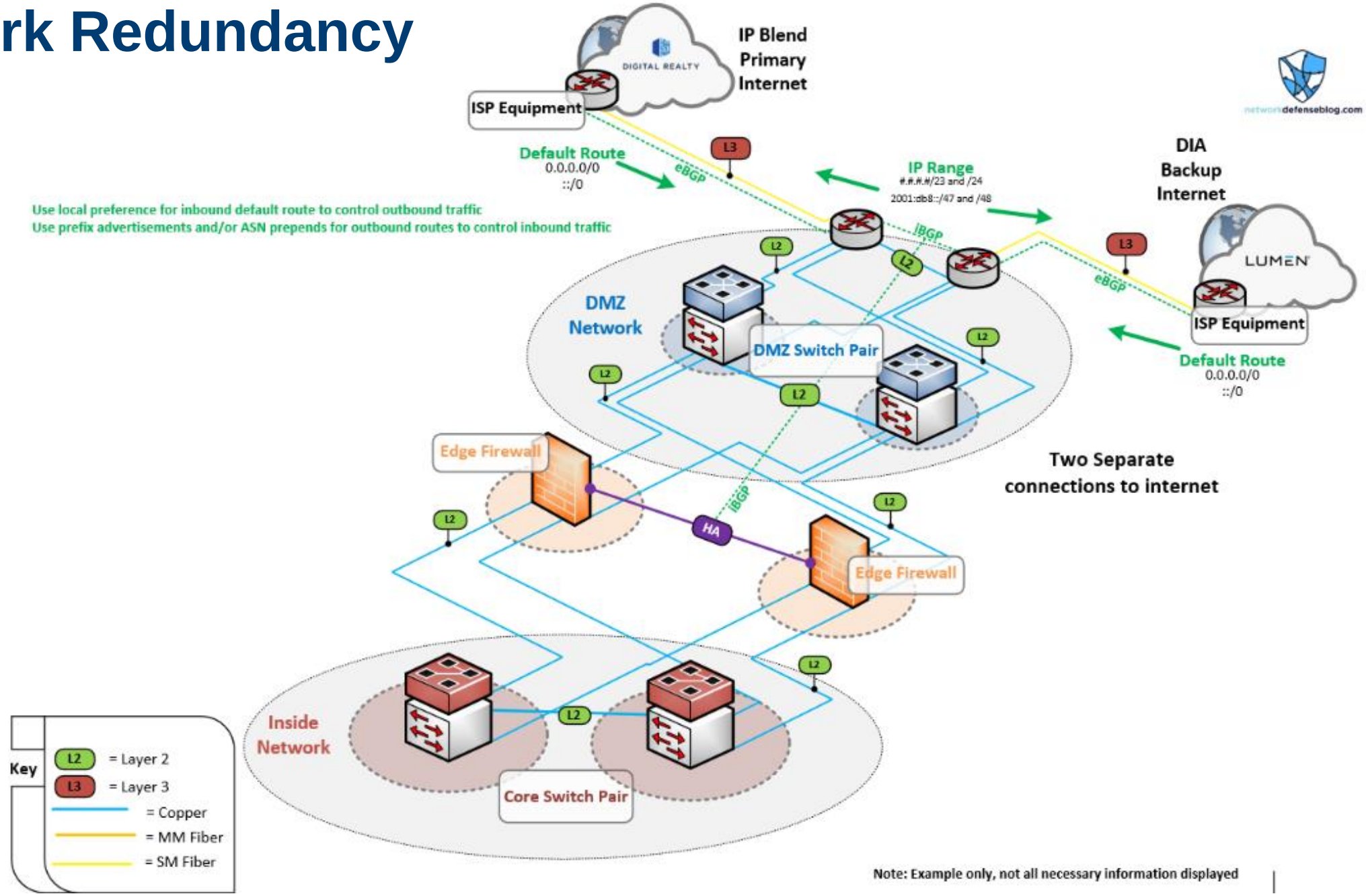


- However, typically have more than 2 servers – storage/network usually serves pool of many servers

BCIT™

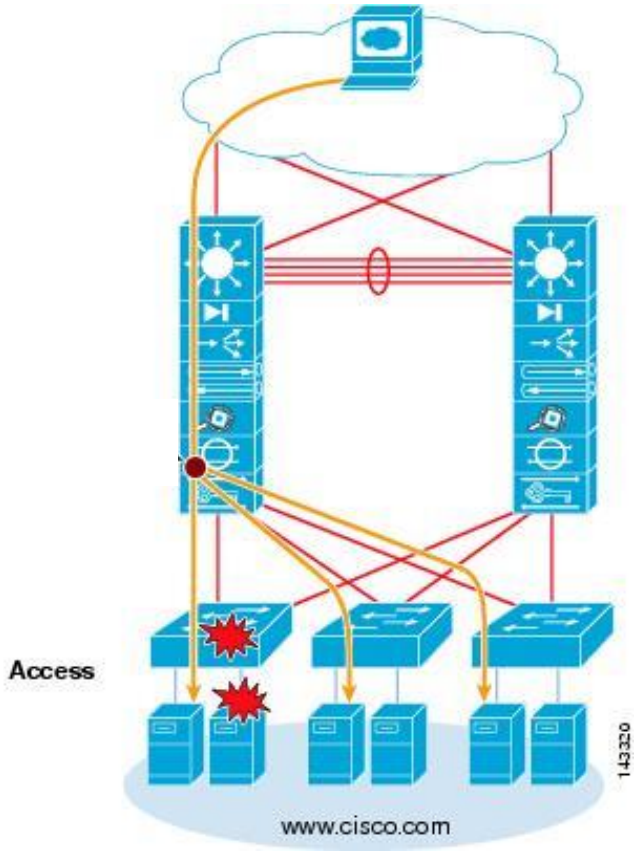
https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

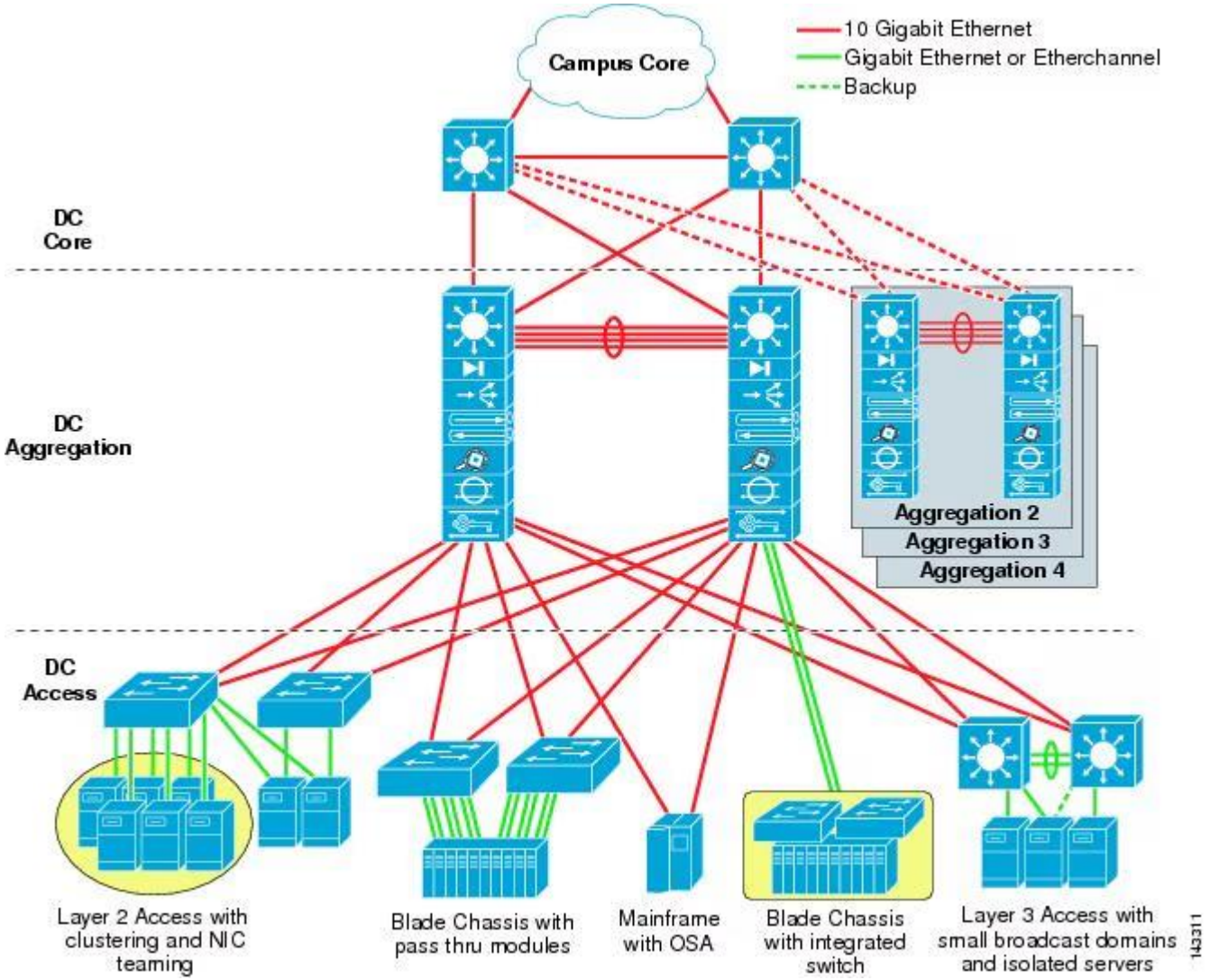
Network Redundancy



https://www.networkdefenseblog.com/post/network-design-network-edge

Network Redundancy

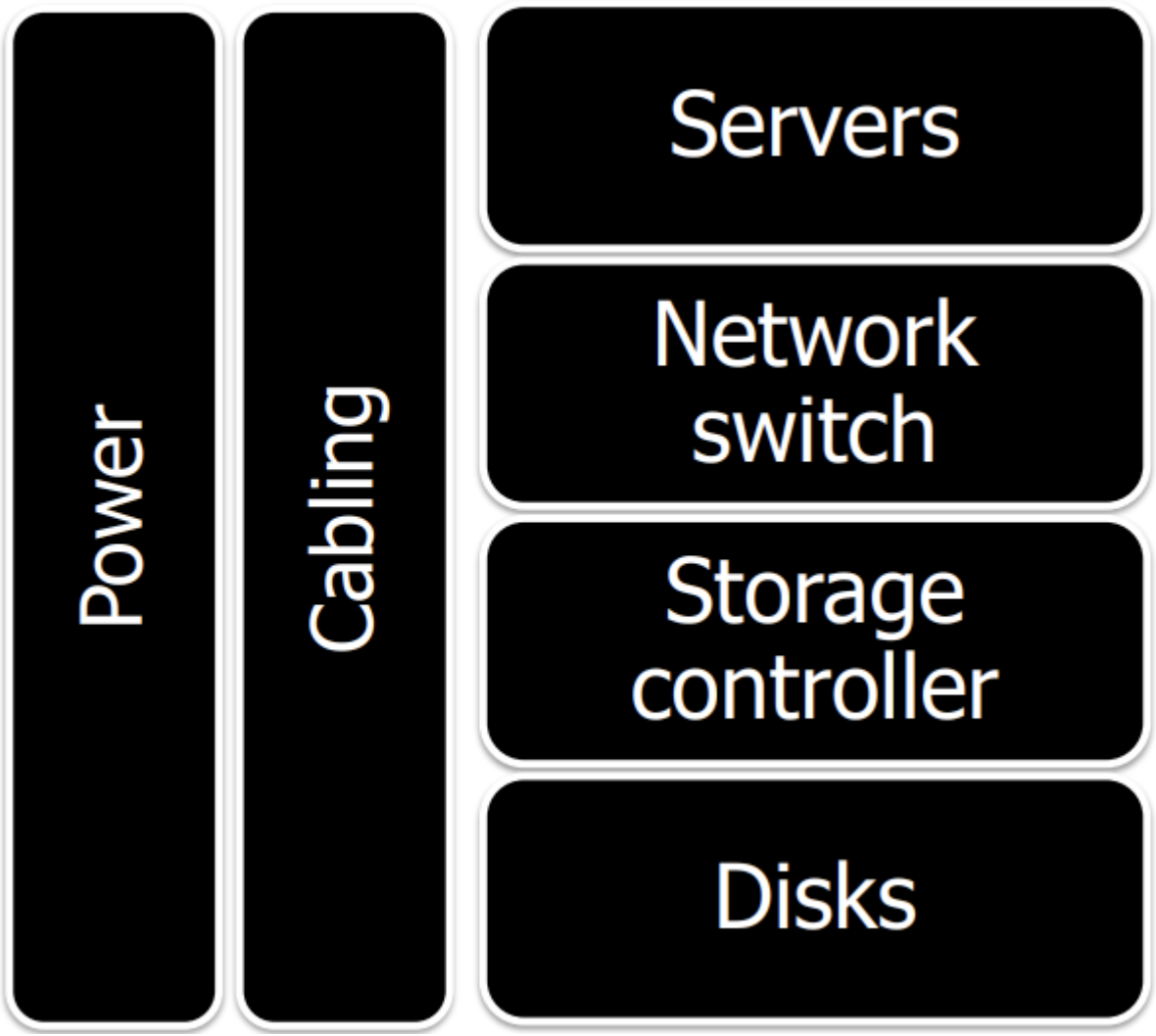


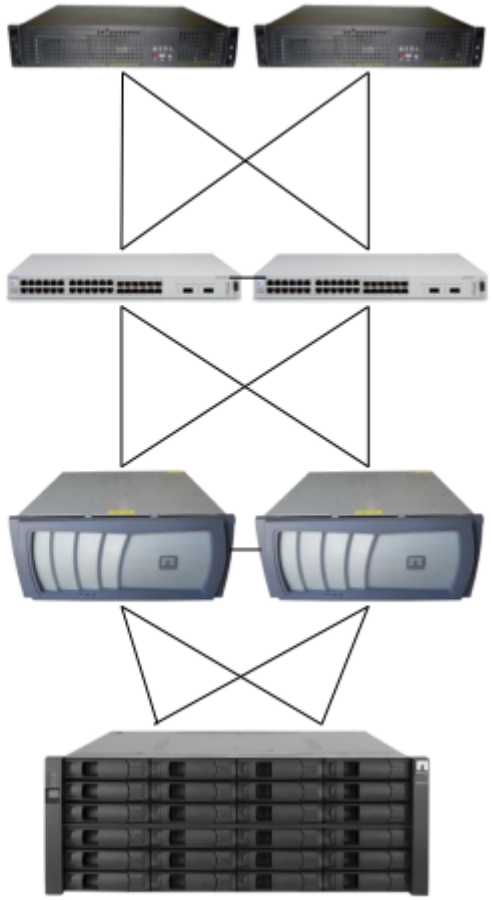


BCIT

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCI_SRND_2_5a_book/DCInfra_2a.html

Complete Redundancy

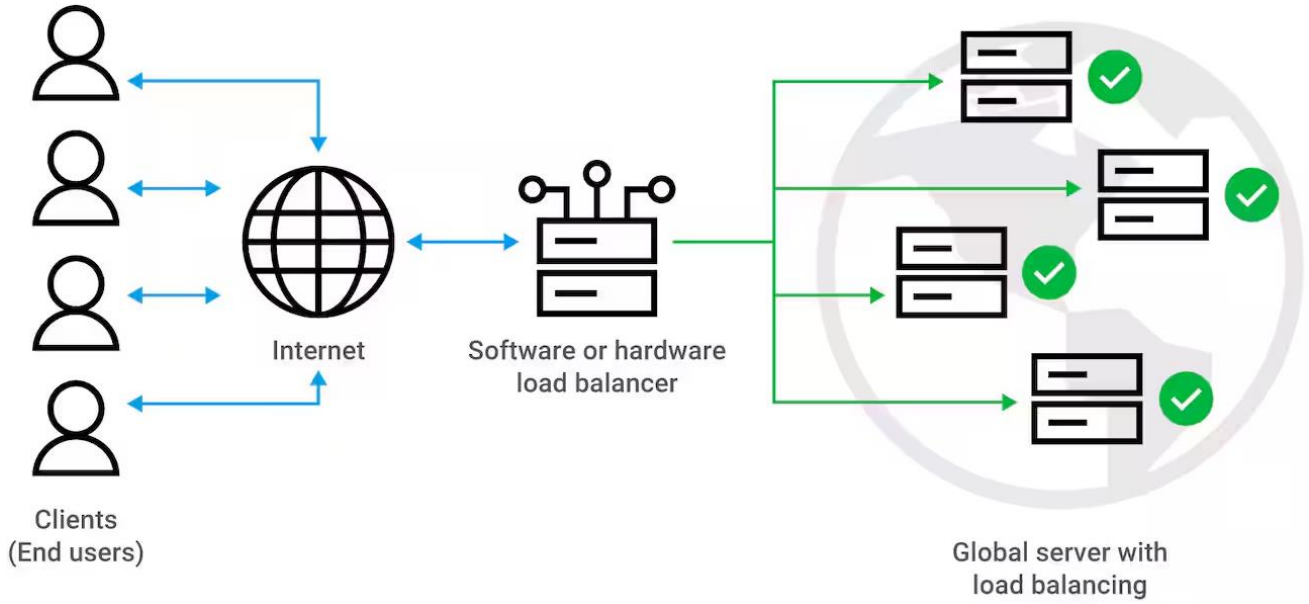


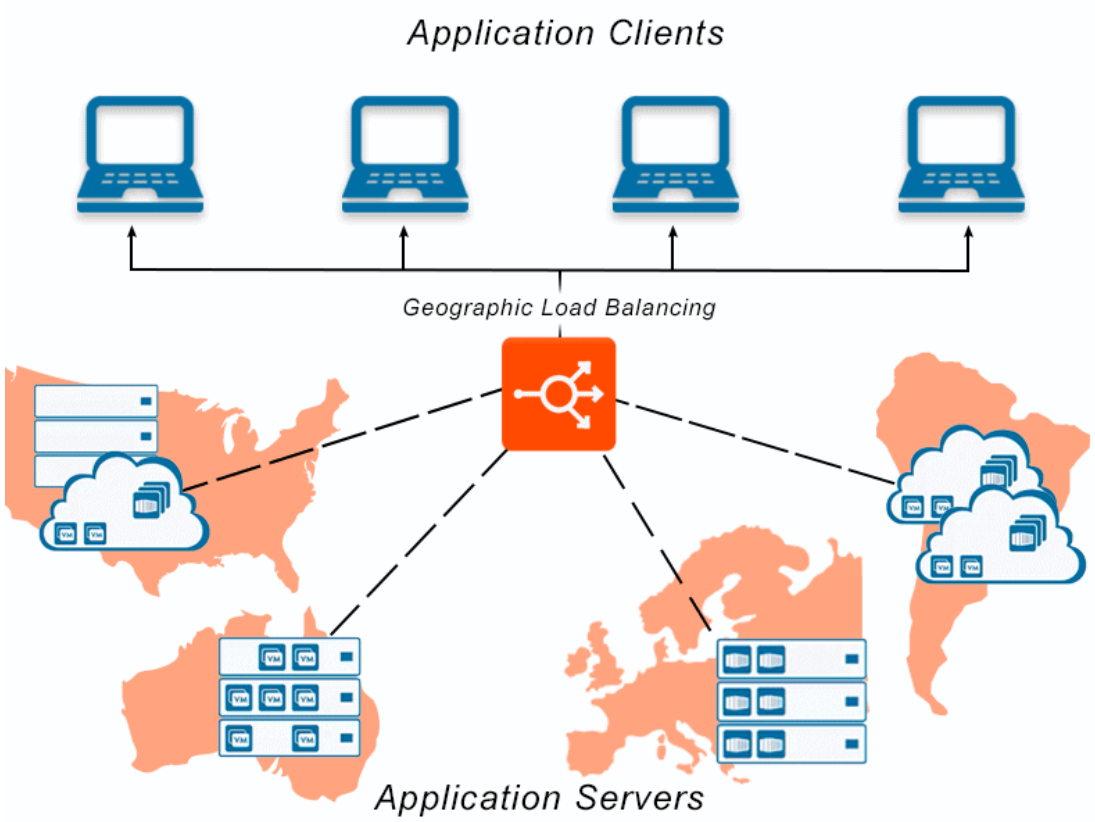


BCIT™

https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

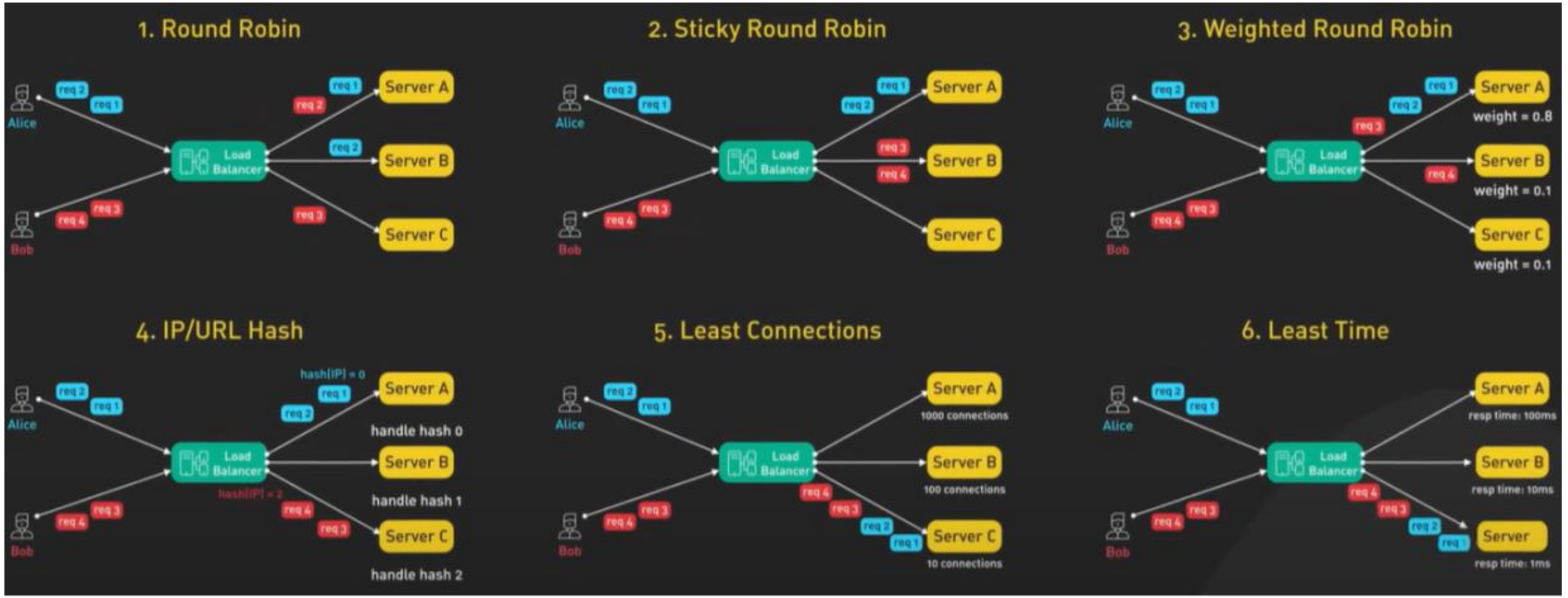
Service Load Balancing





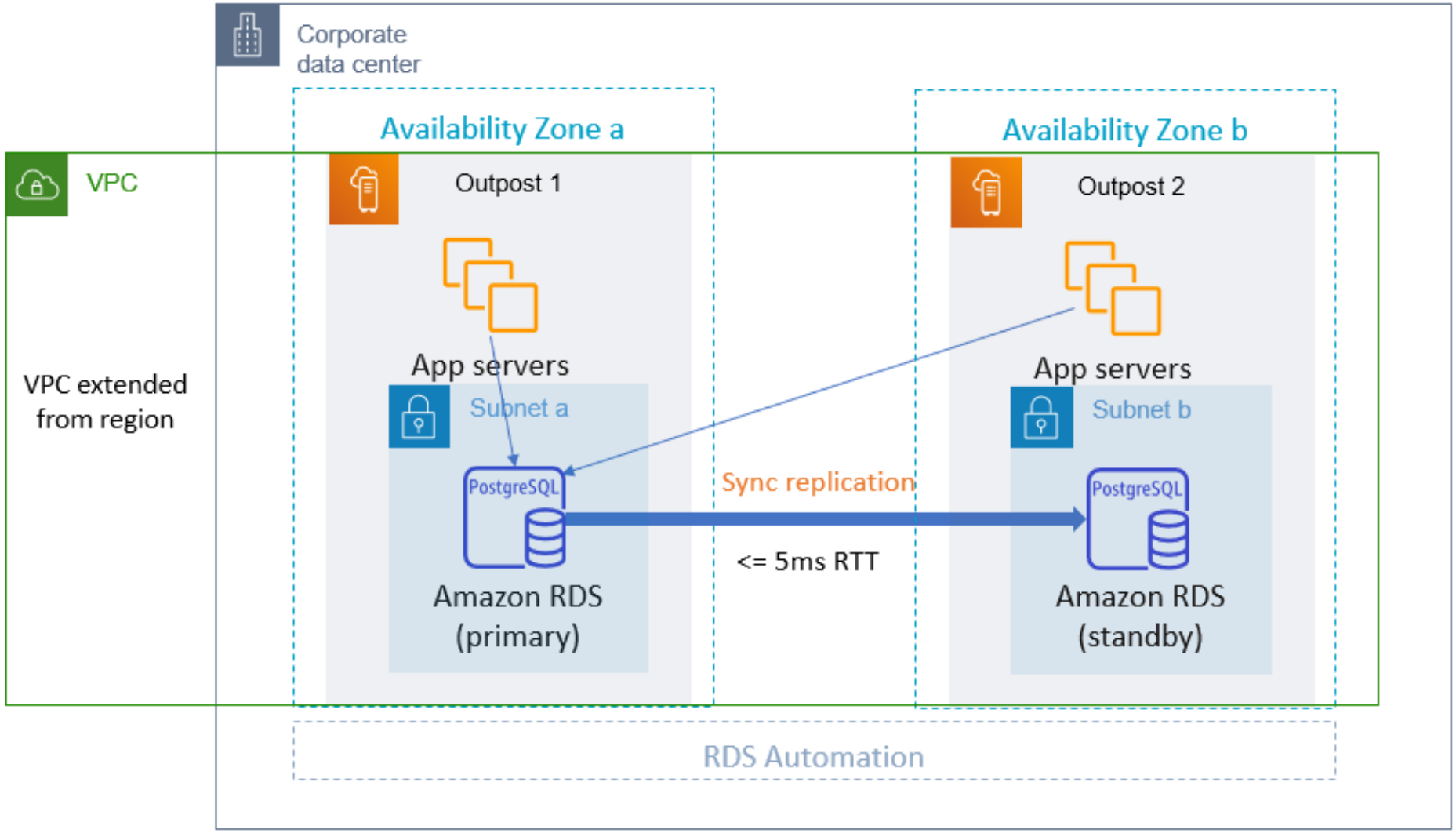
BCIT™

Service Load Balancing



BCIT™

App/DB HA in AWS

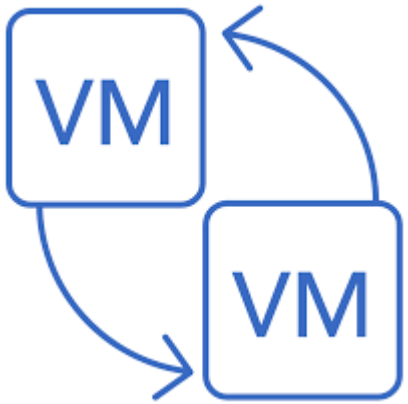


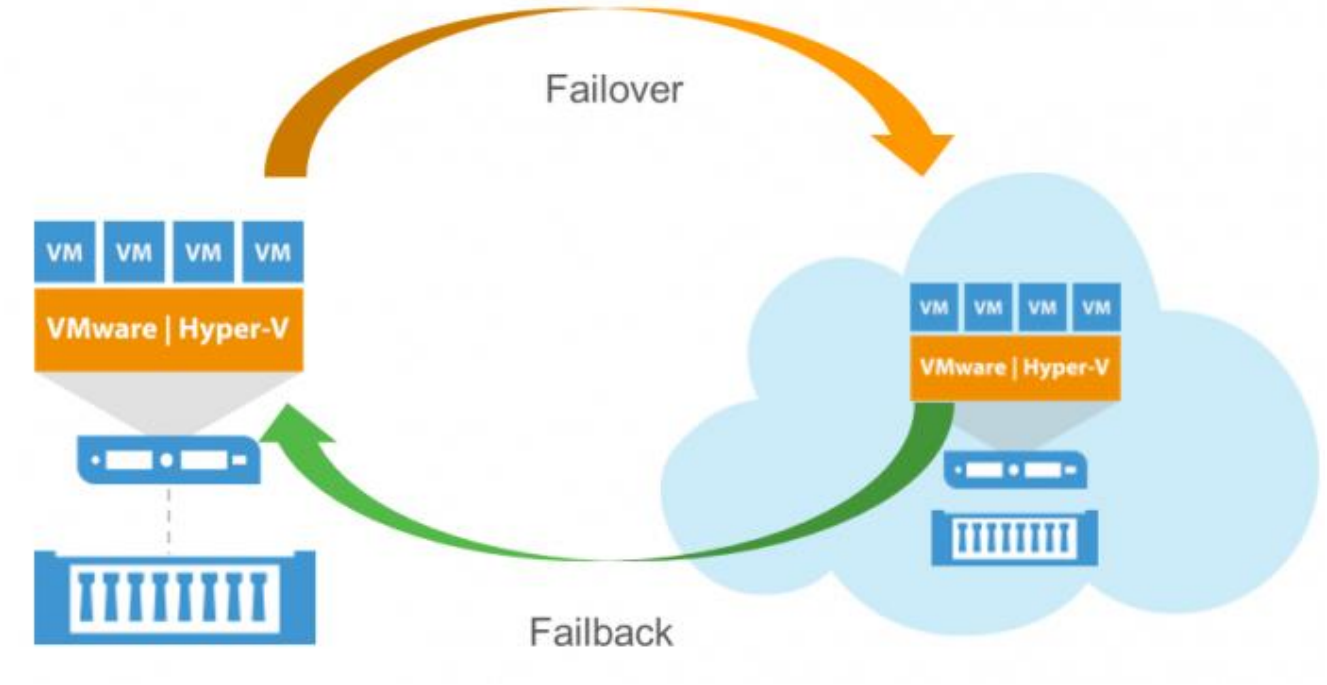
BCIT™

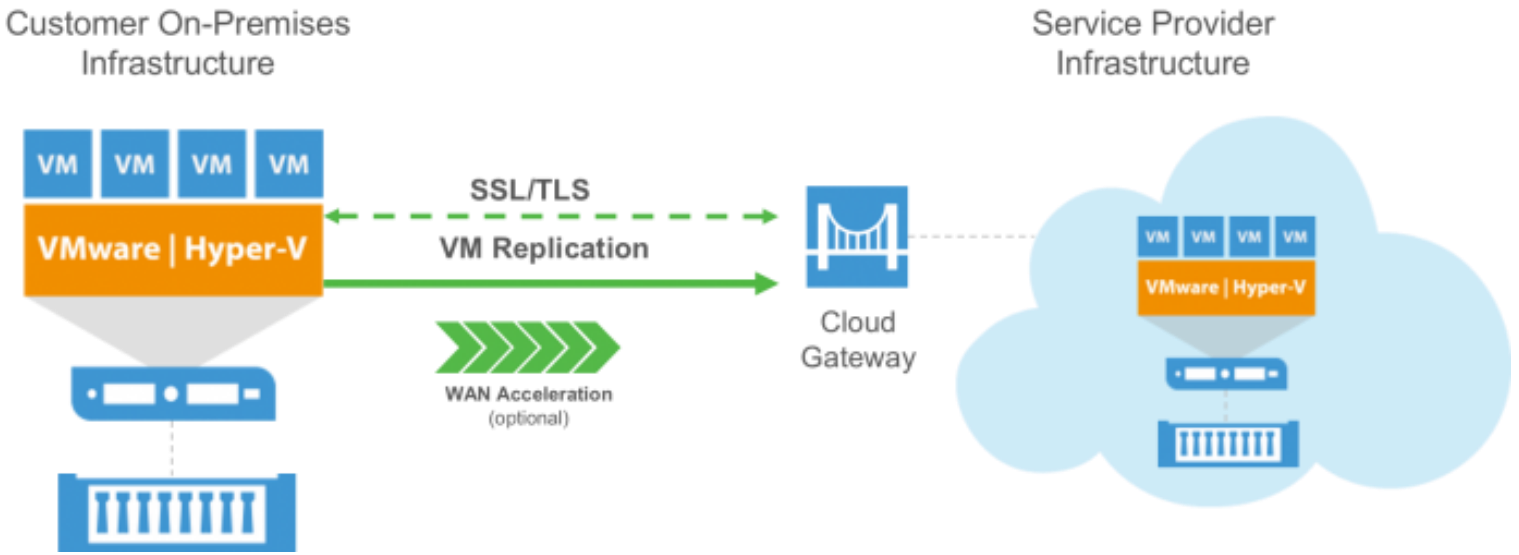
https://aws.amazon.com/blogs/database/deploy-amazon-rds-on-aws-outposts-with-multi-az-high-availability/

VM Replication

VM Replication creates an exact, synchronized copy (replica) of a virtual machine (VM) on a secondary host or storage, ensuring rapid recovery in case of disaster or downtime.

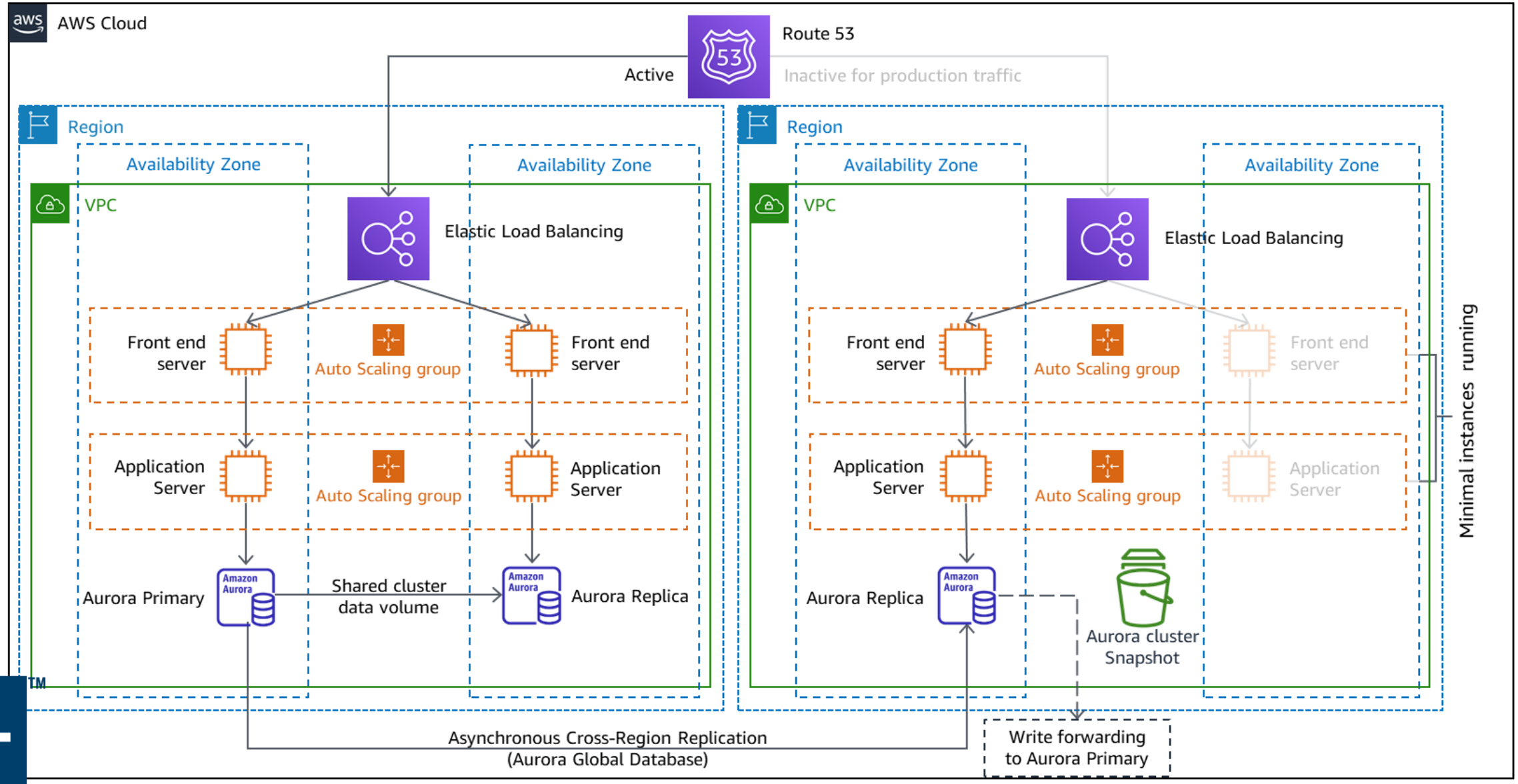






BCIT™

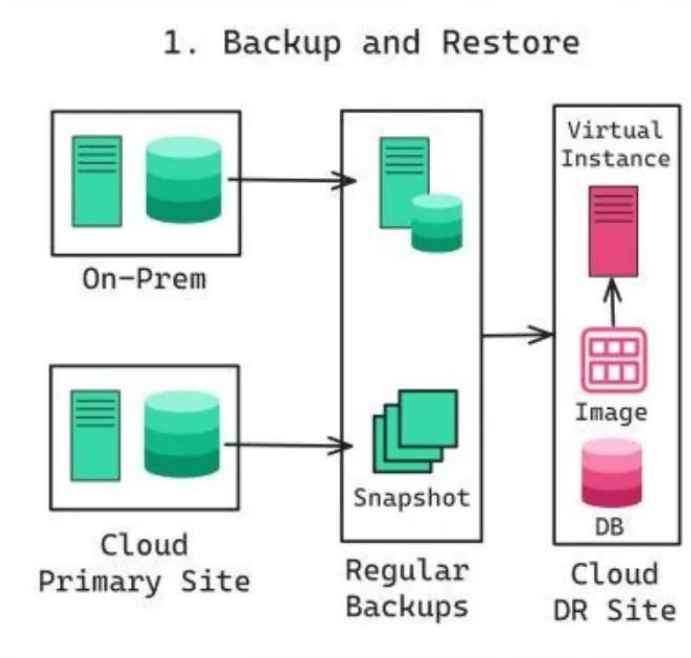
AWS DR

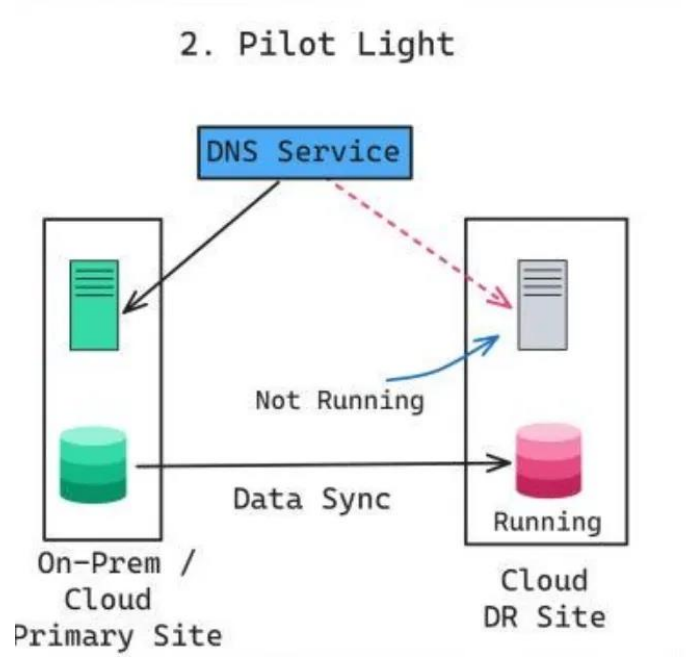


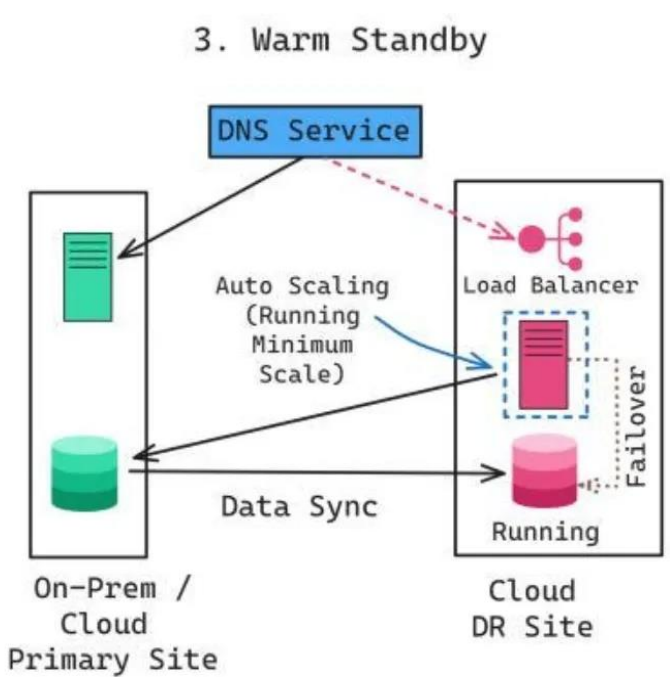
BCIT

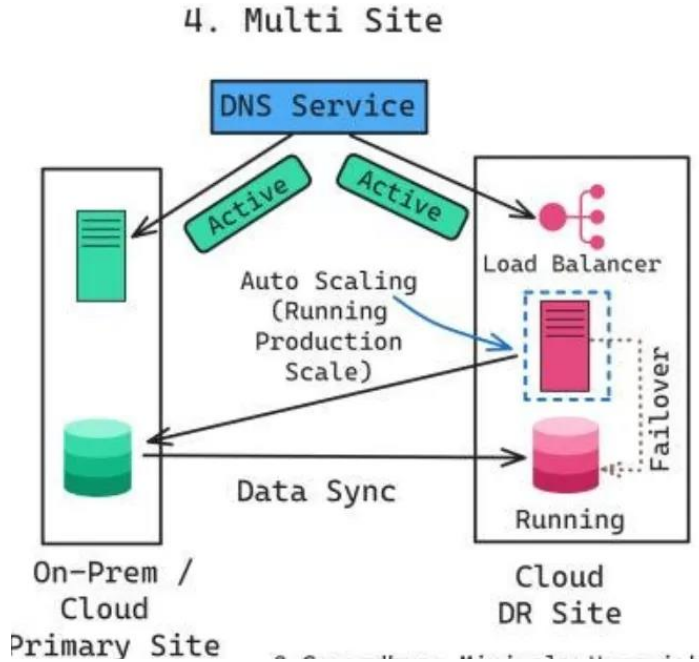
https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

DR Summary









https://medium.com/@maheshsaini.sec/system-design-4-top-cloud-disaster-recovery-strategies-e91750d6c93d

End of Lecture #9

Deadline for Assignment #5
March 21st, 2025

THANK YOU

- Dawood Sajjadi

BCIT™