

A unique opportunity for you to be mentored by Amazonians



Batch 04

Week 1

8-July-2023



Introduction - Program and Team

- What?
 - [BeSA Website](#) and FAQ page
- Who?
 - Core Team
 - Ashish Prajapati, James Eastham, Jamila Jamilova, Parna Mehta and Prasad Rao
 - Extended Team
 - Abhijeet Patwardhan, Giuseppe Battista, Ferdi Rezwan
- Why?
 - We are passionate about mentoring
 - Giving back to community
- When?
 - Every Saturday 8 AM GMT
 - 9 AM UK / 1.30 PM IST / 4.00 AM ET
- Where?
 - Live Session – YouTube Live
 - Recorded Videos – YouTube
 - Resources – BeSA Website
 - Communication – LinkedIn Group
- How?
 - Stage 1 – Technical Track (8 Weeks)
 - Stage 2 – Behavioural Track (4 Weeks)



Intended Target Audience



- Focused toward IT professionals who wants to become Solutions Architect
 - Focus on technical and behavioural concepts (Stage 1)
 - Help you upskill for certifications (Stage 1)
 - Provide interview coaching (Stage 2)

Disclaimers

- This is not a job guarantee program.
- This program is not affiliated with AWS. It is created by volunteers who work at AWS.
- Views shared by us are our own and do not represent our employer.
- In case of any conflicting information always refer to the official AWS Documentation.
- Program is run on best effort basis.



Become a Solutions Architect

3 batches completed in
2022 and 2023.
This is batch 4



4,400+ members
registered and are part
of BeSA LinkedIn group



2700+ subscribers on
BeSA YouTube channel
with 43,500+ views



100+ members
regularly joined
weekend live sessions



60+ members
succeeded in obtaining
AWS certifications



40+ members were
mentored in 1:1
sessions



15+ guest speakers
shared their journey
and career tips



6 participants
successfully secured
positions in AWS



#besaprogram

In coming weeks...

8 Weeks



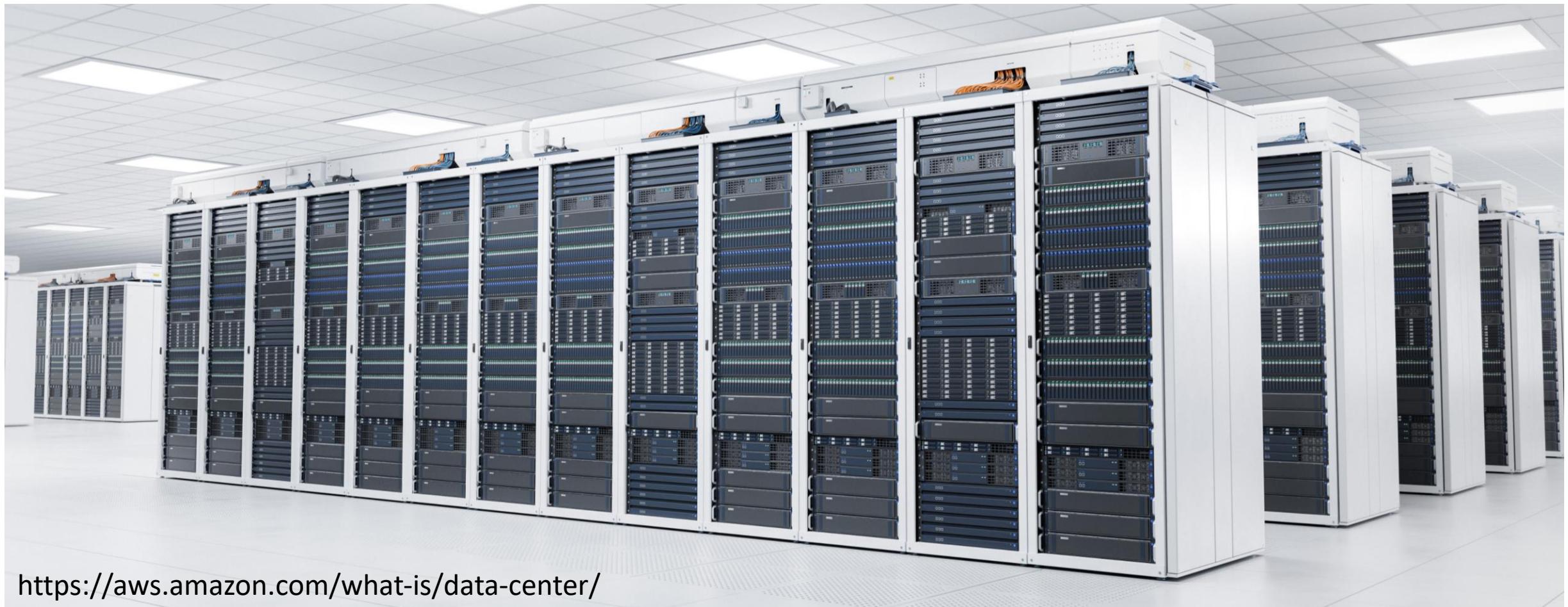
Today's Session

Week 1
08-July



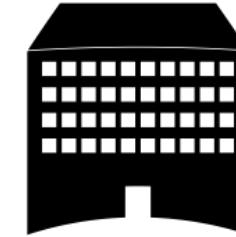
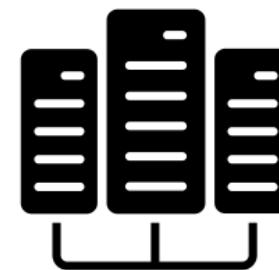
What is a data center?

- A data center is a physical location that contains the infrastructure that IT systems require, such as servers, data storage drives, and network equipment.



<https://aws.amazon.com/what-is/data-center/>

Types of data centers (based on ownership)



Enterprise
Data
Centers

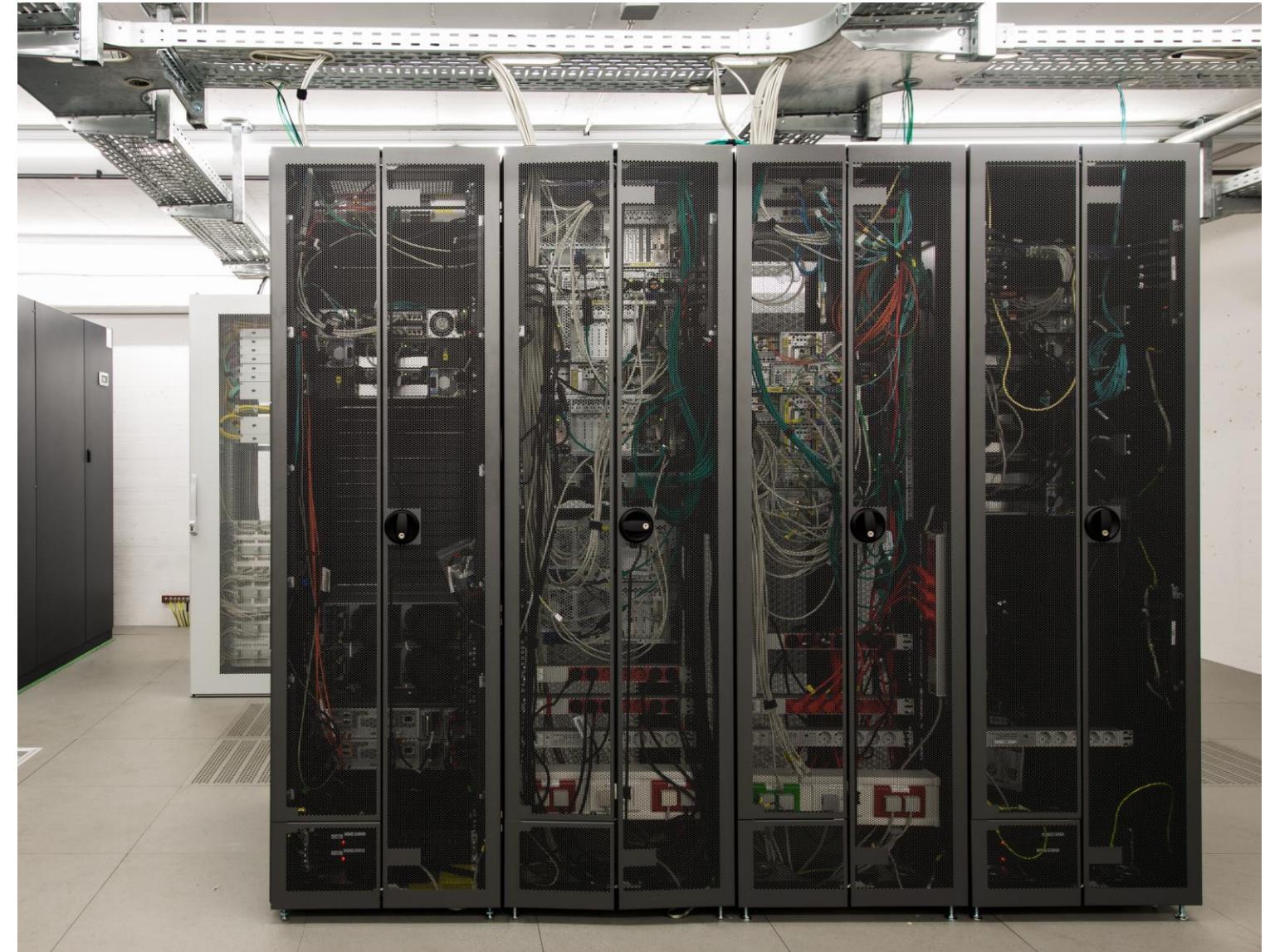
Managed
Services
Data
Centers

Colocation
Data
Centers

Cloud
Data
Centers

Enterprise Data Centers (On-premises Data Centers)

- A private facility built owned, and operated by a company for their own use.
- Most often they are housed on the corporate campus.
- You set up the data center, manage its ongoing operations, and purchase and maintain the equipment.



Managed Services Data Centers

- A datacenter that is managed by a third party that leases (rents out) the equipment and the infrastructure.
- You can leases the equipment and infrastructure instead of buying it.



Colocation Data Centers (“colo”)

- A datacenter white space is rented out to individual companies to host their hardware equipment.
- The colocation data center hosts the infrastructure: building, cooling, bandwidth, security, etc., while the company provides and manages the components, including servers, storage, and firewalls.



Cloud Data Centers

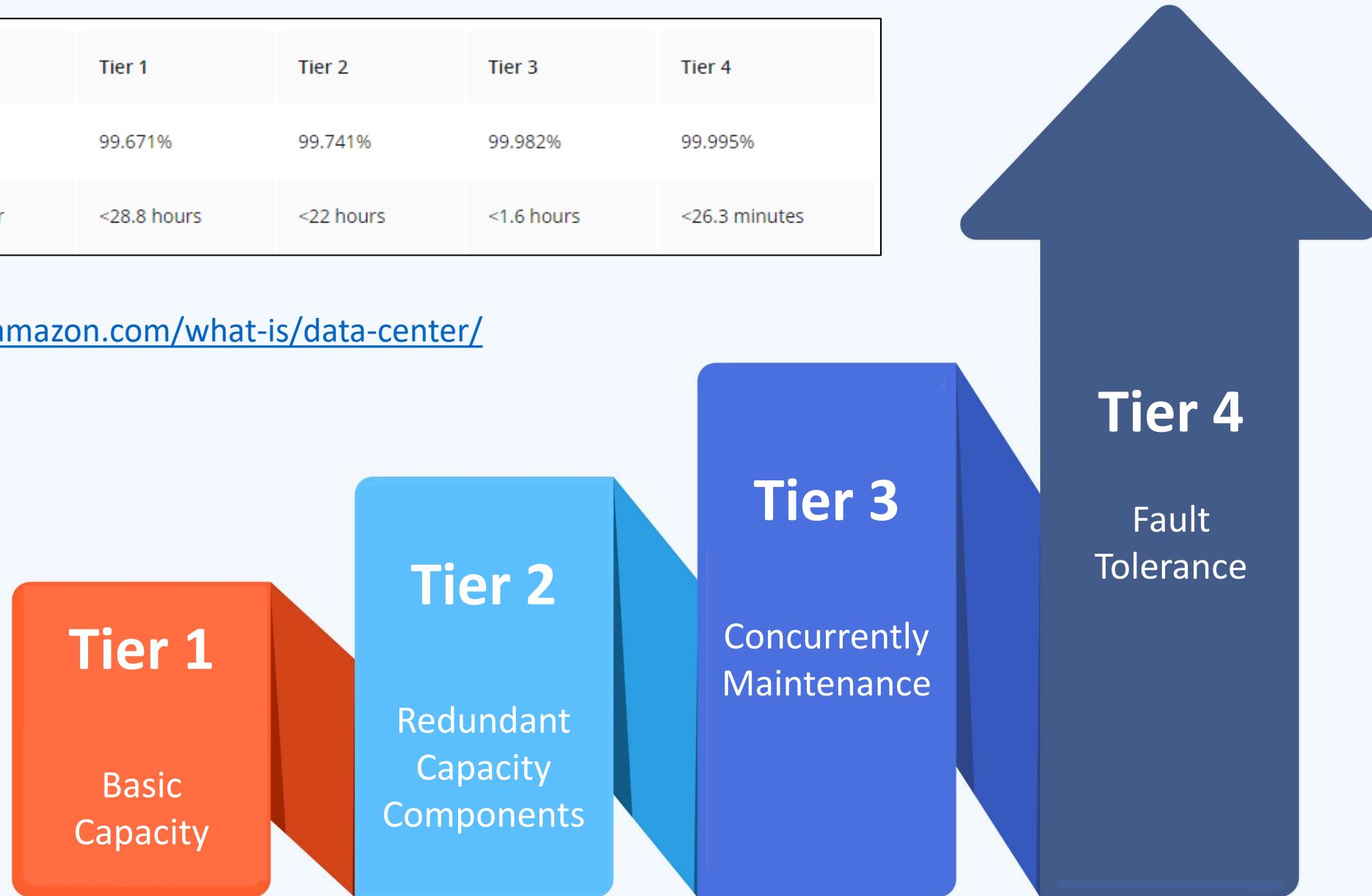
- In this form of data center, data and applications are hosted by a public cloud provider such as AWS, Azure, Google.
- In a cloud data center, you rent both space and infrastructure.



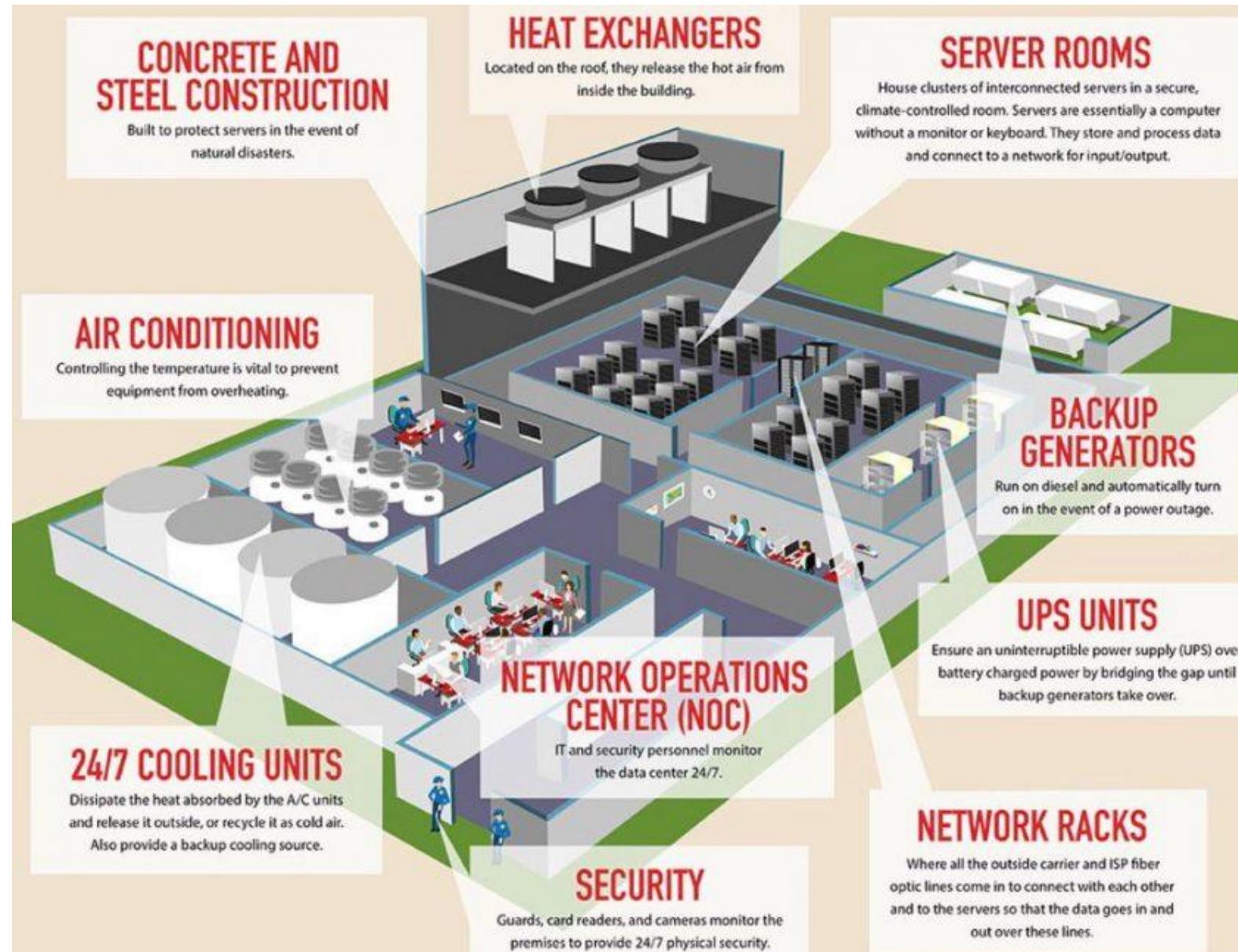
Data Center Tiers

	Tier 1	Tier 2	Tier 3	Tier 4
Uptime guarantee	99.671%	99.741%	99.982%	99.995%
Downtime per year	<28.8 hours	<22 hours	<1.6 hours	<26.3 minutes

<https://aws.amazon.com/what-is/data-center/>



What is inside a data center?

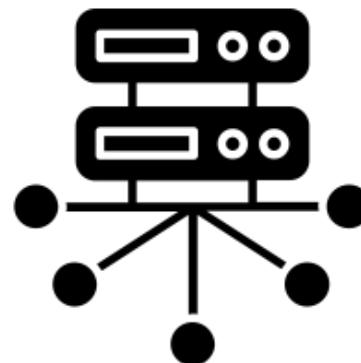


What is inside a data center?

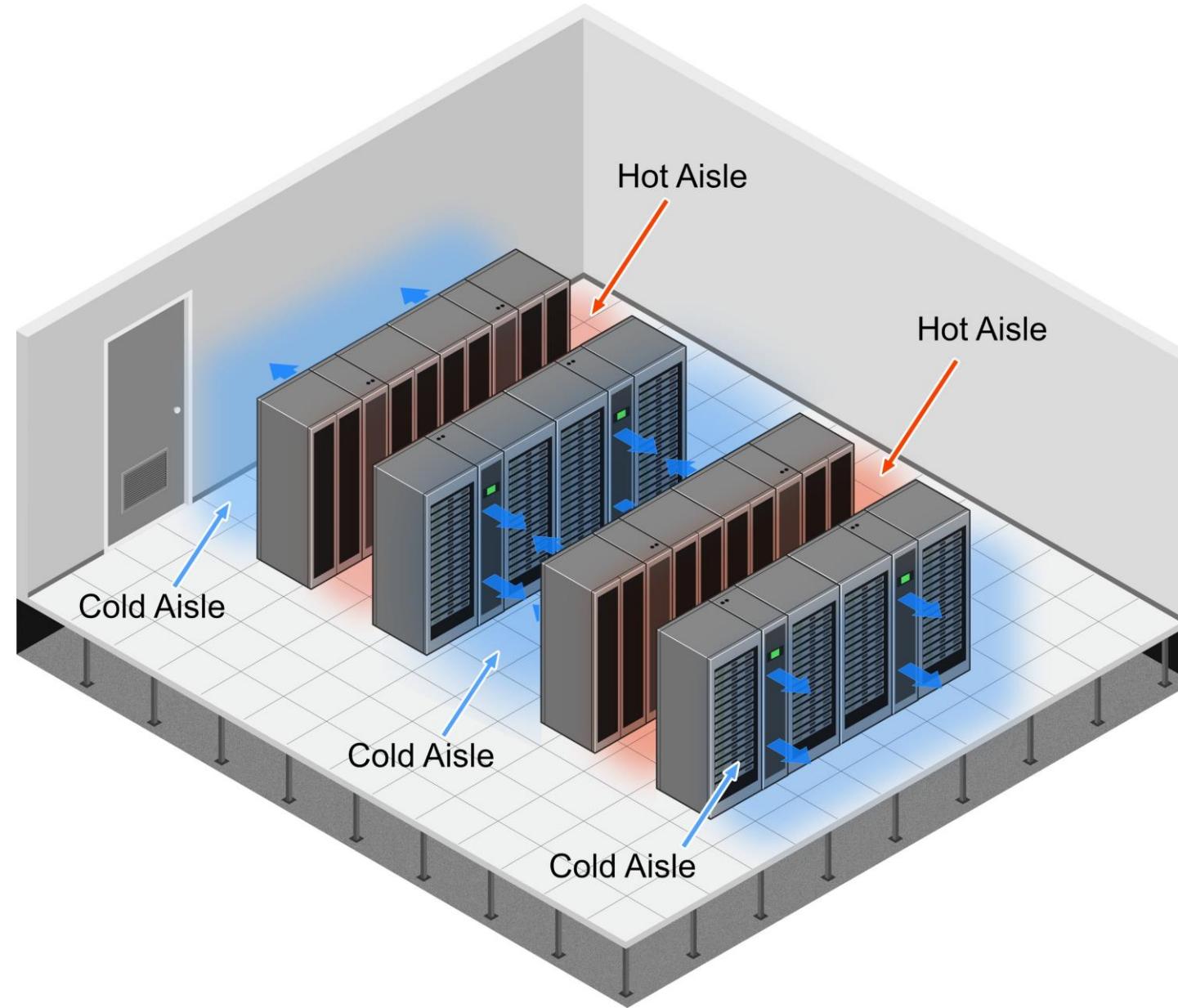


What is inside a data center?

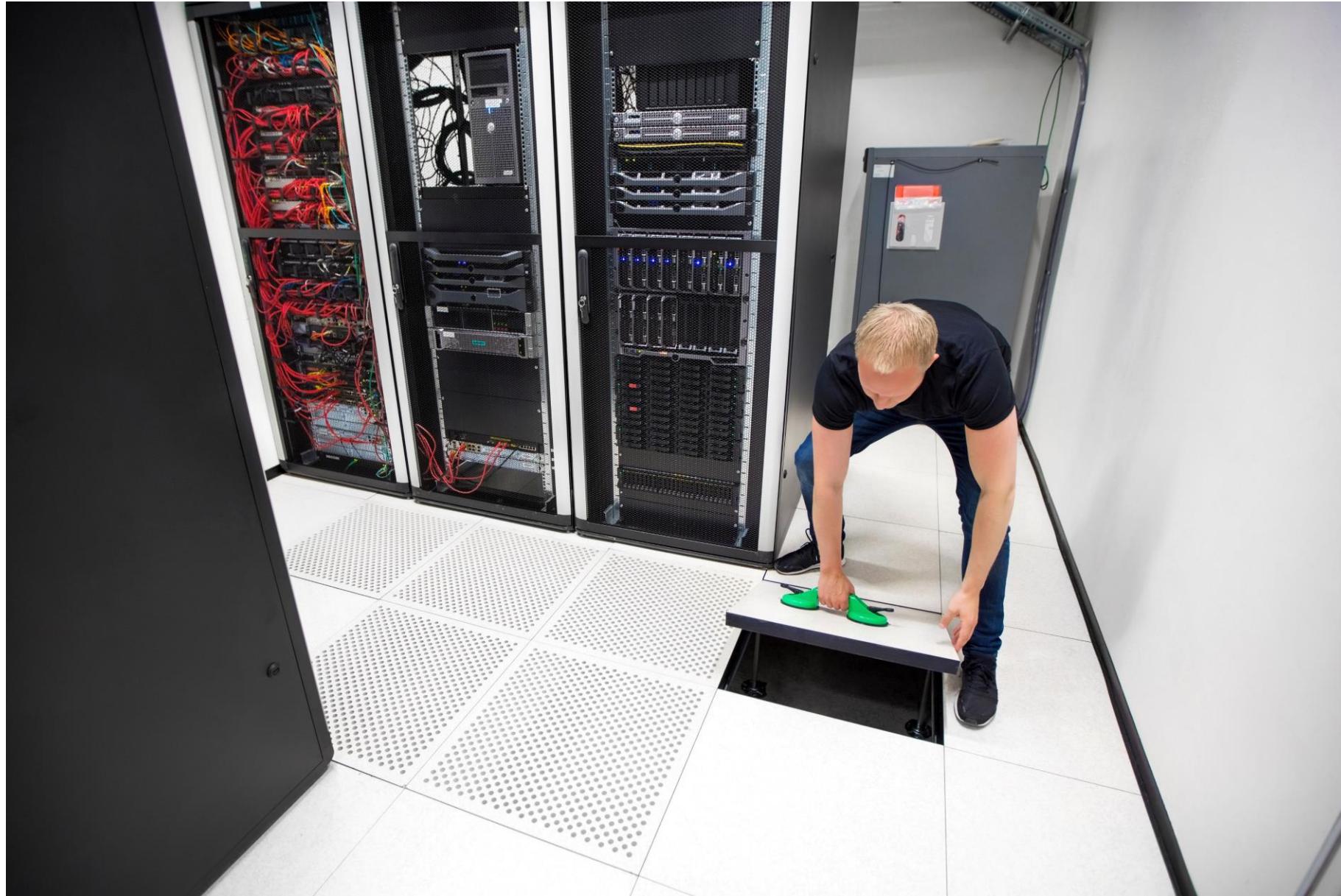
- IT infrastructure
 - Servers
 - Storage
 - Network
- Support infrastructure
 - Power subsystems
 - Uninterruptible power supplies (UPS)
 - Backup generators
 - Ventilation and cooling equipment
 - Fire suppression systems
 - Building security systems



What is inside a data center?



What is inside a data center?





Server Fundamentals

How is a server different from a desktop?



Reliable



Fast

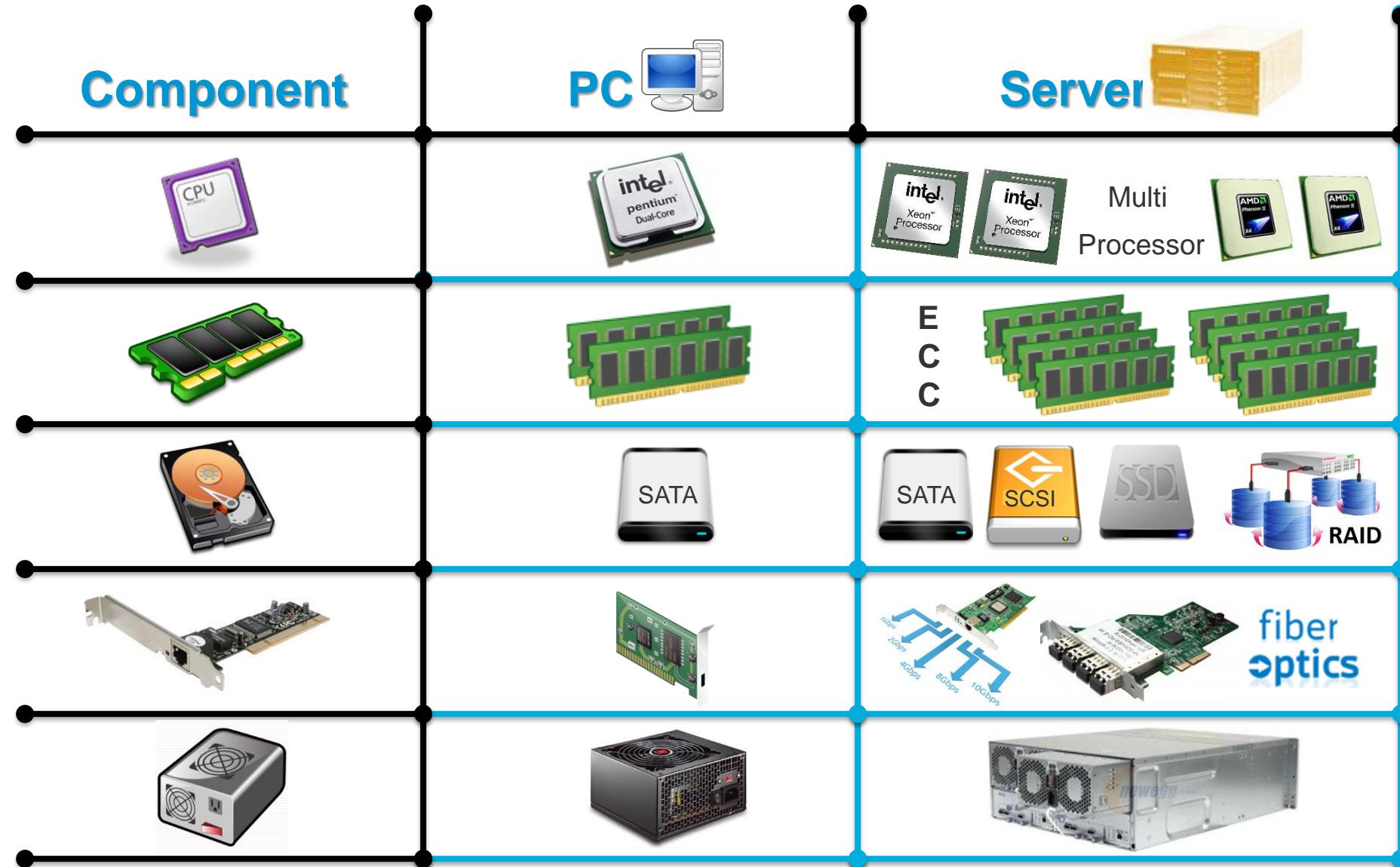


Redundant



Scalable

Key Differences



Server Form Factor

Servers come in three chassis styles.



Tower

Provide standalone computing and can be placed pretty much anywhere.

Rack

As the name suggests, are designed to slot into a rack (server enclosure).

Blade

Provide the highest density computing and are aimed at larger, processing hungry datacenters.

Rack Server



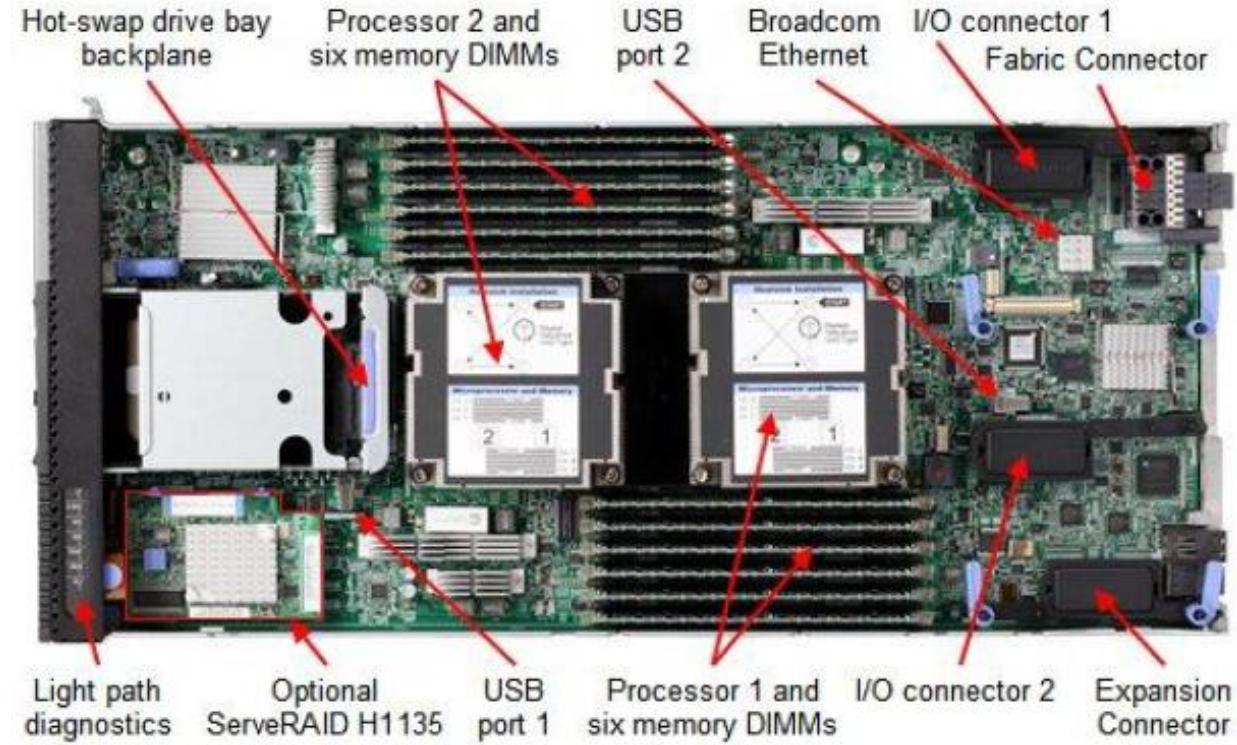
Blade Server



Blade Server

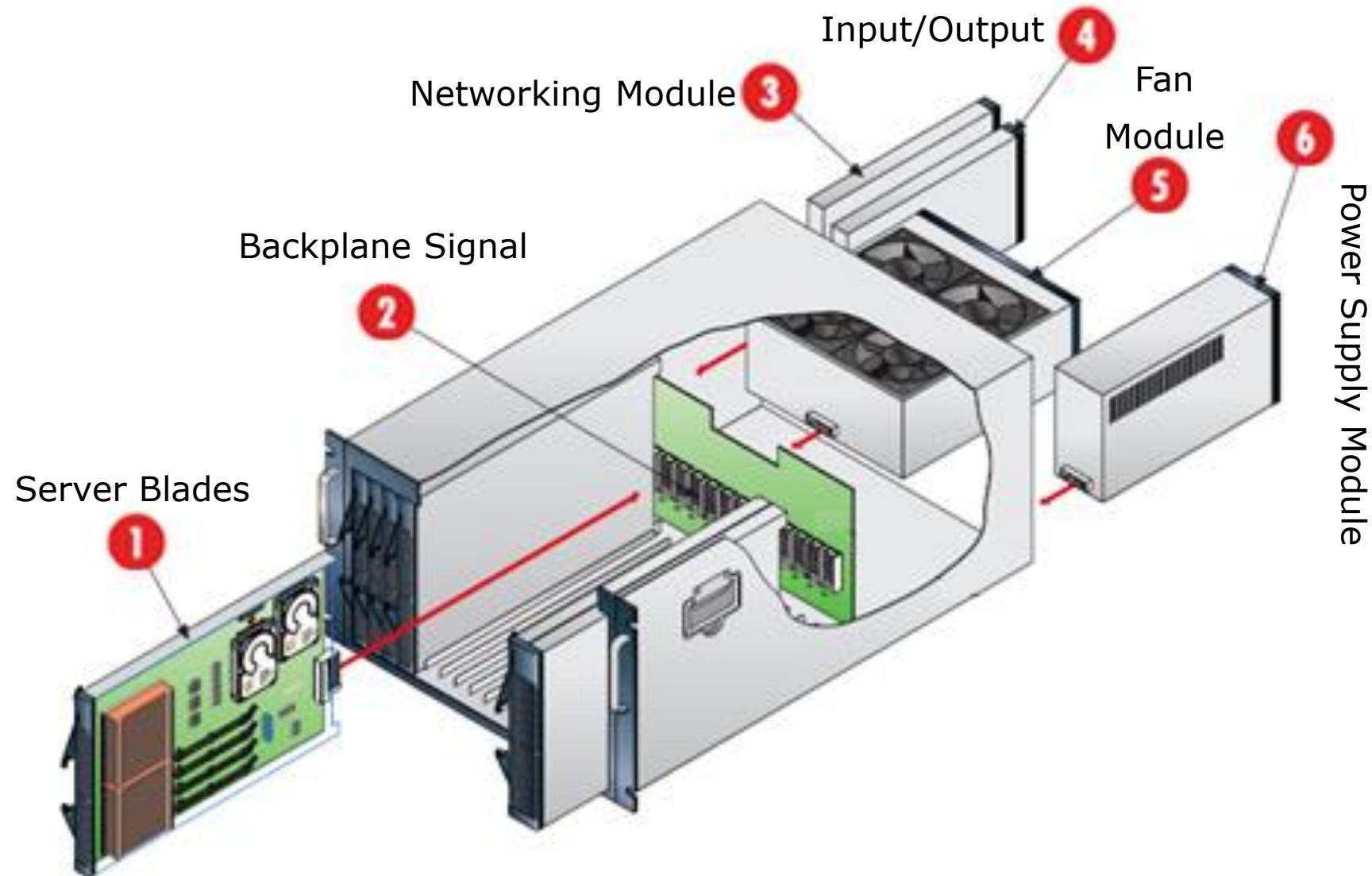


Inside a Blade Server



- A blade environment generally has much less of cabling than tower or rack environments since a lot of the connectivity is handled internally.
- Adding a new server consists of simply sliding it into a slot in the chassis.
- Bladed servers eliminate the space issue but can pose unique power and cooling concerns. Further, when it comes to I/O expansion options, blade servers are a bit limited by their lack of expansion slots.

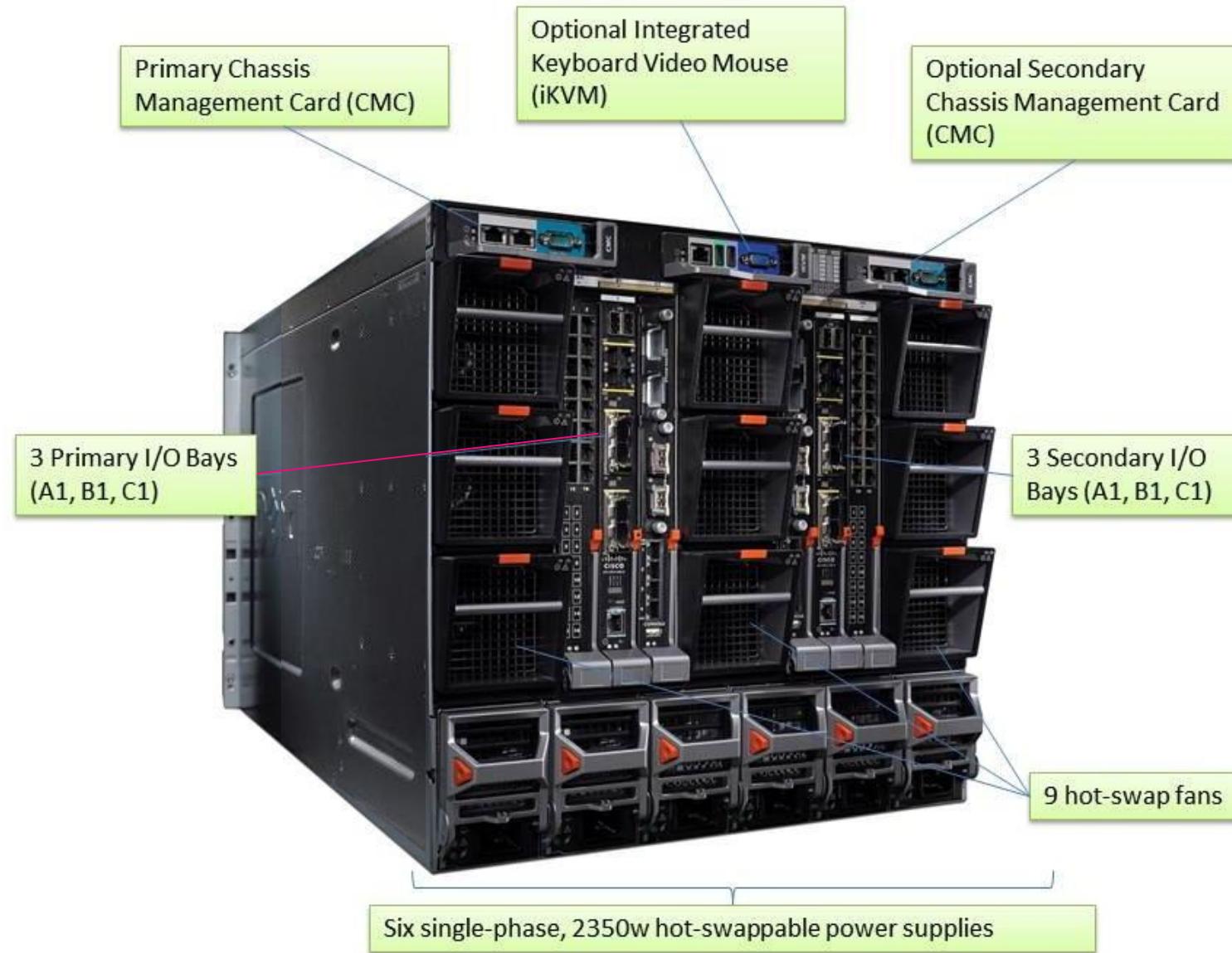
Blade Server Components



Blade Server - Dell M1000e Chassis (front)



Blade Server - Dell M1000e Chassis (rear)



Remote Management Software

https://10.0.72.51/index.html Certificate error Home | Sign Out

iLO 4: WE1SIL01 - ILOCZJ34... Local User: Administrator iLO Hostname: ILOCZJ34.local

hp iLO 4 ProLiant DL360p Gen8

Expand All

- Information
 - Overview
 - System Information**
 - iLO Event Log
 - Integrated Management Log
 - Active Health System Log
 - Diagnostics
 - Location Discovery Services
 - Insight Agent
- + Remote Console
- + Virtual Media
- + Power Management
- + Network
- + Remote Support
- + Administration

System Information - Power Information

Power Supply Summary

Present Power Reading	76 Watts
Power Management Controller Firmware Version	3.2
Power Status	Redundant
HP Power Discovery Services Status	N/A
High Efficiency Mode	Balanced

Power Supplies

Bay	Present	Status	PDS	Hotplug	Model	Spare	Serial	Capacity	Firmware
1		Good, In Use	✓ Yes	✓ Yes	656362-B21	660184-001	5BXRD0	460 Watts	1.03
2		Good, In Use	✓ Yes	✓ Yes	656362-B21	660184-001	5BXRD0	460 Watts	1.03

POWER: ON UID: OFF 100%

Remote Management Software

Integrated Dell Remote Access Controller 6 - Enterprise

[Support](#) | [Help](#) | [About](#) | [Logout](#)



[Properties](#) | [Setup](#) | [Power Management](#) | [Logs](#) | [Alert Management](#) | [Console/Media](#) | [VFlash](#)

PowerEdge R610
root , Admin

[System Summary](#) | [System Details](#)

System Summary

[Print](#) | [Refresh](#)

Server Health

Status	Component
✓	Batteries
✓	Fans
✓	Intrusion
✓	Power Supplies
✓	Temperatures
✓	Voltages

Quick Launch Tasks

- [Power ON / OFF](#)
- [Power Cycle System \(cold boot\)](#)
- [Launch Viewer](#)
- [View System Event Log](#)
- [View iDRAC Log](#)
- [Update Firmware](#)



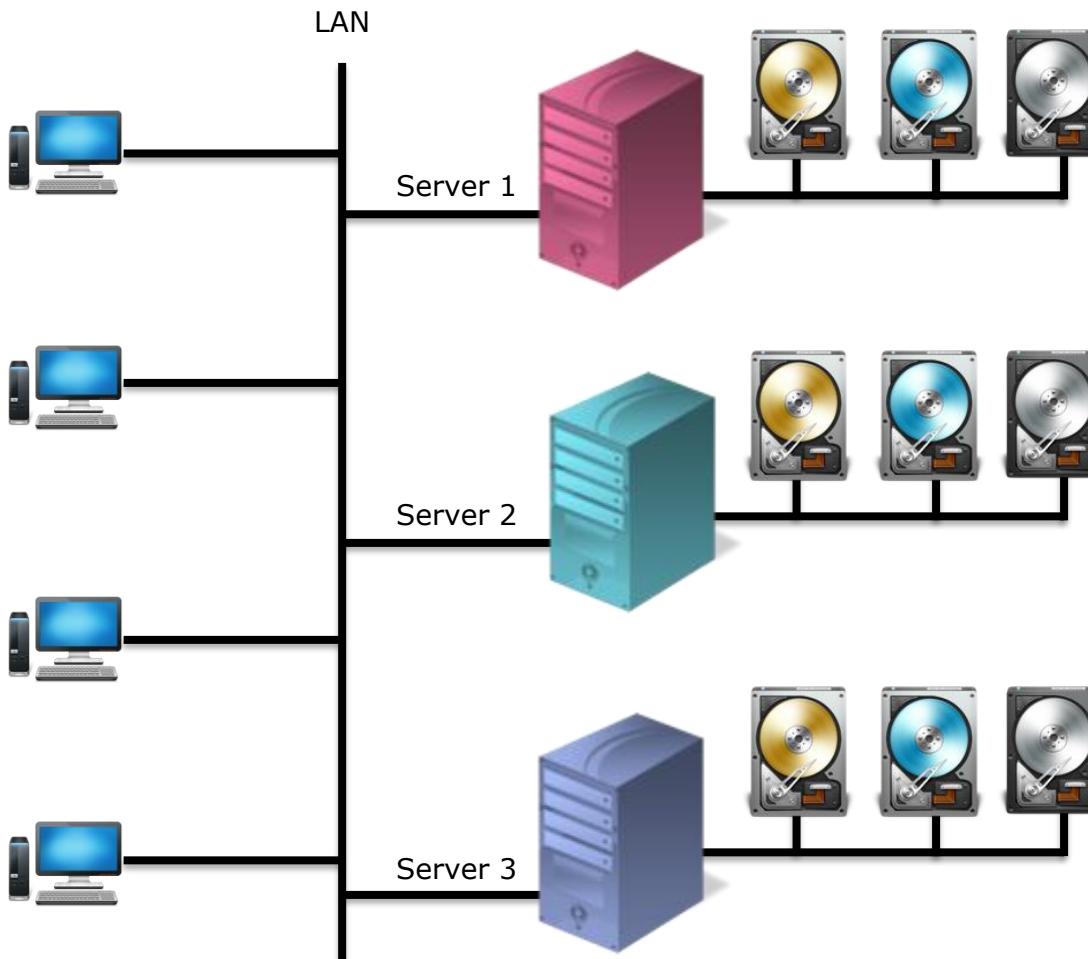
Storage Fundamentals

Storage Architecture – Local Storage

- Fast
- Low Cost
- Typically used for installing OS and non critical data

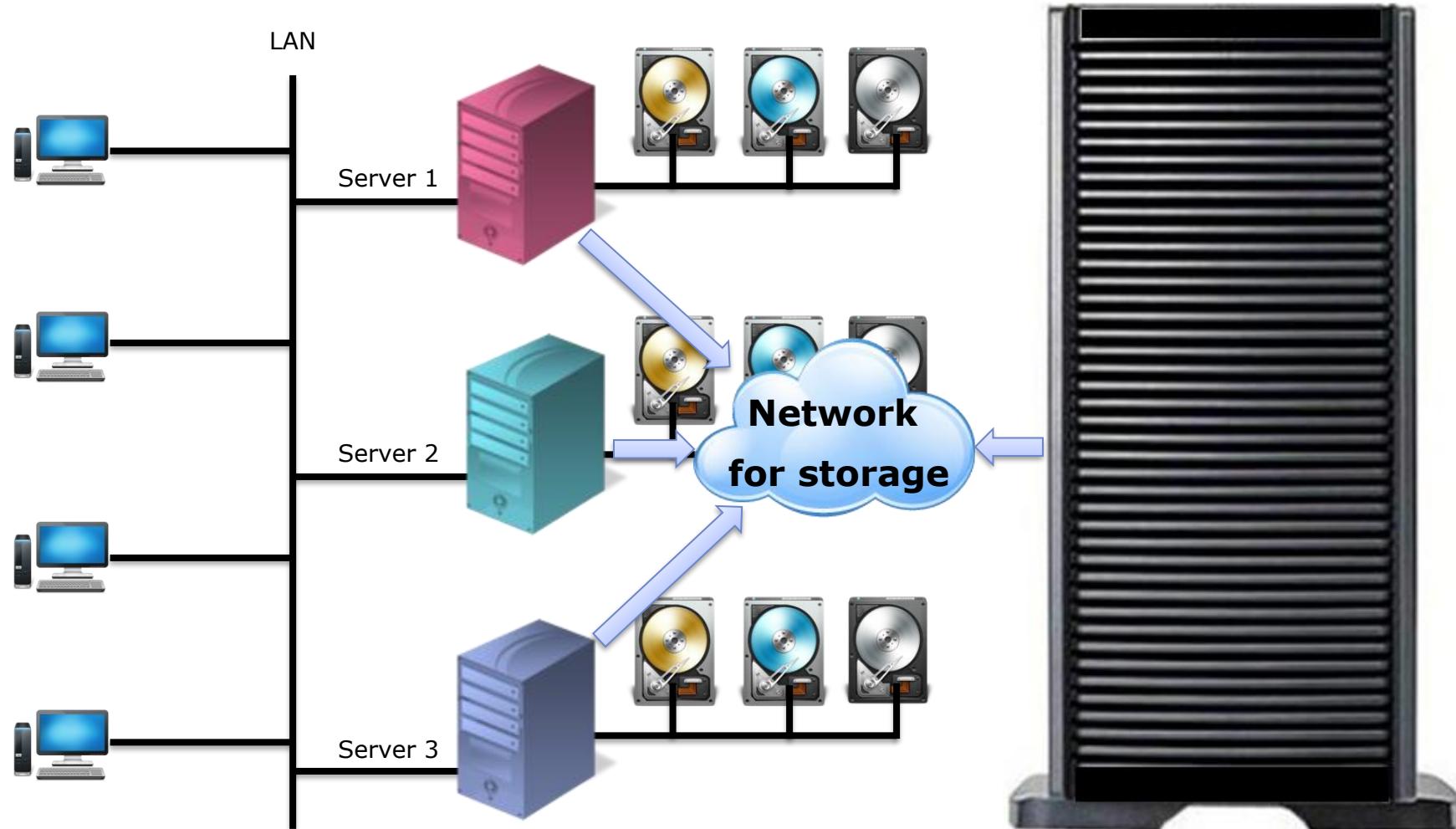


Storage Architecture – Local Storage

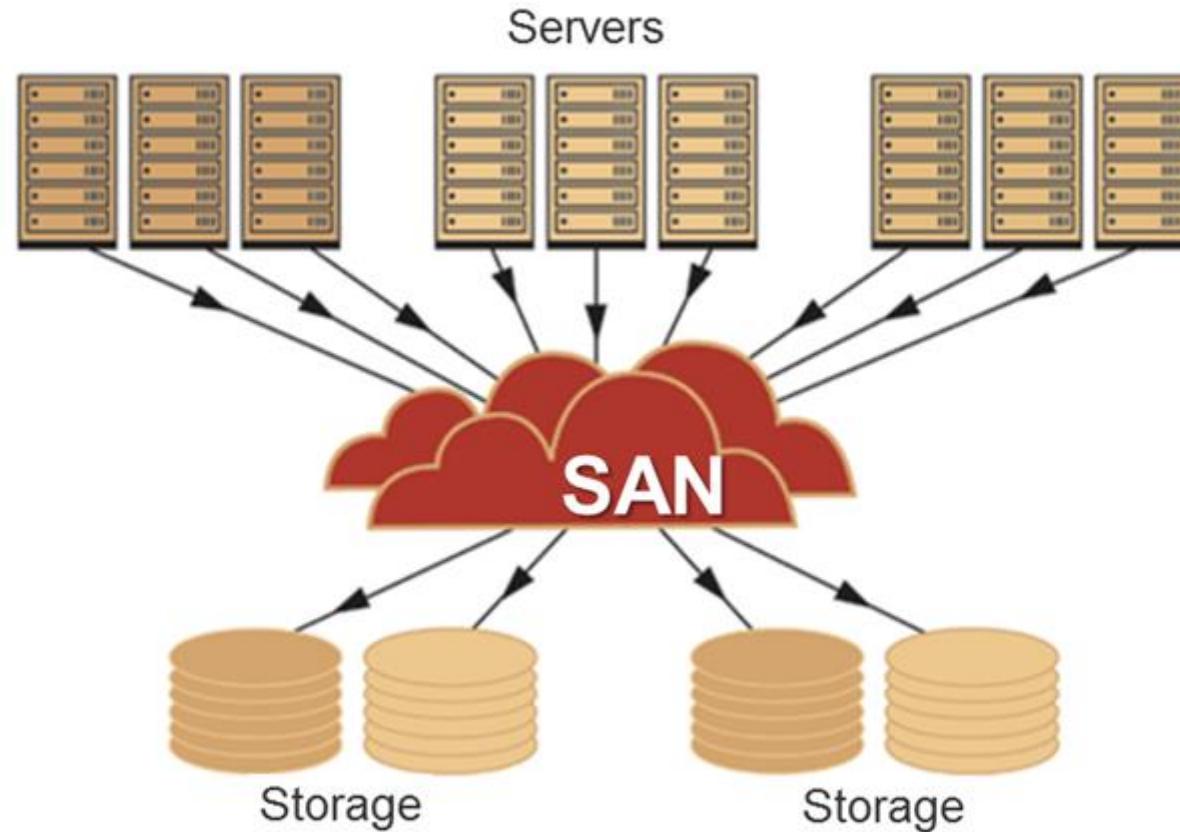


- Storage connected to a single Server.
- Other servers cannot directly access the data
- Generally connected together by SCSI cables (25 meters)
- Capacity is limited

Storage Architecture – Centralized Storage

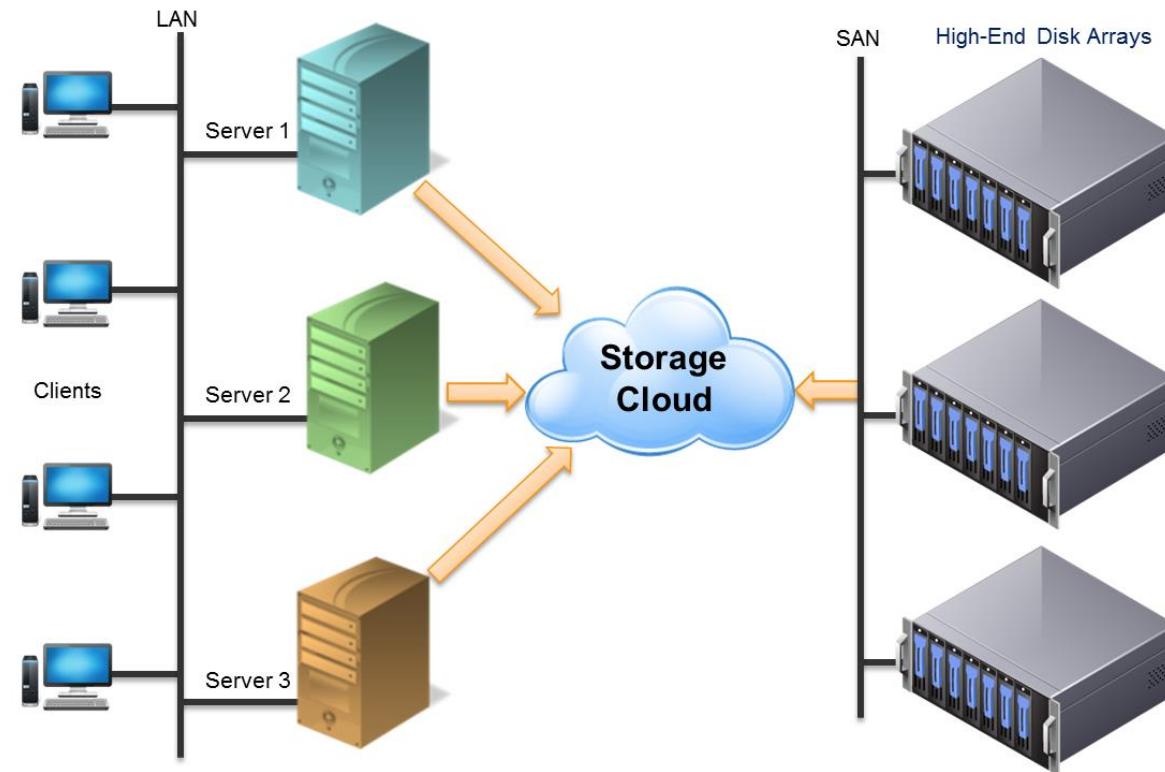


Storage Area Network (SAN)



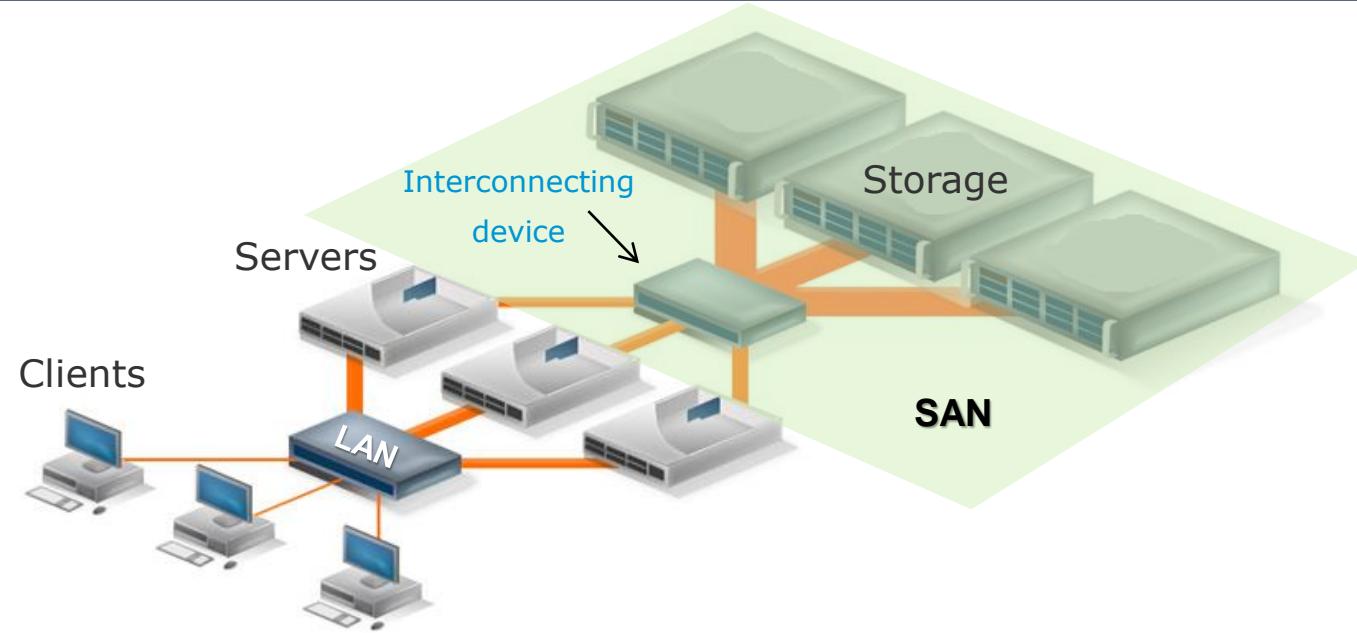
SNIA defines the SAN as a network whose primary purpose is the transfer of data between computer systems and storage elements.

Storage Area Network (SAN)



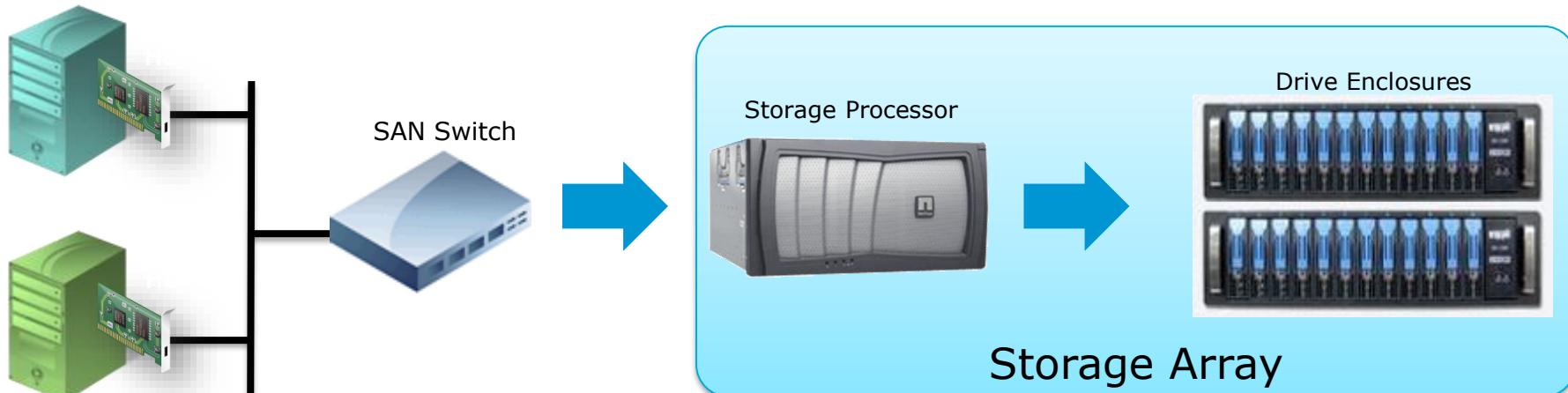
- It is sometimes referred to as “the network behind the servers.”
- Client computers are not connected to the SAN, but communicate with the servers to access files from the storage devices.
- A SAN makes it appear as though a disk array that is remotely located is locally attached to the server.

Storage Area Network (SAN)



- A SAN allows “any-to-any” connection across the network, using interconnect devices.
- Special networking protocols allow servers to send block-level read and write operations to the storage devices.
- Performance is similar to data access from direct attached storage, but with greater distances and shared storage.
- Access to data through logical blocks and not to file

SAN : Components



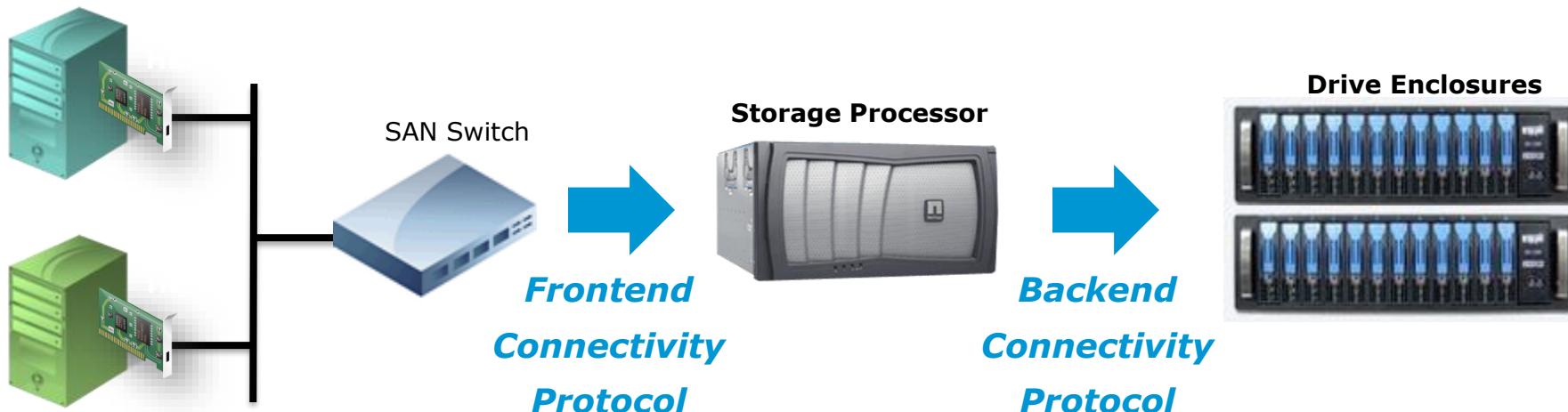
HBA: An HBA (Host Bus Adapter) is the interface card that connects a host to a SAN. For redundancy, you can use multiple HBAs.

SAN Switch: SAN switches connect various elements of the SAN. Particular, they connect hosts to storage controllers.

Storage Processor: It a server responsible for performing a wide range of functions for the storage system like RAID, volume management. etc.

Drive Enclosure: Is a hardware which houses hard disks drives

SAN : Protocols



Frontend Connectivity Protocol

- Frontend connectivity of a SAN is where the servers /Host are connected either directly or through the SAN switch
 - Fibre Channel Protocol
 - iSCSI
 - FCoE

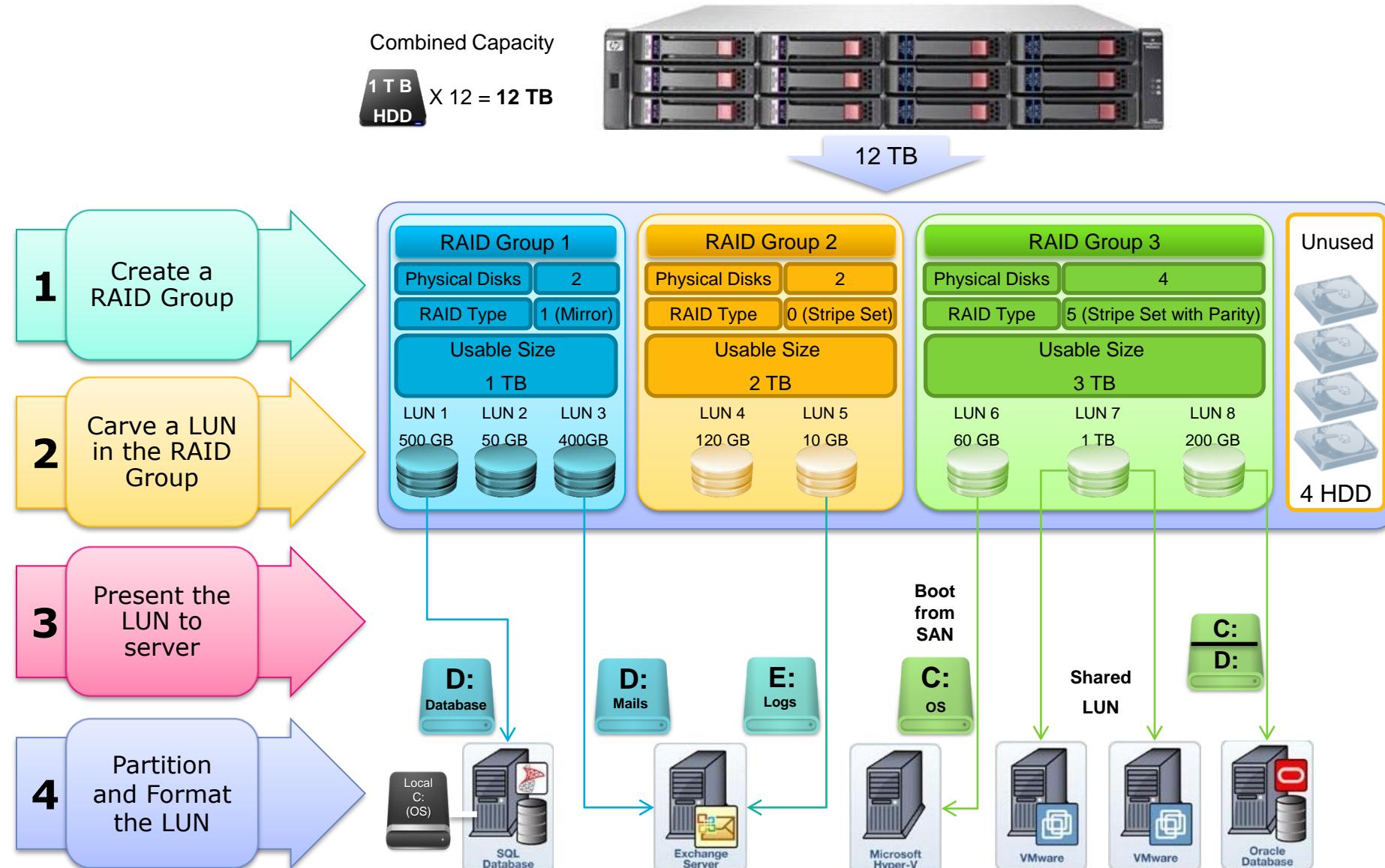
Backend Connectivity Protocol

- Backend Connectivity of a SAN connects to drive enclosures which house the hard disk drives for storing data
 - SCSI
 - SATA
 - Fibre Channel
 - SAS
 - FATA

LUN (Logical Unit Number)

- Storage devices have a lot of hard disks in its back-end. In order to provide redundancy, protection and additional functionality, the hard disks are not directly presented to the servers.
- Available storage capacity is sliced into usable chunks, and presented to servers. This sliced storage is called a LUN (Logical Unit Number).
- Once presented to the server it looks like a local hard disk to the server.
- LUNs are the virtual representations of a disk. In reality, a LUN may span multiple physical disks.
- Each logical unit has an identification (ID), known as the LUN ID, which allows it to be uniquely identified.
- LUNs are accessed via SAN protocols, iSCSI/FC/FCoE.

Carving and Presenting a LUN



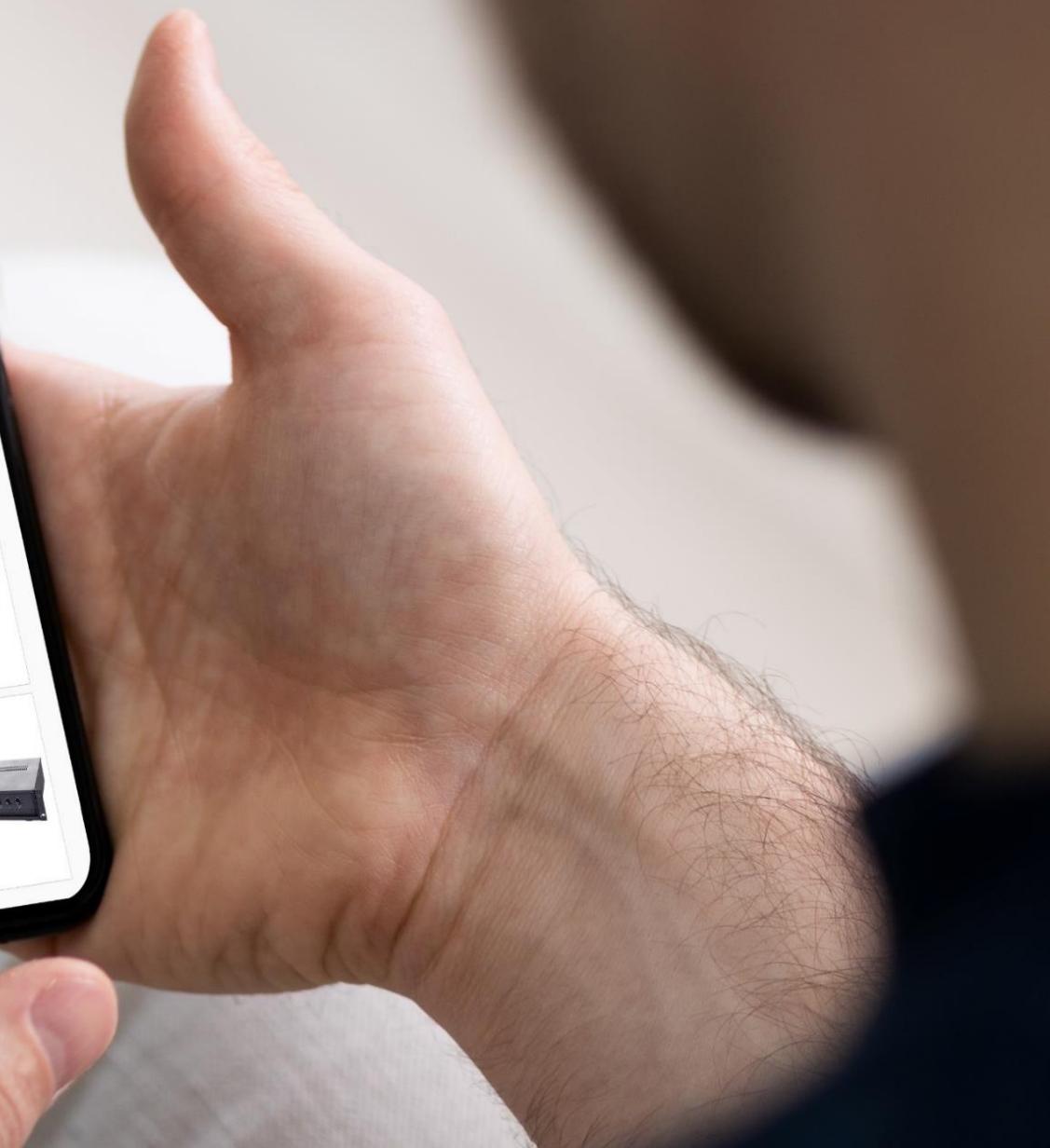
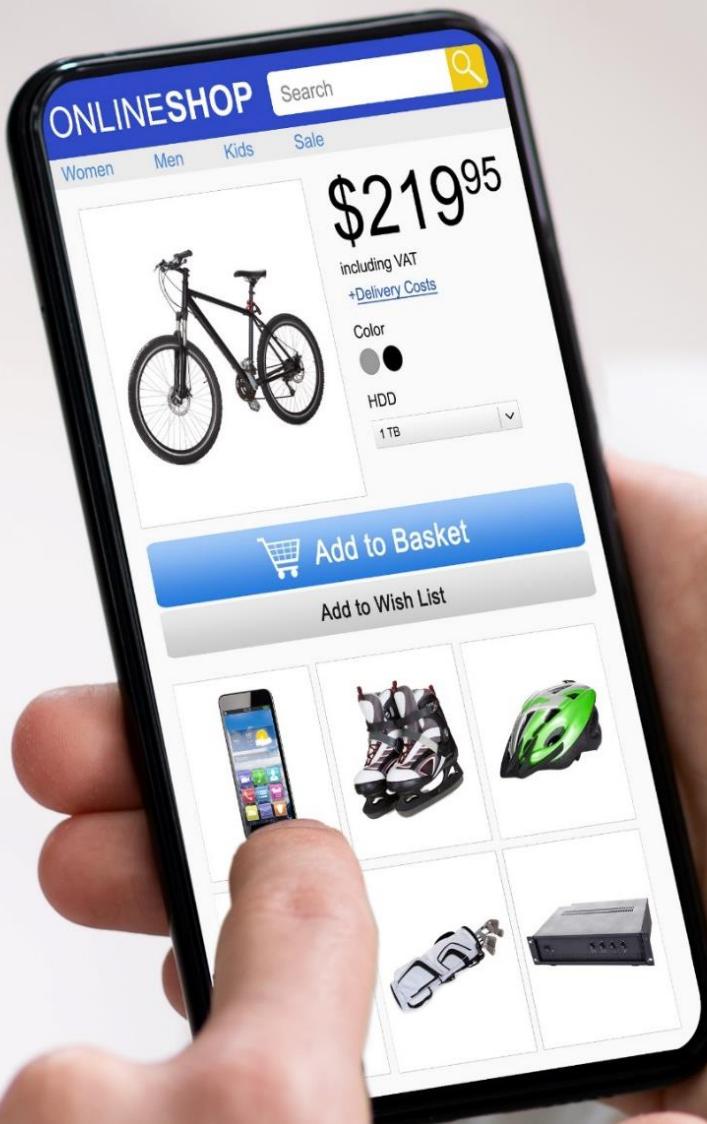


5 Minutes
Break



If you are back
type in chat...

What you
recently
purchased
online?



Security Track

Week 1



Cost of a Data Breach Report 2022 – By IBM Security

- Average Time to **identify** a Security breach?

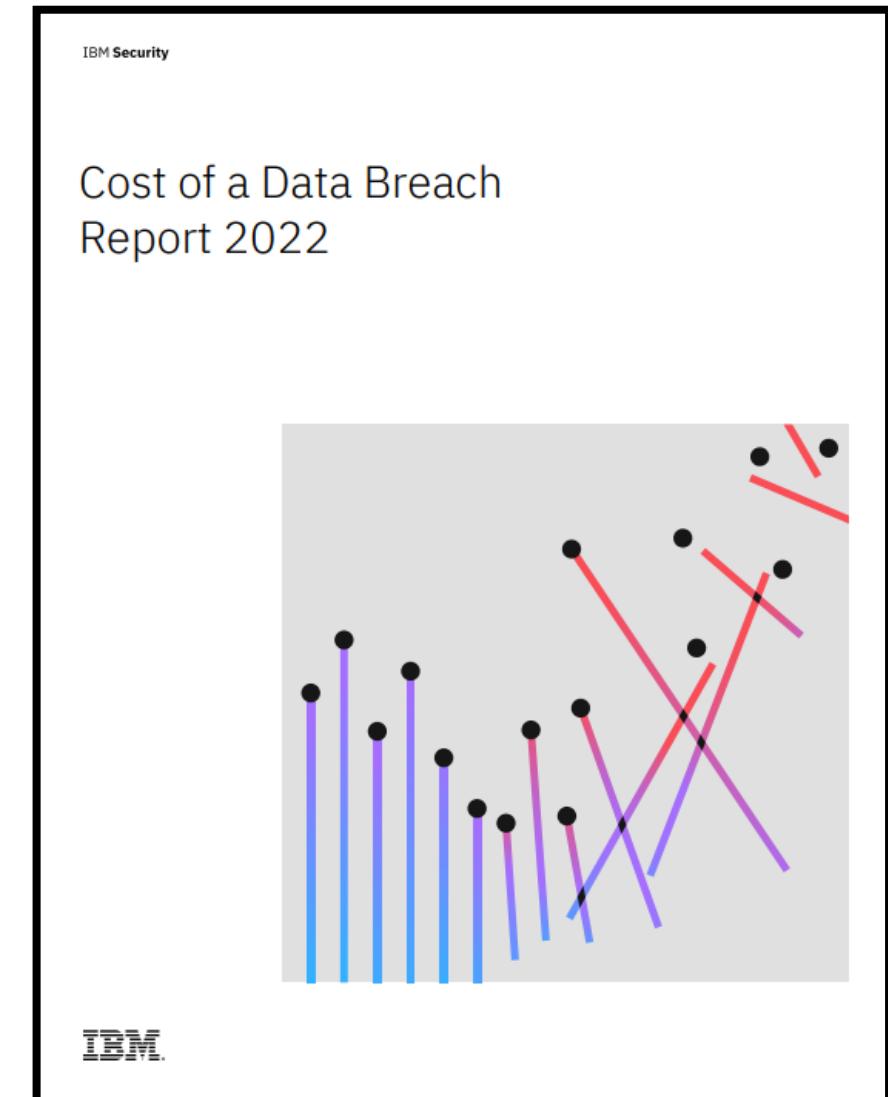
207 Days

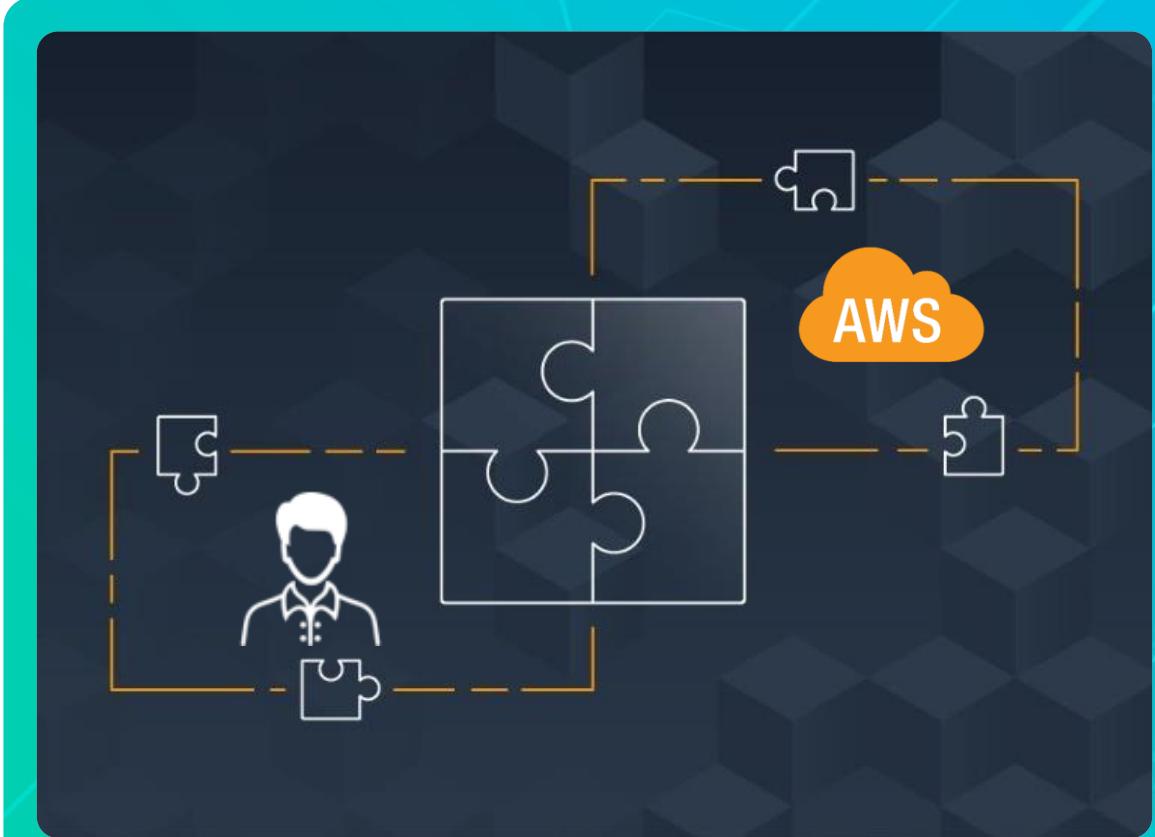
- Average Time to **contain** a breach?

70 Days

- Average time to identify and contain a data breach

277 Days





Shared Responsibility Model

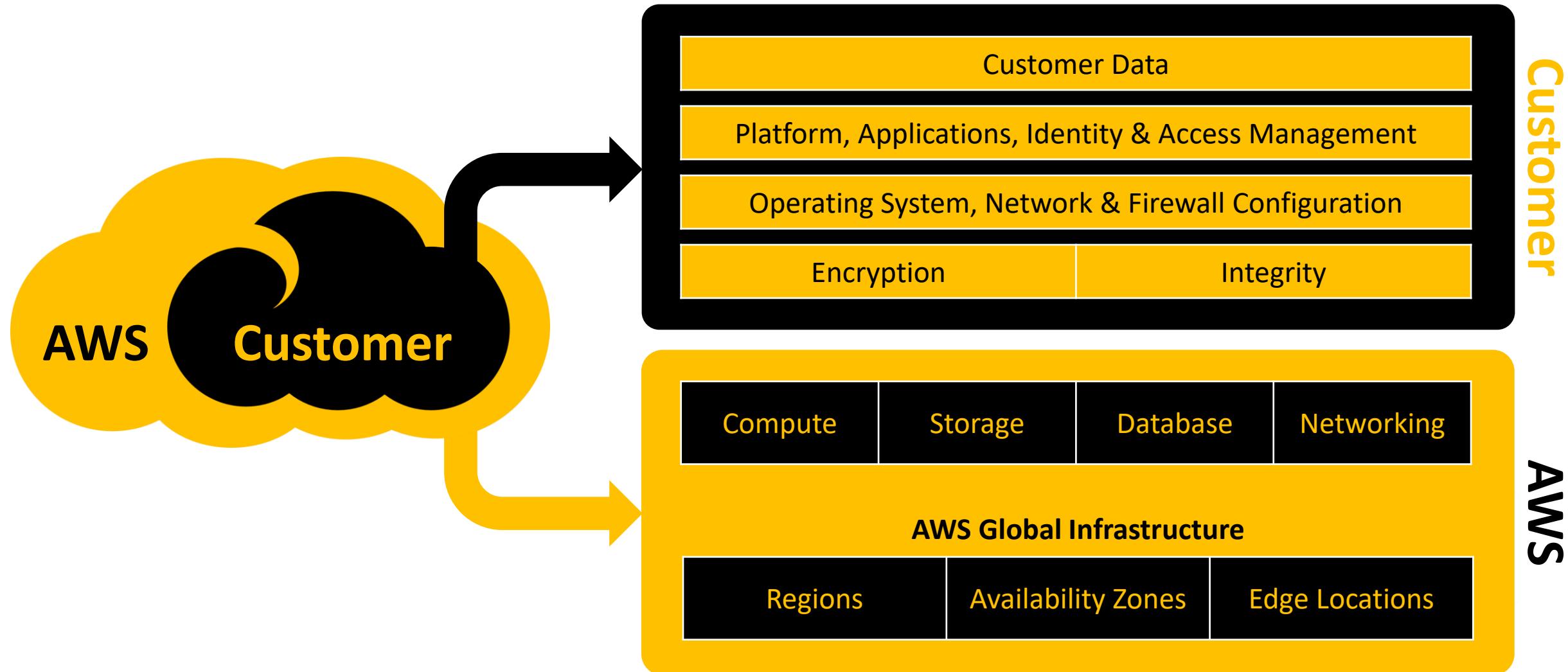
Shared Responsibility for my apartment

	Building Management Responsibility	My Responsibility
	Door Phone	Always verify before remotely opening door
	Camera	Ensure its operational
	Access Card	Keep it safe
	Lock and Key	Always lock
	Fire Exit	Keep it clear

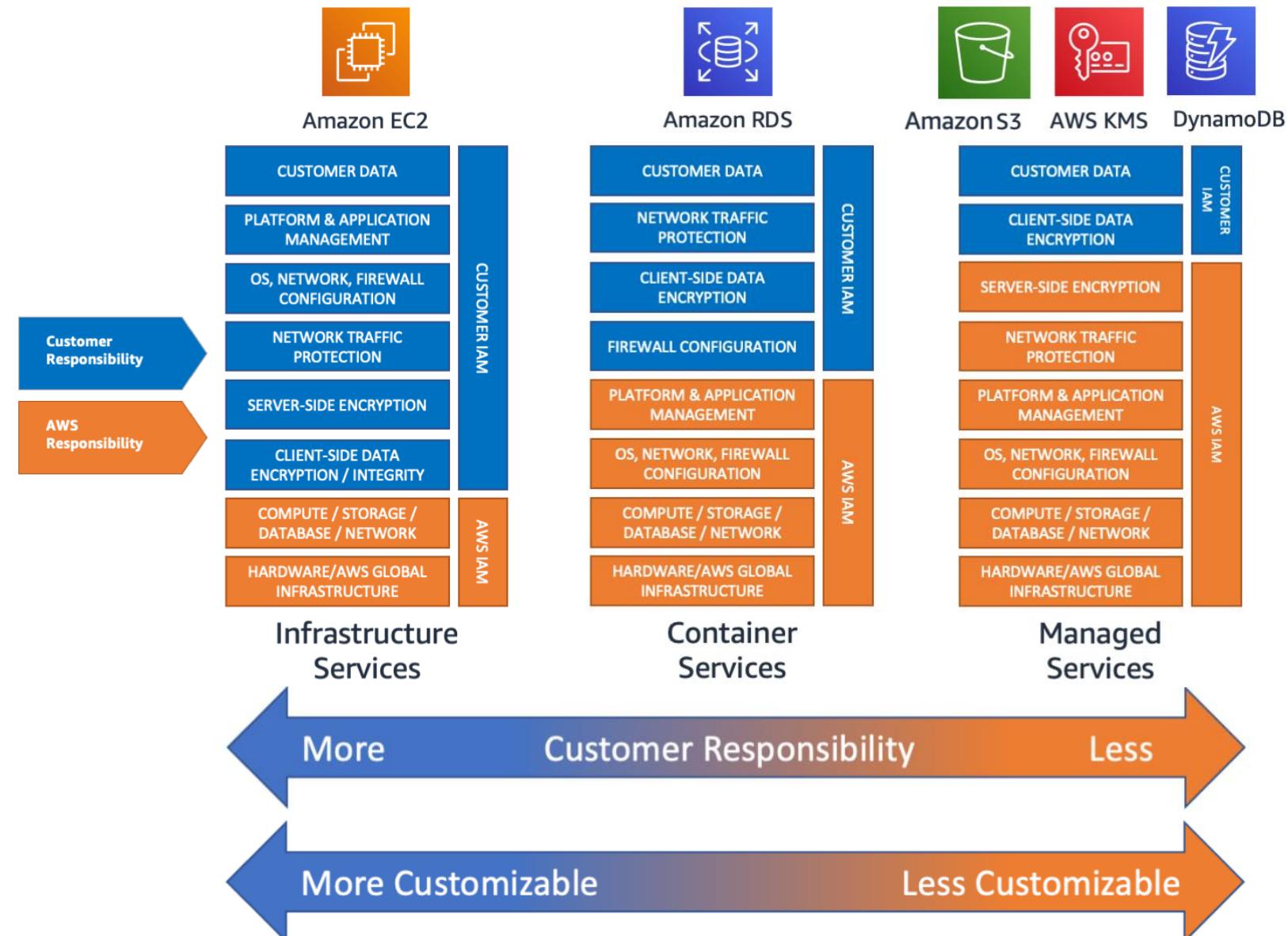
AWS Shared Responsibility Model



AWS Shared Responsibility Model



AWS Shared Responsibility Model





AWS Security Services

AWS Foundational and Layered Security Services



AWS Security Hub



AWS Organizations



AWS Transit Gateway



Amazon VPC



AWS IoT Device Defender



Amazon Cloud Directory



AWS Control Tower



AWS Trusted Advisor



Amazon VPC PrivateLink



AWS Direct Connect



Resource Access manager



AWS Directory Service



Amazon GuardDuty



Amazon Inspector



Amazon CloudWatch



AWS Step Functions



AWS OpsWorks



AWS CloudFormation

Automate

Identify



Protect



Detect



Respond



Recover



AWS Service Catalog



AWS Config



AWS Shield



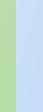
IAM



AWS Secrets Manager



KMS



Amazon Cognito



AWS Well-Architected Tool



AWS Systems Manager



AWS WAF



AWS Firewall Manager



AWS Certificate Manager



AWS CloudHSM



AWS IAM Identity Center



Amazon Macie



Amazon Detective



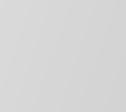
Amazon CloudWatch



AWS CloudTrail



Amazon S3 Glacier



Snapshot



Archive



Amazon GuardDuty



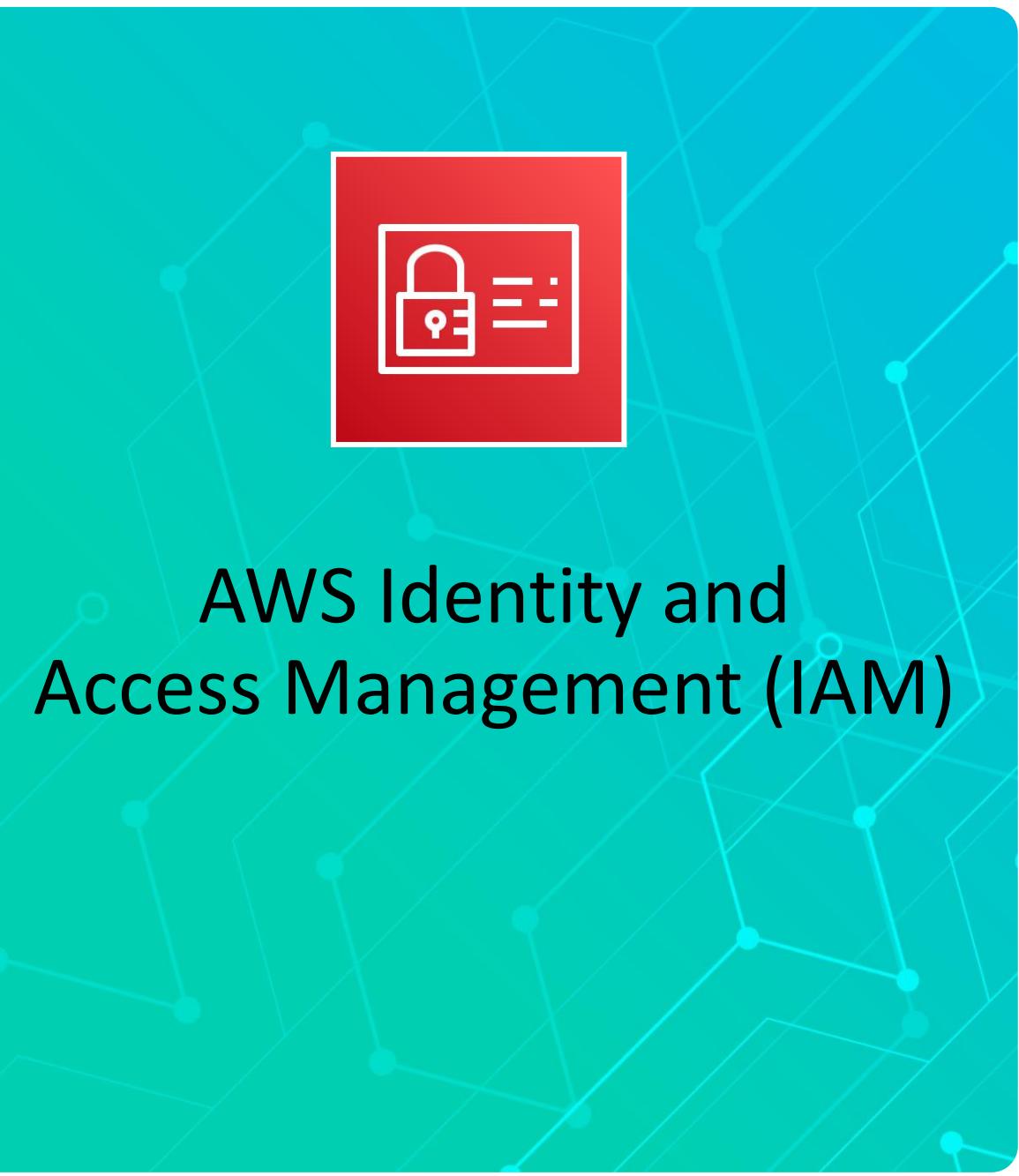
AWS Step Functions



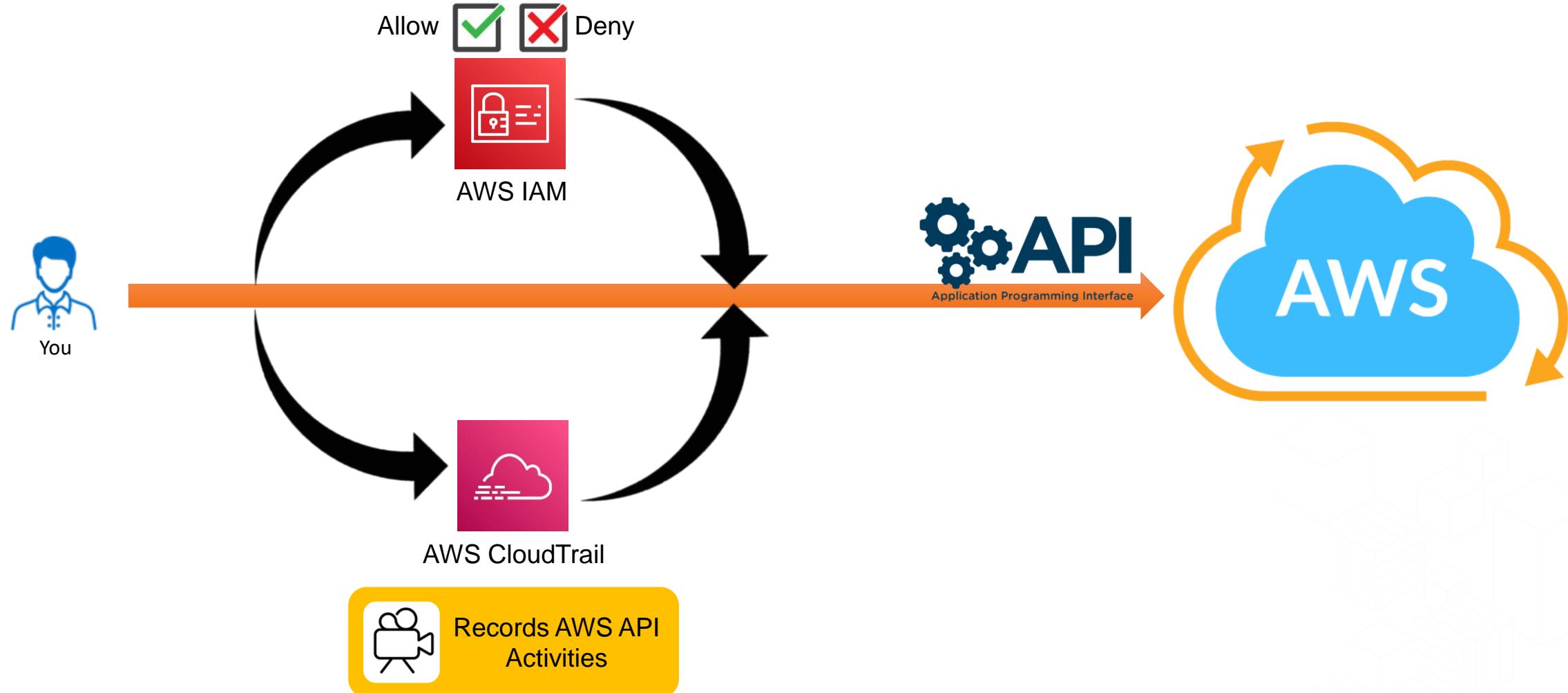
AWS OpsWorks



AWS CloudFormation



Flow of a request to AWS



Traveling to another country

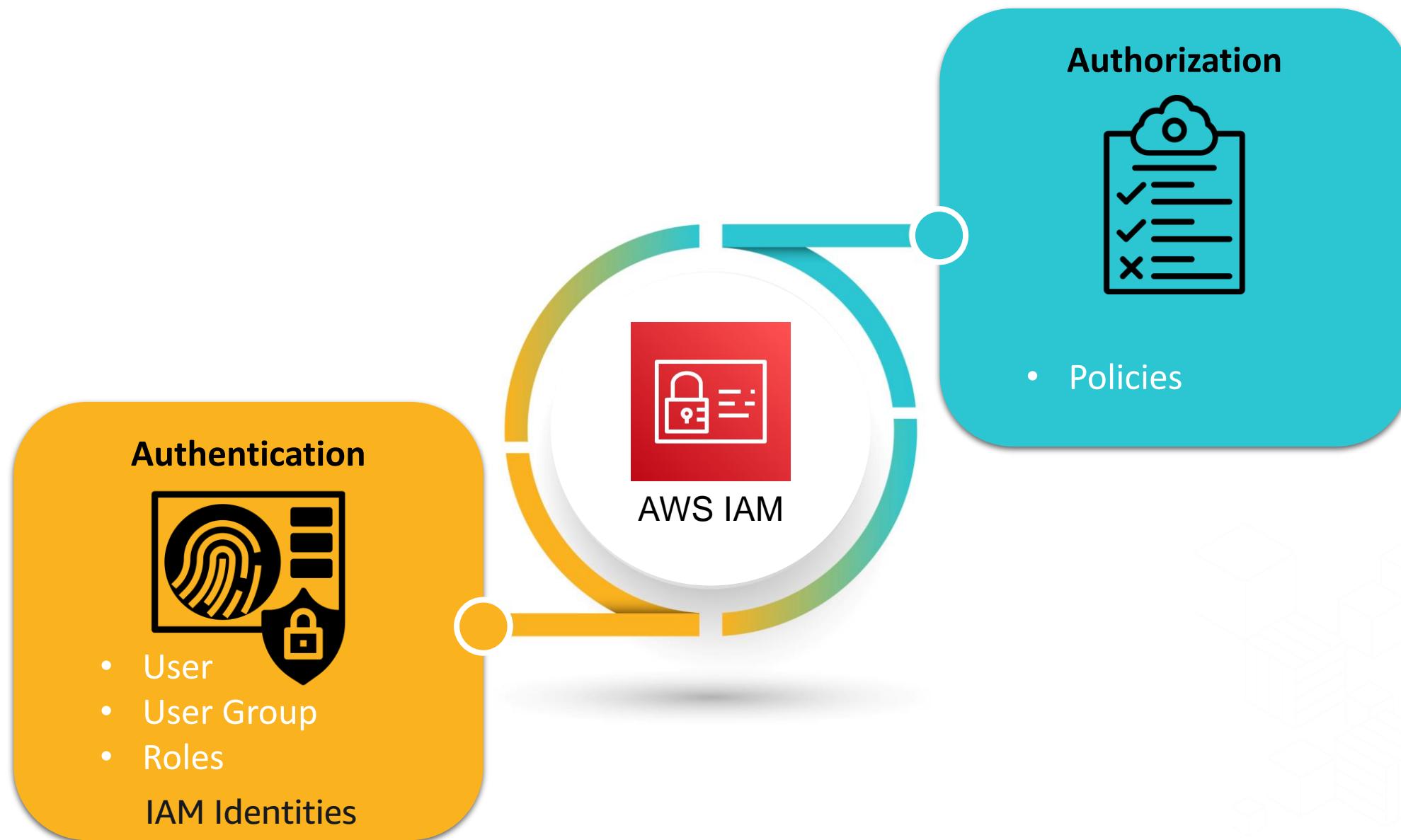
- Visa (Tourist visa / Work visa)

What can you do?

(Authorization)

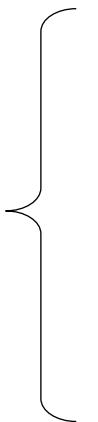


AWS IAM



Accessing AWS Services

IAM Username
and Password

A screenshot of the AWS Management Console sign-in page. It includes fields for 'Account' (12 Digit Account ID), 'User Name' (IAM Username), 'Password', 'MFA Code' (Optional MFA), and checkboxes for 'I have an MFA Token' and 'Sign In'. A note at the bottom says 'Sign-in using root account credentials'.

AWS
Management
Console

Access Key and
Secret Access Key



```
C:\Users>aws configure
AWS Access Key ID [None]: Access Key
AWS Secret Access Key [None]: Secret Access Key
Default region name [None]: Region
Default output format [None]: JSON / Text / Table
```



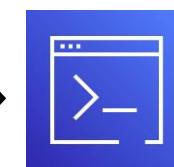
AWS
Command
Line Interface

A screenshot of a code editor showing the contents of a 'credentials' file in the '.aws' directory. It contains a section named '[default]' with 'aws_access_key_id = Access Key' and 'aws_secret_access_key = Secret Access Key'.

AWS Tools
and SDKs



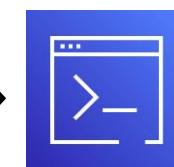
AWS
Management
Console



AWS
Command
Line Interface



AWS Tools
and SDKs



AWS
Command
Line Interface

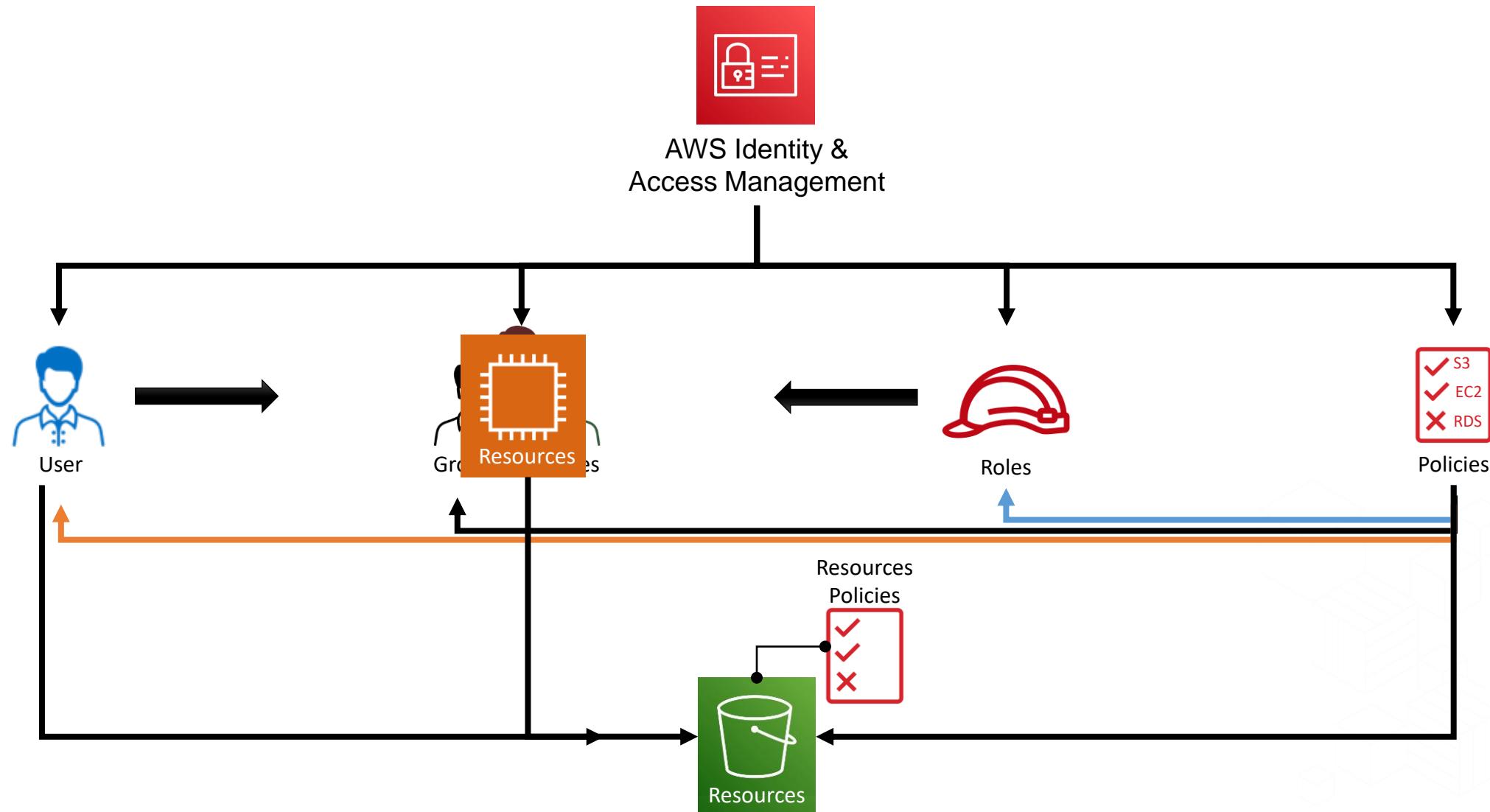


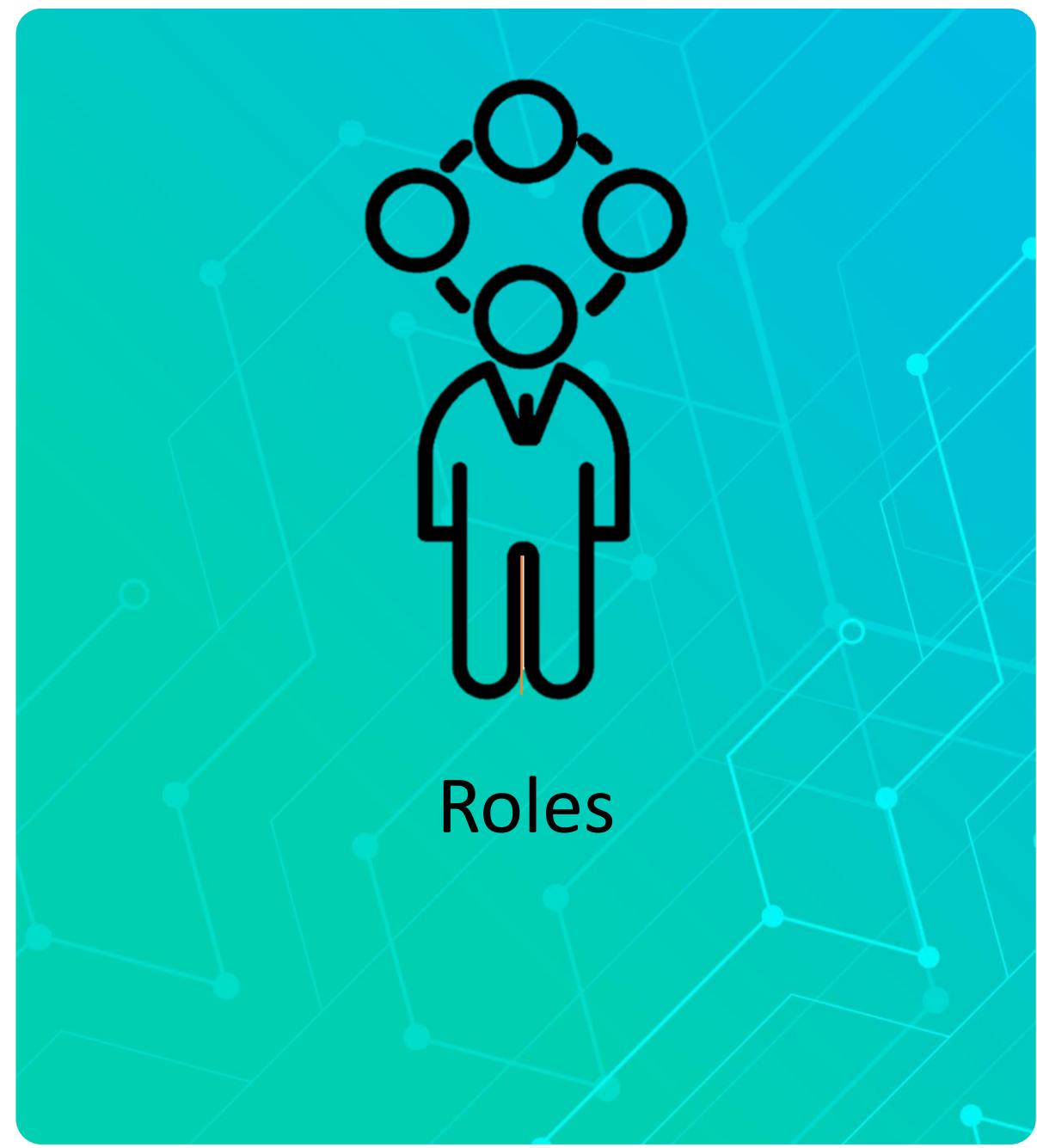
API
Application Programming Interface



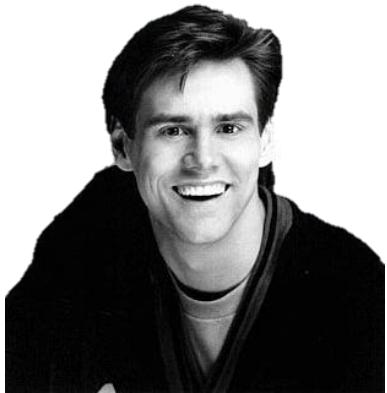
AWS

AWS IAM Summary





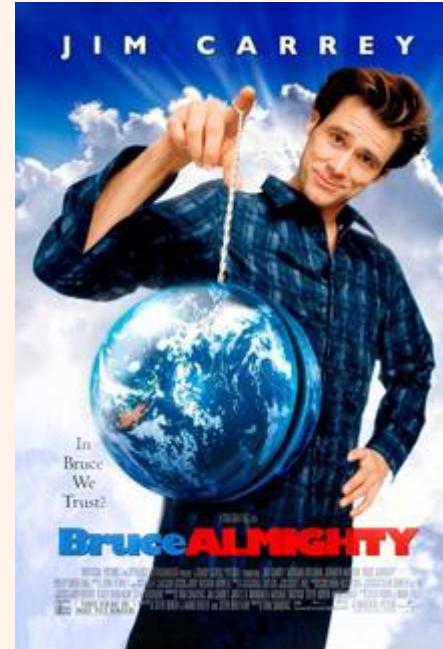
Understanding Role



Jim Carrey

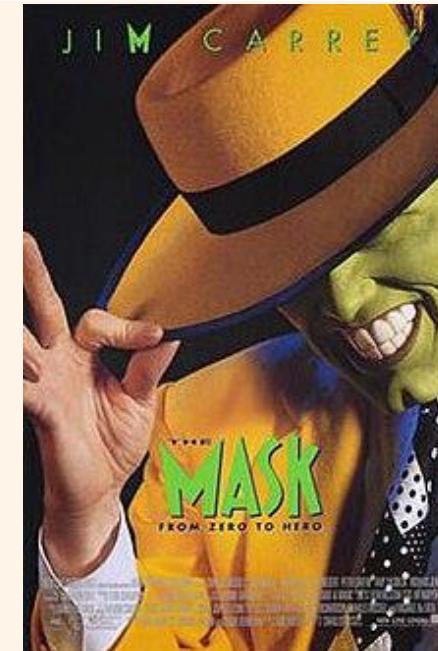
Canadian-American
Actor

Bruce Almighty



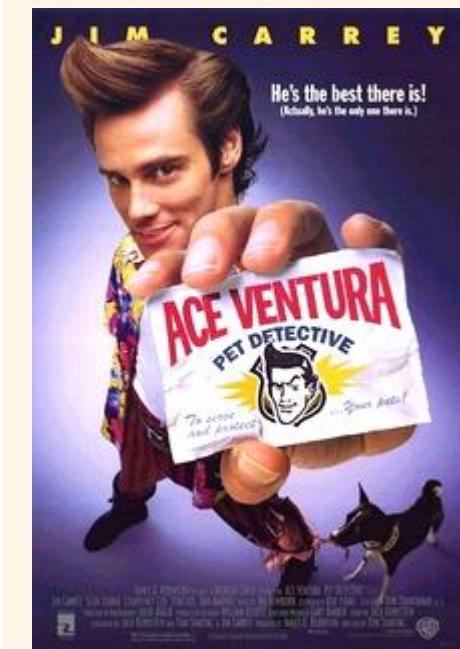
Role
God

The Mask



Role
The Green Thing

Ace Ventura



Role
Pet Detective

Assuming a role

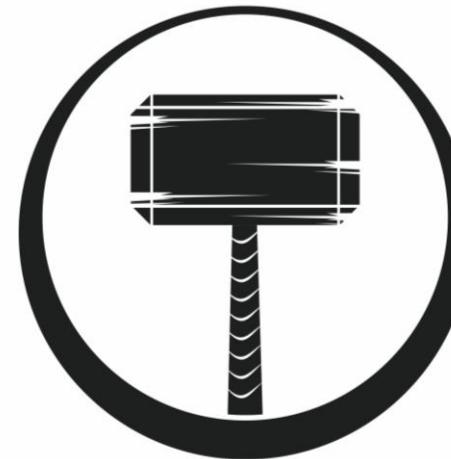


<https://cinespia.org/event/the-mask/>

<https://www.youtube.com/watch?v=GEVfiRbYA8o>

Trust Policy

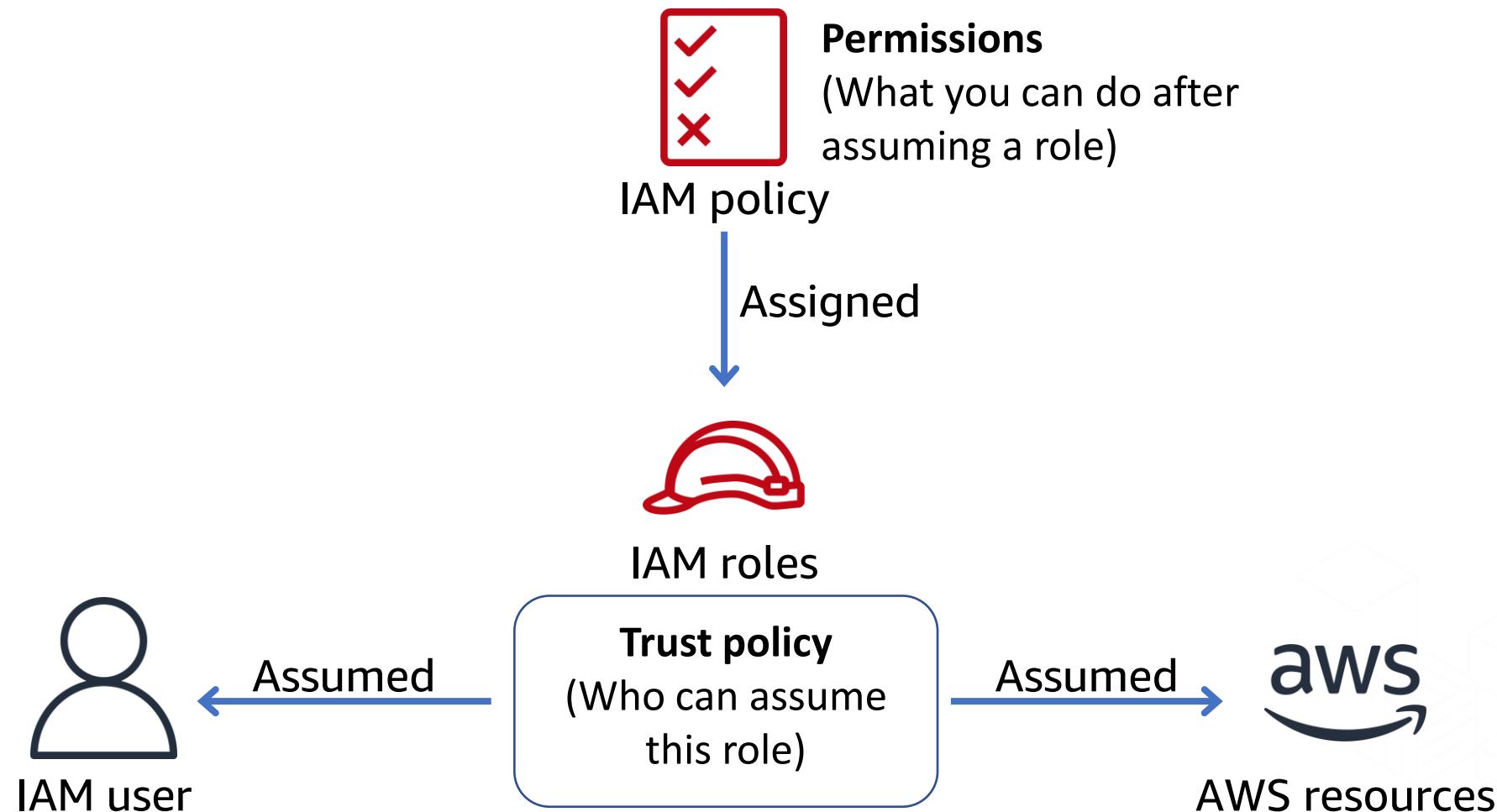
- Mjölnir - can only be lifted by Thor. It trusts Thor to lift it.



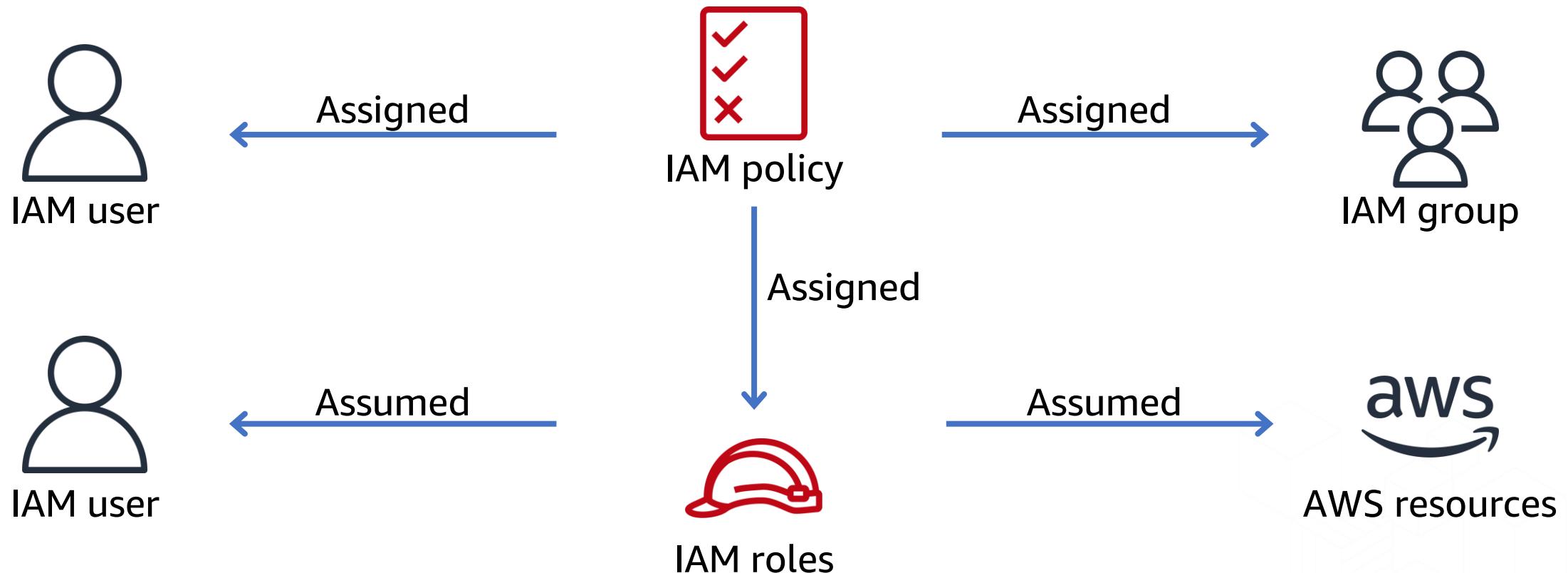
Mjölnir trusts Thor



IAM Role – Trust Policy



IAM Role



Facts to remember

- Roles can be assumed within AWS account or across AWS accounts.
- At a time only one role can be assumed.
- Trusted Entities to assume a role can be external (SAML / Web Identity).
- Behind the scene AWS Security Token Service (STS) generates a set of temporary security credentials that you can use to access AWS resources.

Try Web Identity Federation Playground - 

Service Summary Cards (SSC)

Reference:

[FAQs](#)

Category:

Security,
Identity, and
Compliance



AWS Identity and
Access Management
(IAM)

Complete book:

[Click Here](#)

More SSCs:

[Click Here](#)

Created by:

[Ashish Prajapati](#)



What?

- AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS Services. With IAM, you can specify who can access which services and resources, and under which conditions.
- With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

Why?

- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

When?

- You want to grant different fine-grained permissions to different people for different resources.
- You want to add two-factor authentication to your account and to individual users for extra security.
- You need to use existing corporate identities to grant secure access to AWS resources using identity federation.

Where?

- IAM is a global service.
- You use IAM to control access to tasks that are performed using the AWS Management Console, the AWS Command Line Tools, or service API operations using the AWS SDKs.

Who?

- You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.
- You can create multiple IAM users under your AWS account or enable temporary access through identity federation.

How?

- With IAM, you define who can access what by specifying fine-grained permissions. IAM then enforces those permissions for every request. Access is denied by default and access is granted only when permissions specify an “Allow”.
- You can delegate access to users or AWS services to operate within your AWS account.

How
much?

- There is no charge to use IAM.



Become a Solutions Architect

A day in the life of an Amazonian



Abhijeet Patwardhan
Global Engagement Manager



**Thank you for attending.
See you next Saturday (15-July-2023)**



Become a Solutions Architect

For content check **Resources Link** on BeSA Home Page

