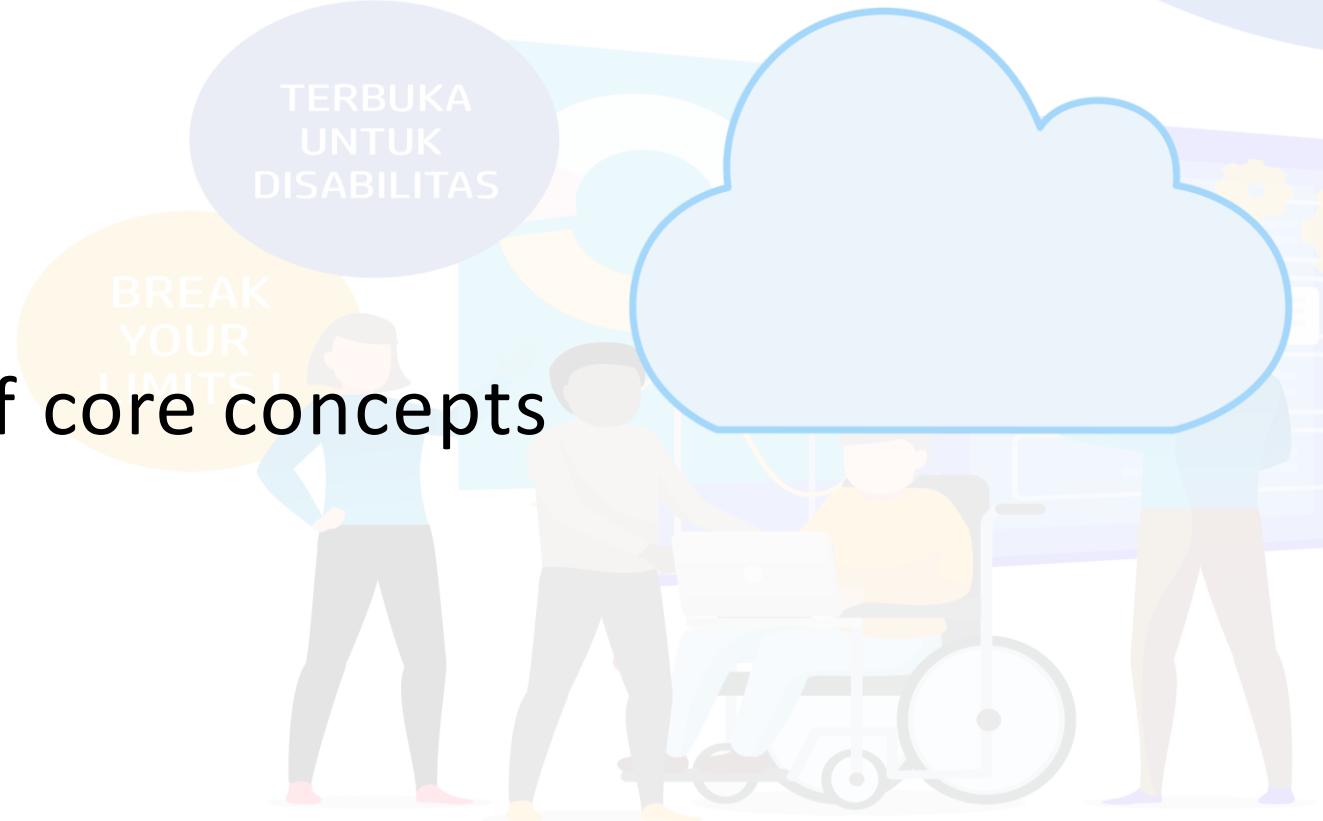


AWS Cloud Practitioner Training Materials

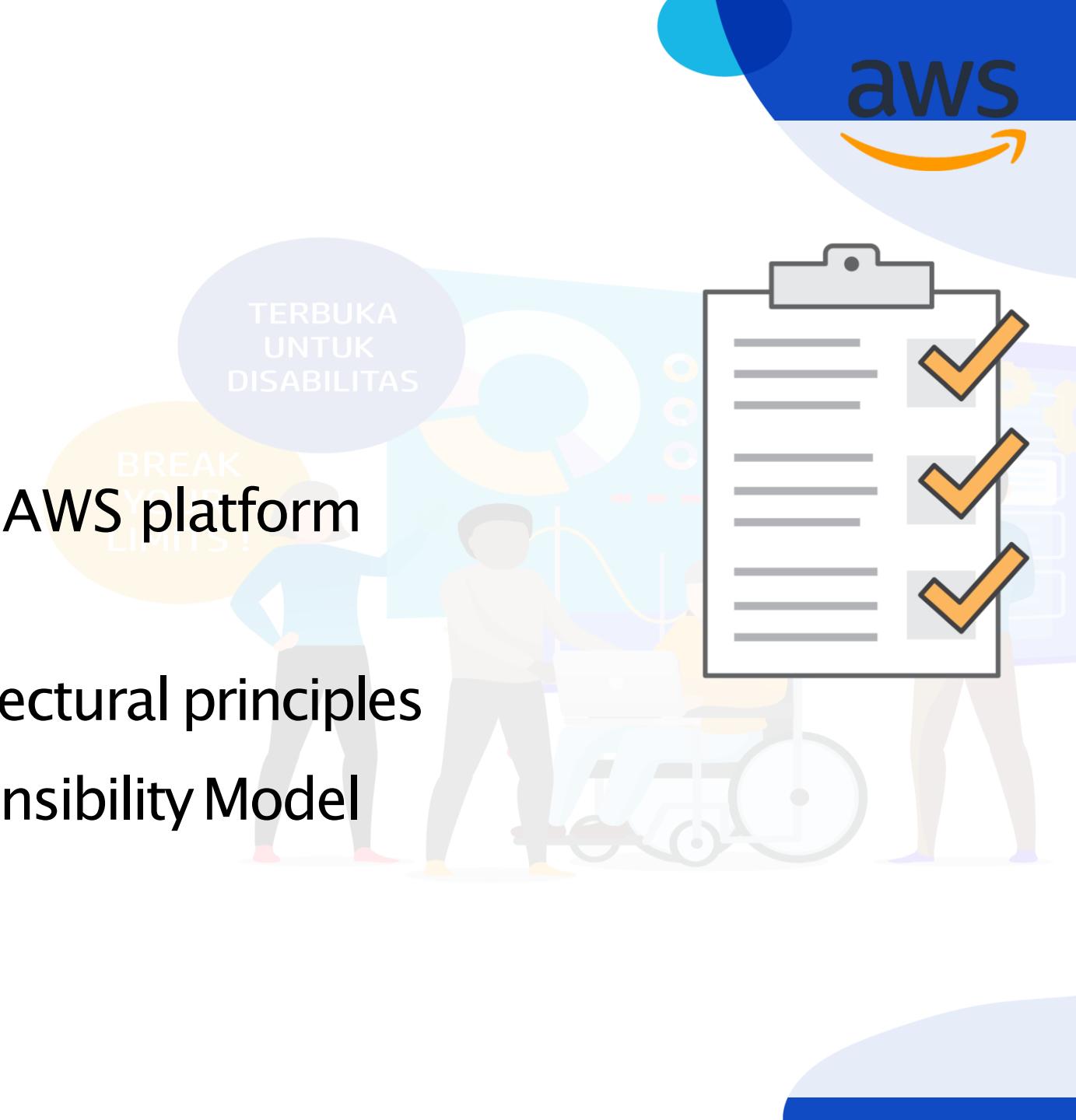
Introduction

- The AWS Cloud
- Detailed overview of core concepts



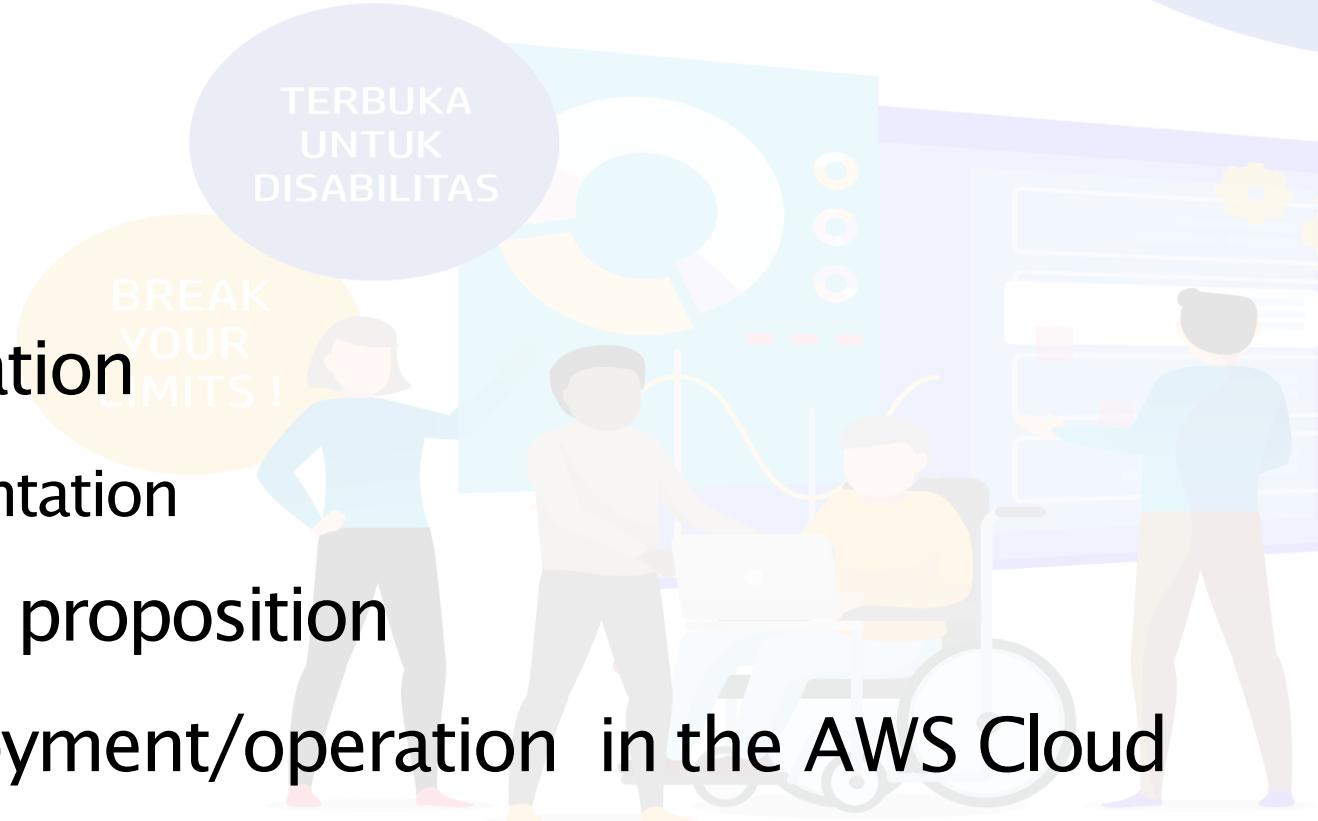
Course Objectives

- Define the AWS Cloud
- Describe the key services on the AWS platform
 - Common use cases
- Describe basic AWS Cloud architectural principles
- Describe the AWS Shared Responsibility Model
 - Basic security and compliance



Course Objectives Cont'd.

- Define pricing models
- Identify sources of documentation
 - ▶ Whitepapers and AWS Documentation
- Describe the AWS Cloud value proposition
- Define characteristics of deployment/operation in the AWS Cloud



Course Outline

- Course Overview
- Module 1: AWS Cloud Concepts
- Module 2: AWS Core Services
- Module 3: AWS Security
- Module 4: AWS Architecting
- Module 5: AWS Pricing
- Course Summary

TERBUKA
UNTUK
DISABILITAS

Module 1

Introduction to:

Cloud

The AWS cloud



Module 2

AWS Core Services

■ Overview of Services and Categories

■ Introduction to:

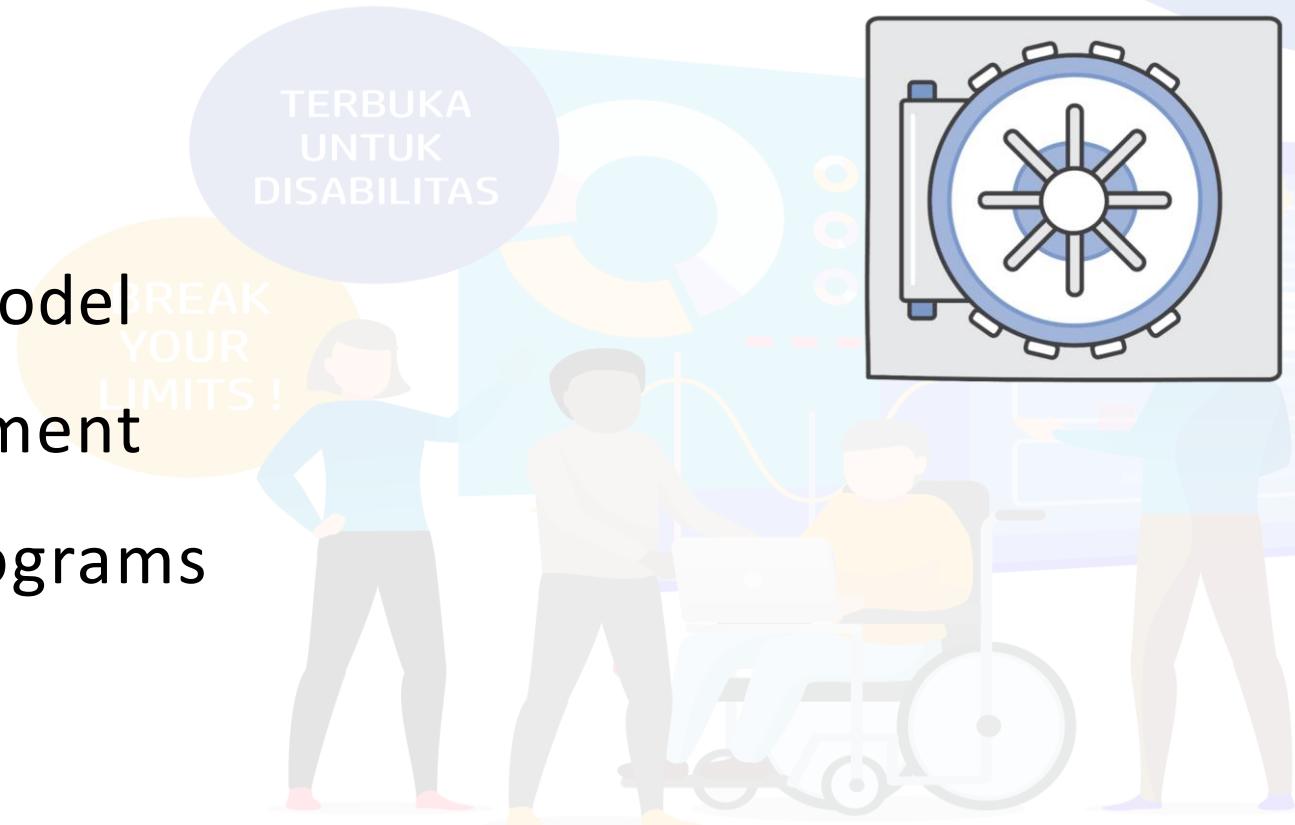
- ▶ The AWS Global Infrastructure
- ▶ Amazon VPC
- ▶ Security Groups
- ▶ Amazon EC2
- ▶ Amazon Elastic Block Store
- ▶ Amazon S3
- ▶ AWS Database Solutions



3

AWS Security

- Introduction to AWS Security
- The AWS Shared Responsibility Model
- AWS Access Control and Management
- AWS Security and Compliance Programs
- AWS Security Resources



4

AWS Architecting

■ Introduction to the AWS Well-Architected Framework

■ Reference Architecture

■ Fault Tolerance and High Availability

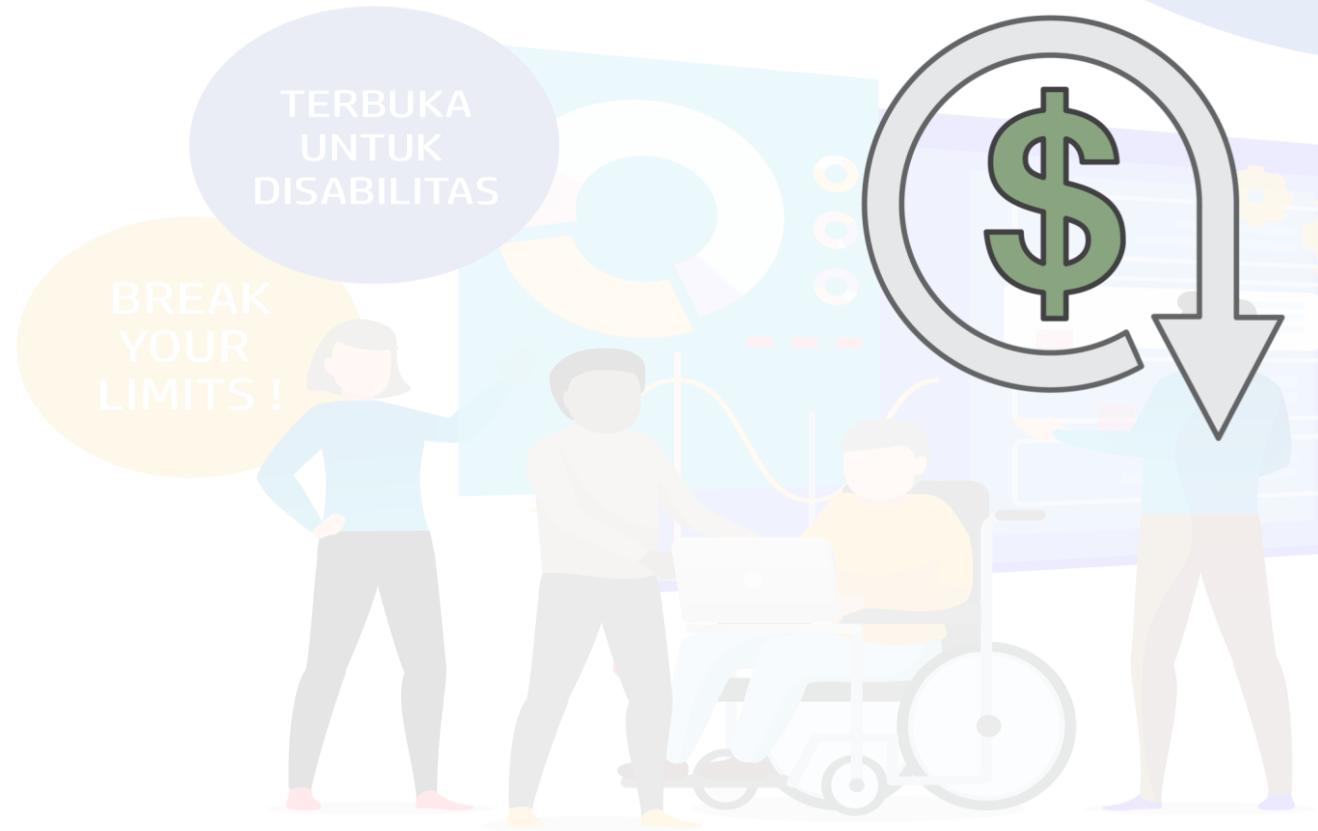
■ Web Hosting



Module 5

AWS Pricing and Support

- Fundamentals of AWS Pricing
- Pricing Details for
 - ▶ Amazon EC2
 - ▶ Amazon S3
 - ▶ Amazon EBS
 - ▶ Amazon RDS
 - ▶ Amazon CloudFront
- The TCO Calculator Overview
- AWS Support Plans Overview



Module 1: Cloud Concepts Overview



LOGO
UNIV/POITEK
KOMINFO

DIGITAL
TALENT
SCHOLARSHIP

Introduction to the AWS Cloud



Cloud Computing

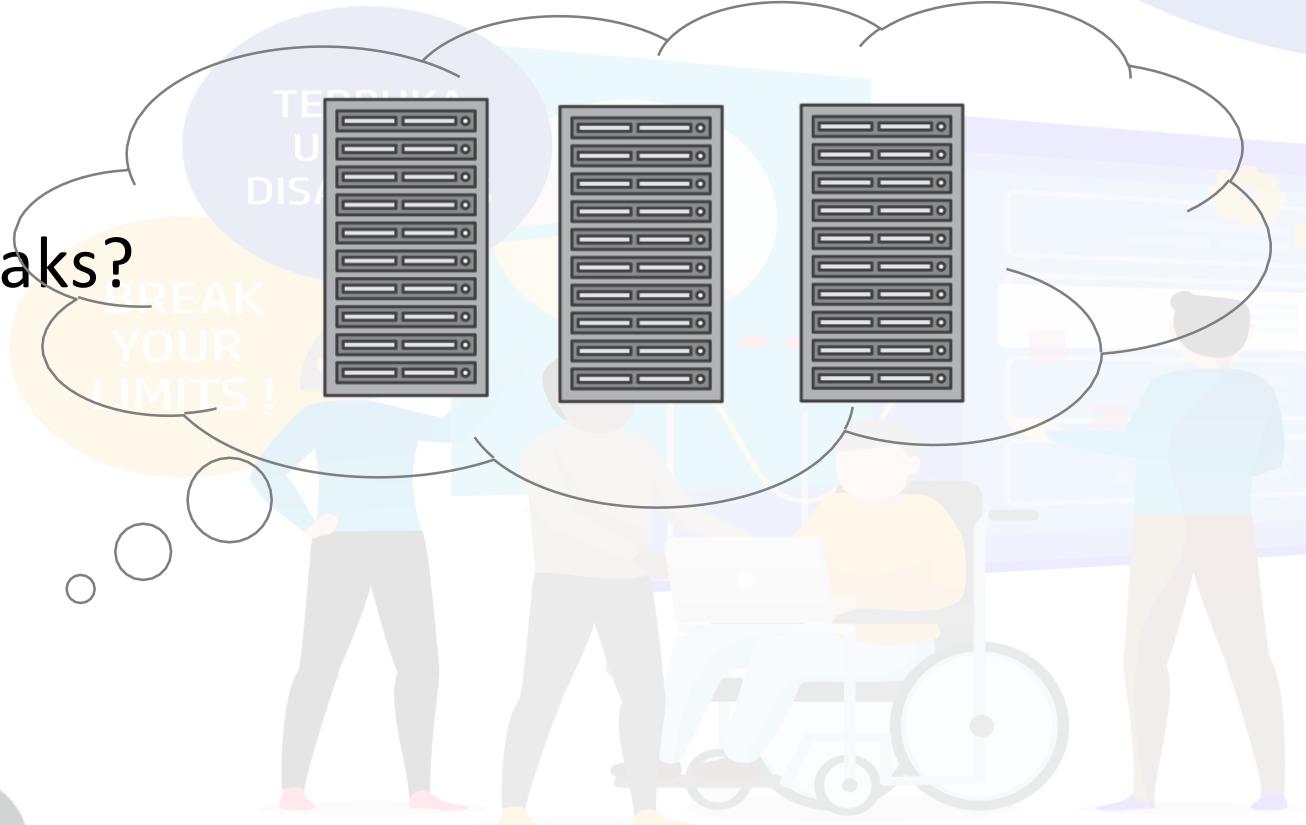
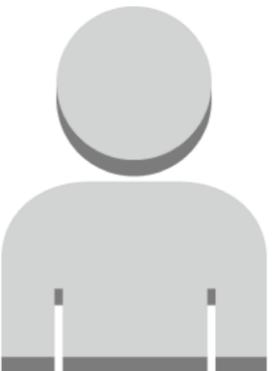
- On-demand delivery of IT resources and applications via the internet with pay-as-you-go pricing

Before AWS

■ Guessing theoretical maximum peaks?

▶ Is there enough resource capacity?

▶ Is this sufficient storage?



With AWS

- With AWS:
 - Servers
 - Databases
 - Storage
 - Higher-level applications



With AWS

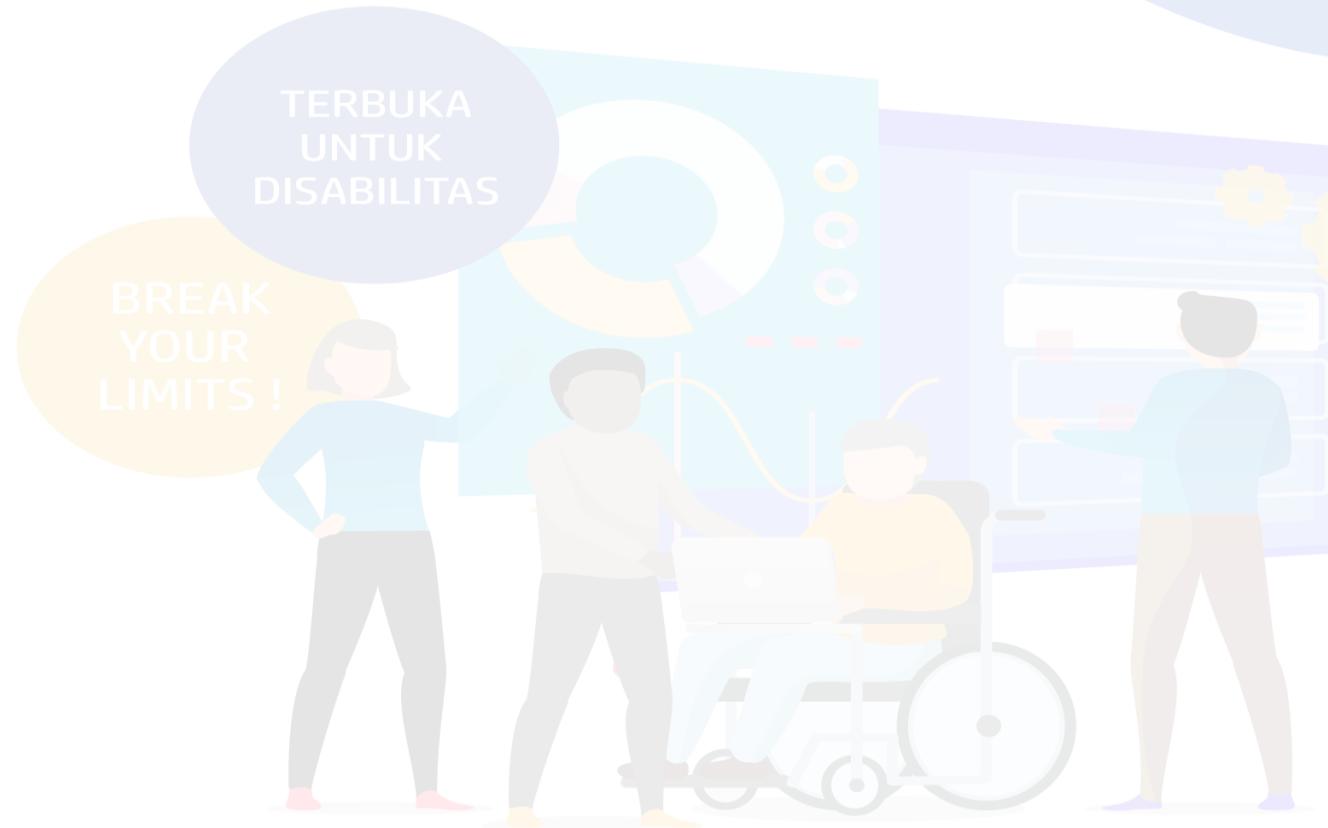
- Resources can be:
 - ▶ Initiated within seconds
 - ▶ Treated as “temporary and disposable”
- Free from the inflexibility and constraints



Agility

3 factors:

- ─ Speed
- ─ Experimentation
- ─ Culture of innovation



Agility: Increase Speed and Global Reach

- Instant global reach
- Rapid availability of new resources



Agility: Increase Experimentation

- AWS enables
 - ▶ Operations as code
 - ▶ Safe Experimentation
 - ▶ Comparative testing



Agility: Increase Innovation

- Quick experimentation with low cost/risk
- More experimentation and more often

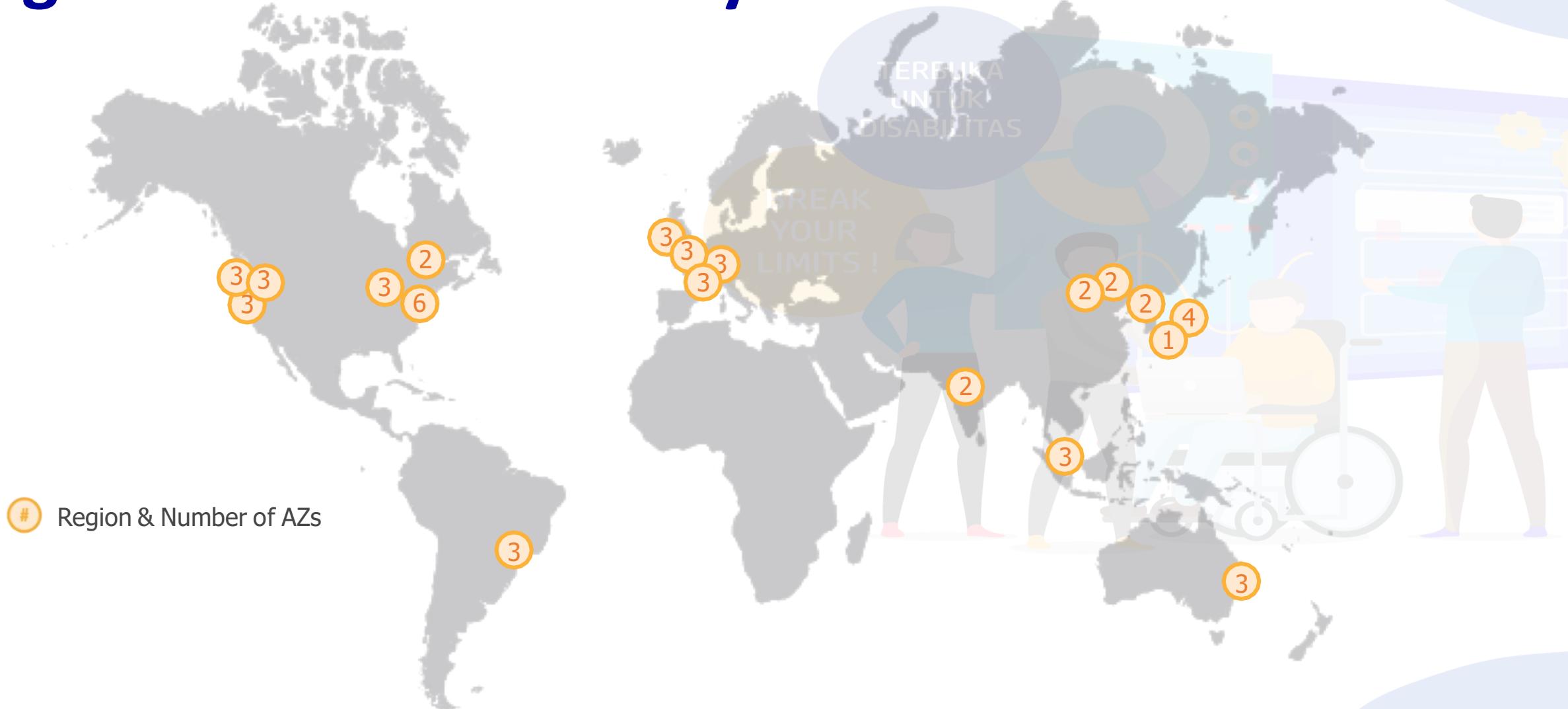


Agility: The AWS Infrastructure

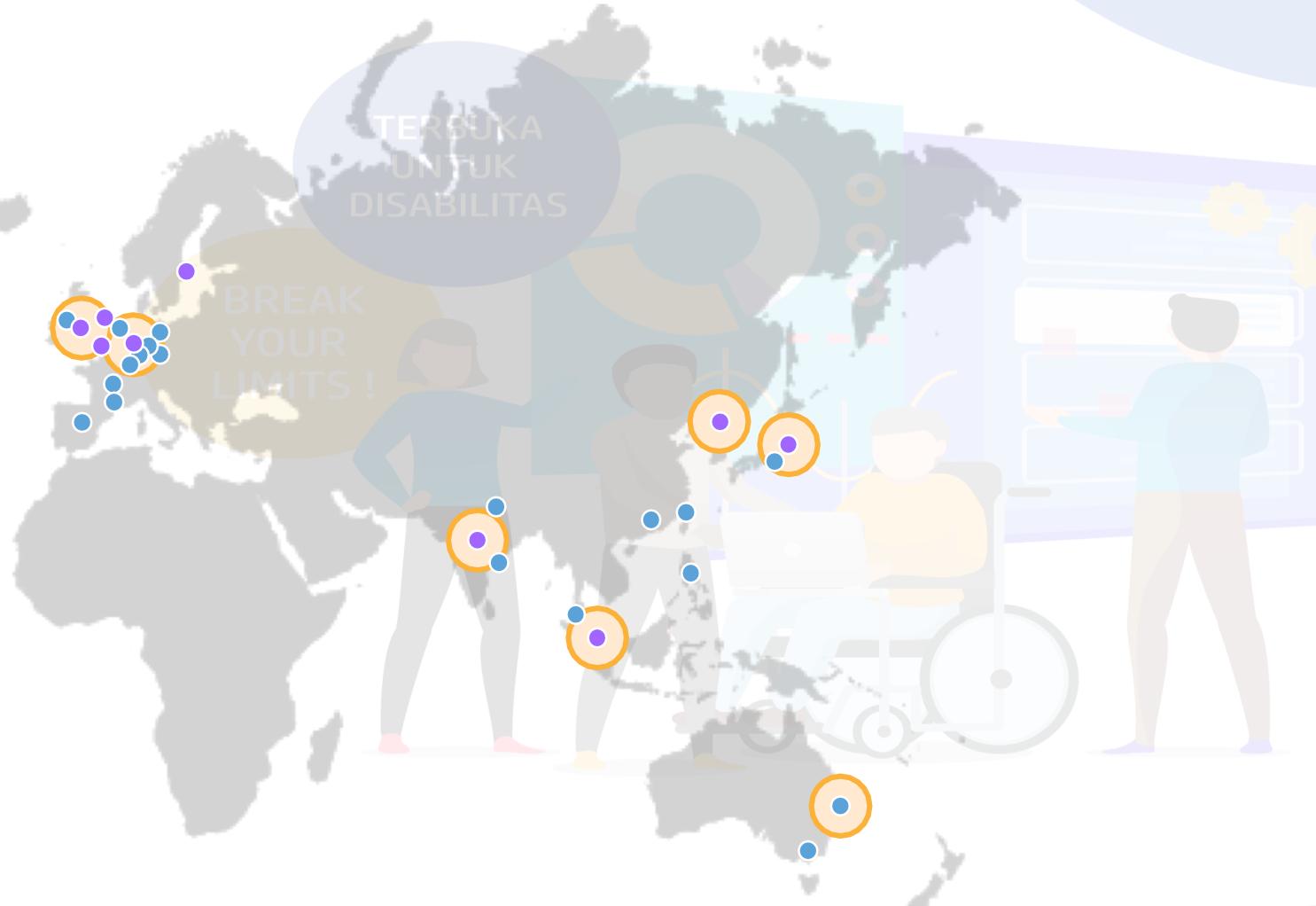
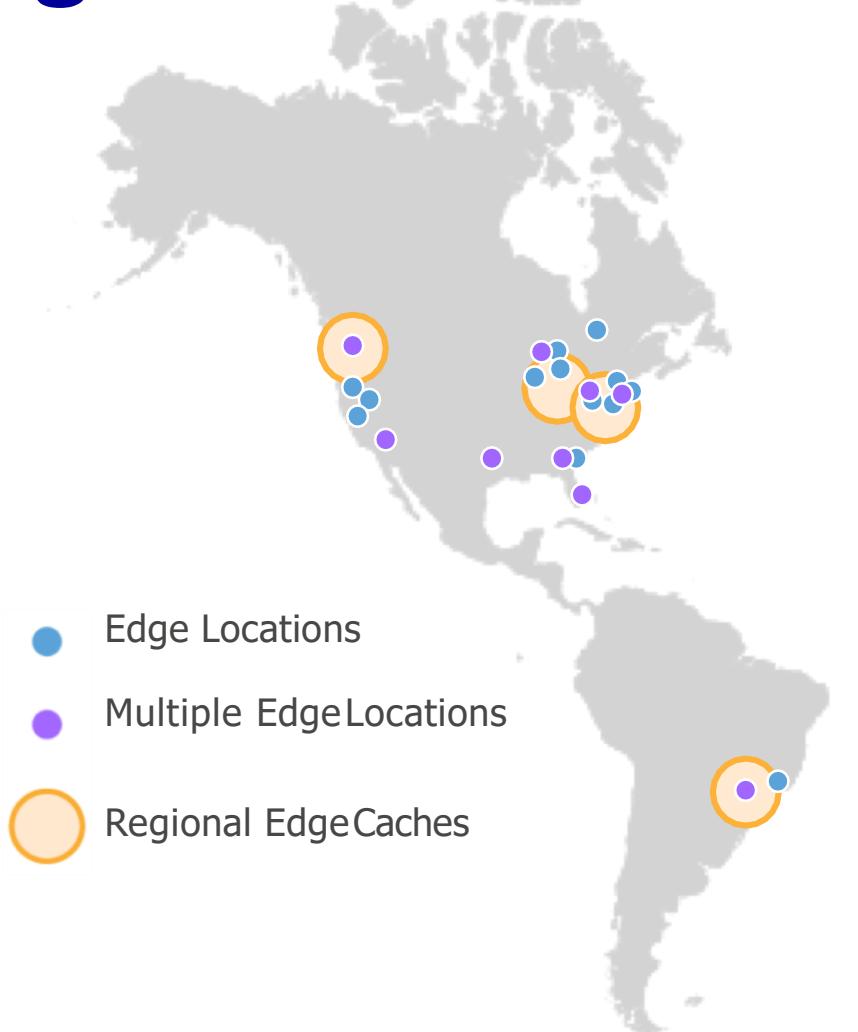
- Instant elasticity
- Scalability
- Flexible
- Reliability
- Secure



Regions and Availability Zones



Edge Locations



High Availability

- High availability:
 - ▶ Functional and accessible systems
 - ▶ Minimized downtime
 - ▶ No human intervention



Fault Tolerance

■ Fault Tolerance:

- ▶ Operational applications during component failure
- ▶ Built-in redundancy of components



Elasticity, Scalability, and High Performance

AWS

- Elastic infrastructure
- Innovative new services/products
- Deployment in multiple regions
 - Lower latency
 - Better customer experience



Elasticity, Scalability, and High Performance

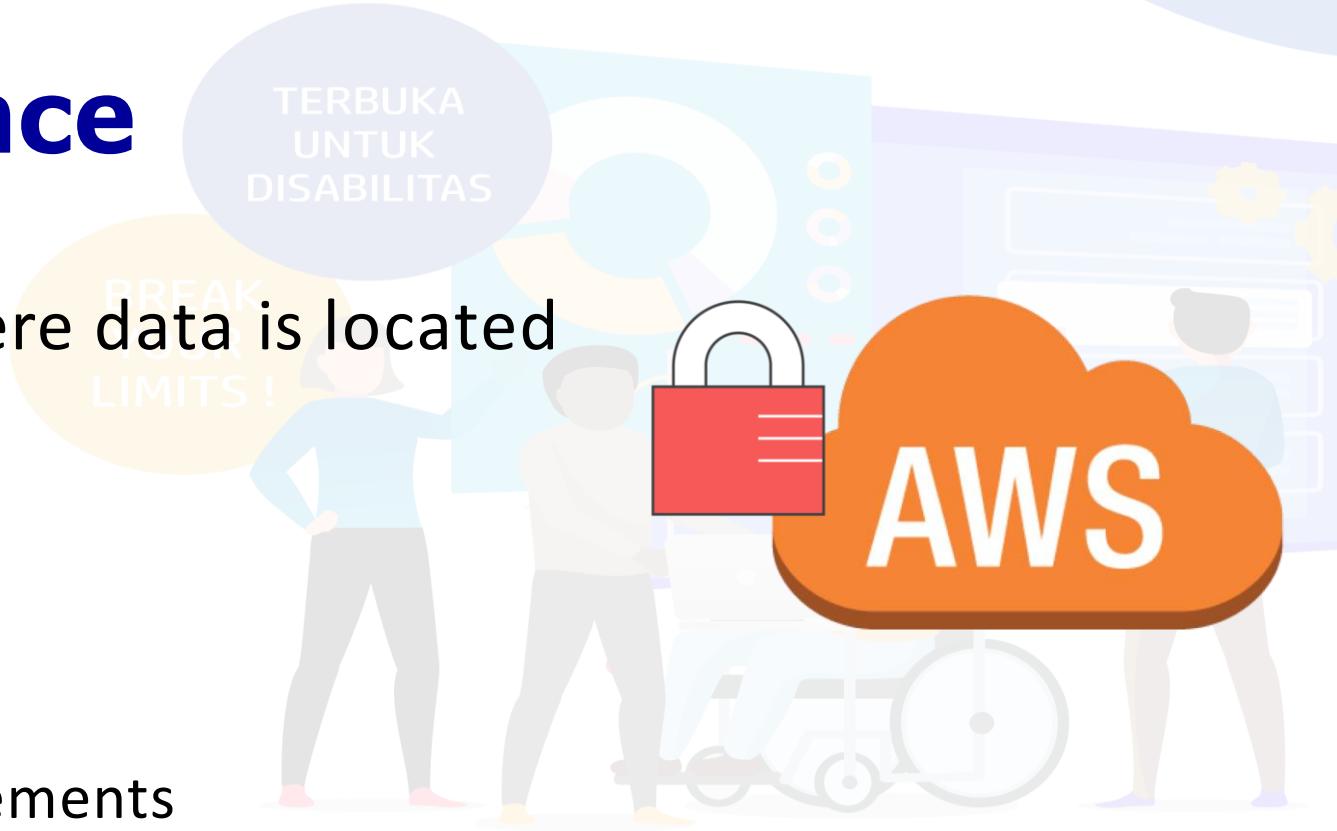
Customer

- Use services at your own pace
- Use tools to meet your needs
- Adapt your consumption
 - ▶ Scale up as workload grows
 - ▶ Shutdown unneeded resources
 - ▶ Use Auto Scaling

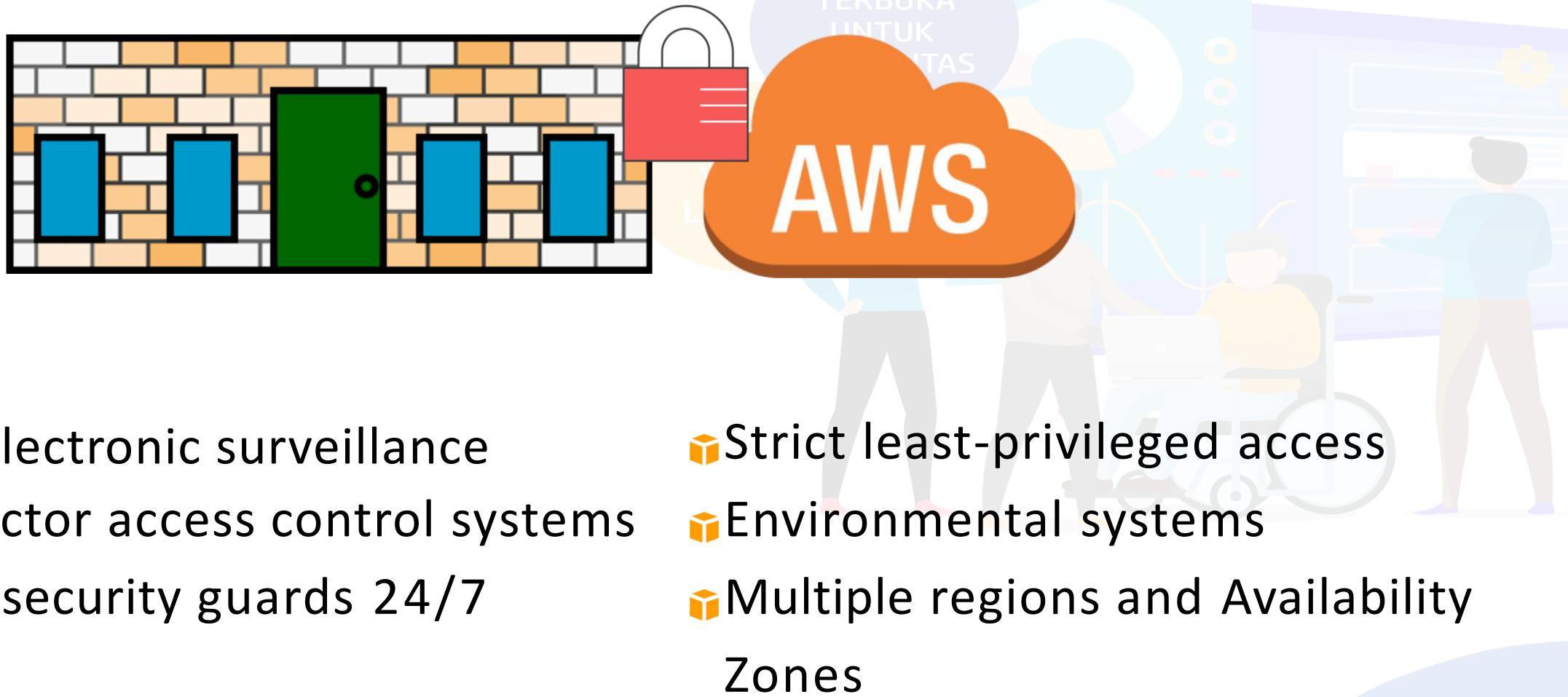


Security and Compliance

- You retain control over region where data is located
- Security auditing
 - Periodic and manual
- AWS cloud offer capabilities
 - For governance
 - To meet the strictest security requirements

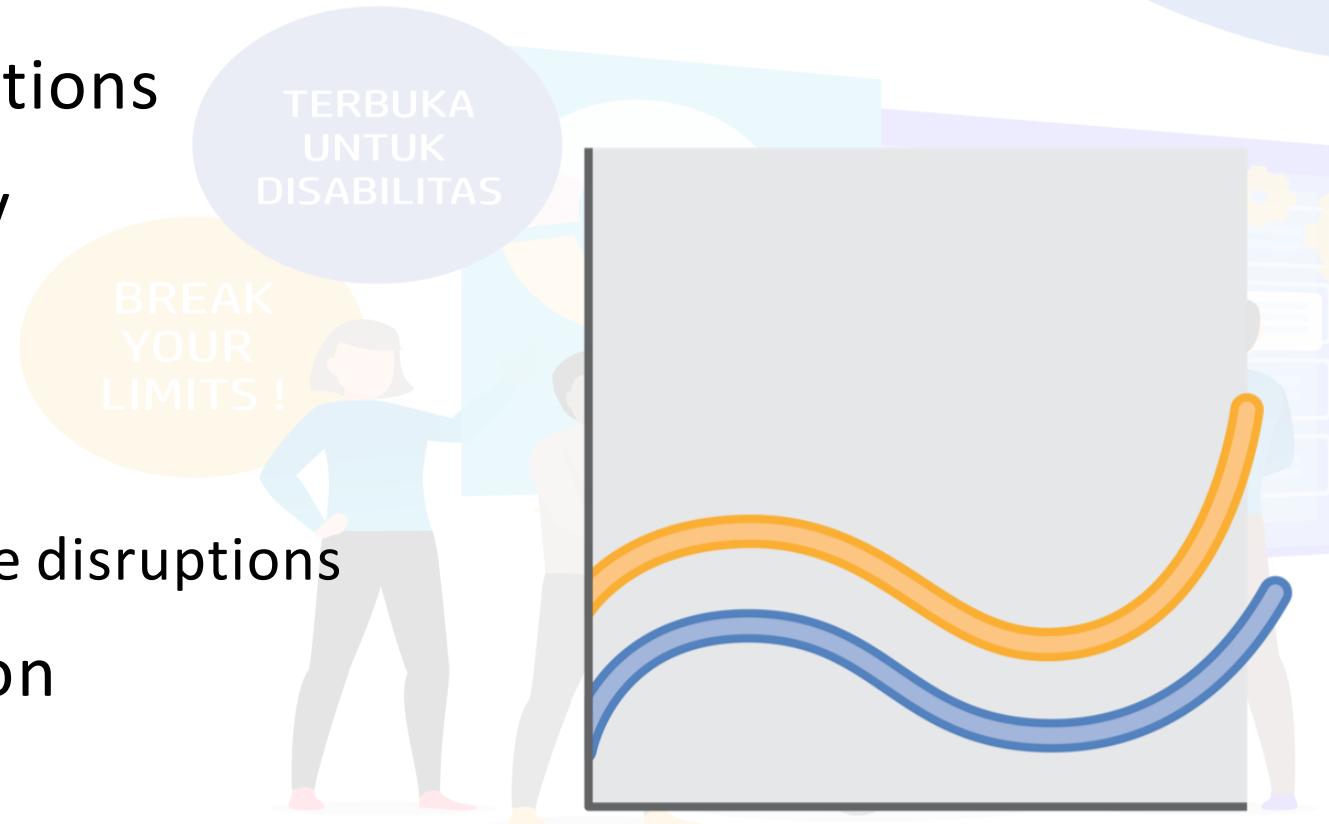


Security and Compliance



Reliability

- High-performing and reliable solutions
- Achieve greater flexibility/capacity
- Reliability:
 - ▶ Recover from failures
 - ▶ Resources that demand and mitigate disruptions
- Must have well-planned foundation
 - ▶ Reduce uncertainty of forecasting
 - ▶ Detect failure and automatically heal itself
- Unmatched by on-premise solutions



Pricing: Pay as you go

Benefits

- ▶ Redirect focus to innovation and invention
- ▶ Adapt to changing business needs
- ▶ Improve responsiveness to changes
- ▶ Reduce risk or overprovisioning or missing capacity



Conclusion

- Connect with customers
- Develop ground-breaking new insights
- Scientific breakthroughs
- Deliver innovative new products and services

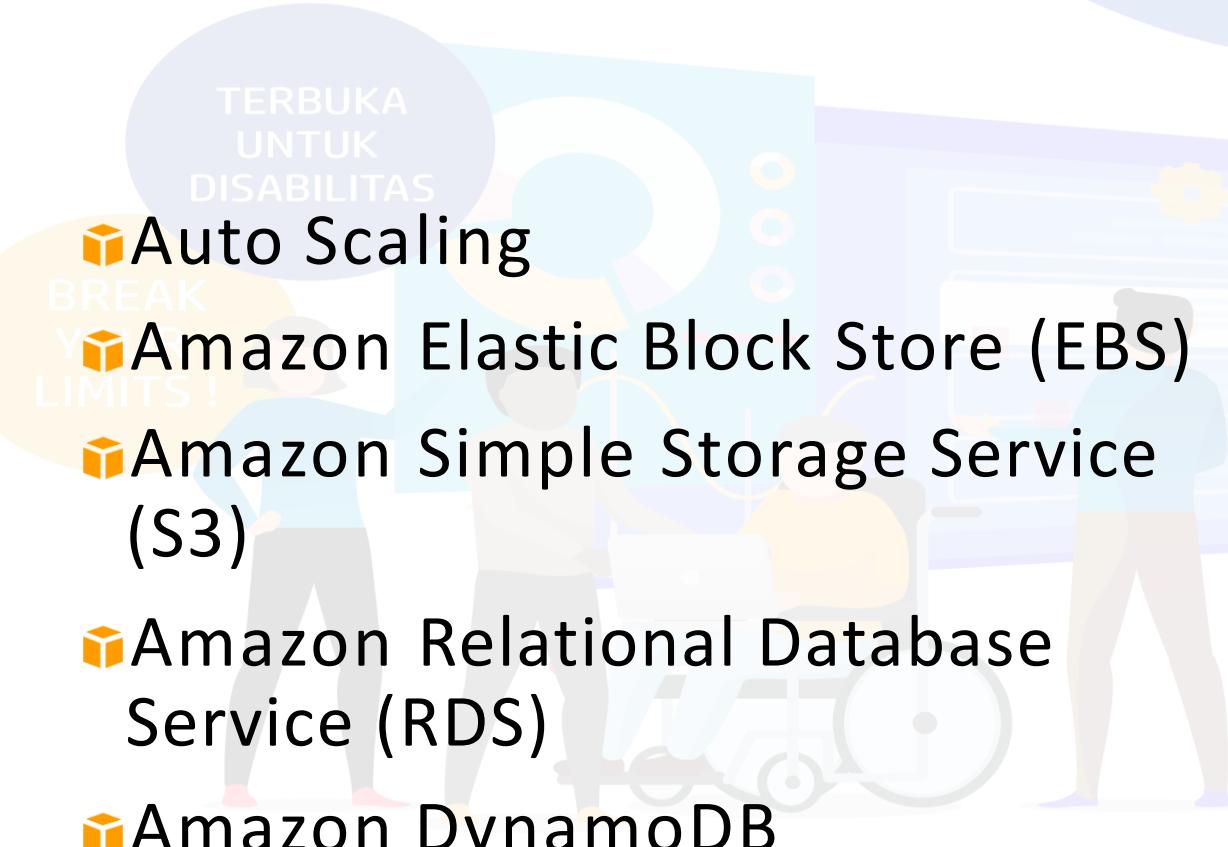




Module 2: AWS Technology Overview

Topics

- AWS Global Infrastructure
- Amazon Virtual Private Cloud (VPC)
- Security groups
- Compute Services
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)



AWS Global Infrastructure



TERBUKA
UNTUK
DISABILITAS

BREAK
THE
LIMITS!

Introduction to Services and Categories



Compute



Storage



Database



Migration



Networking & Content
Delivery



Developer Tools



Management Tools



Media Services



Security, Identity &
Compliance



Analytics



Machine Learning



Mobile Services



AR & VR



Application Integration



Customer Engagement



Business Productivity



Desktop & App Streaming



Internet of Things



Game Development

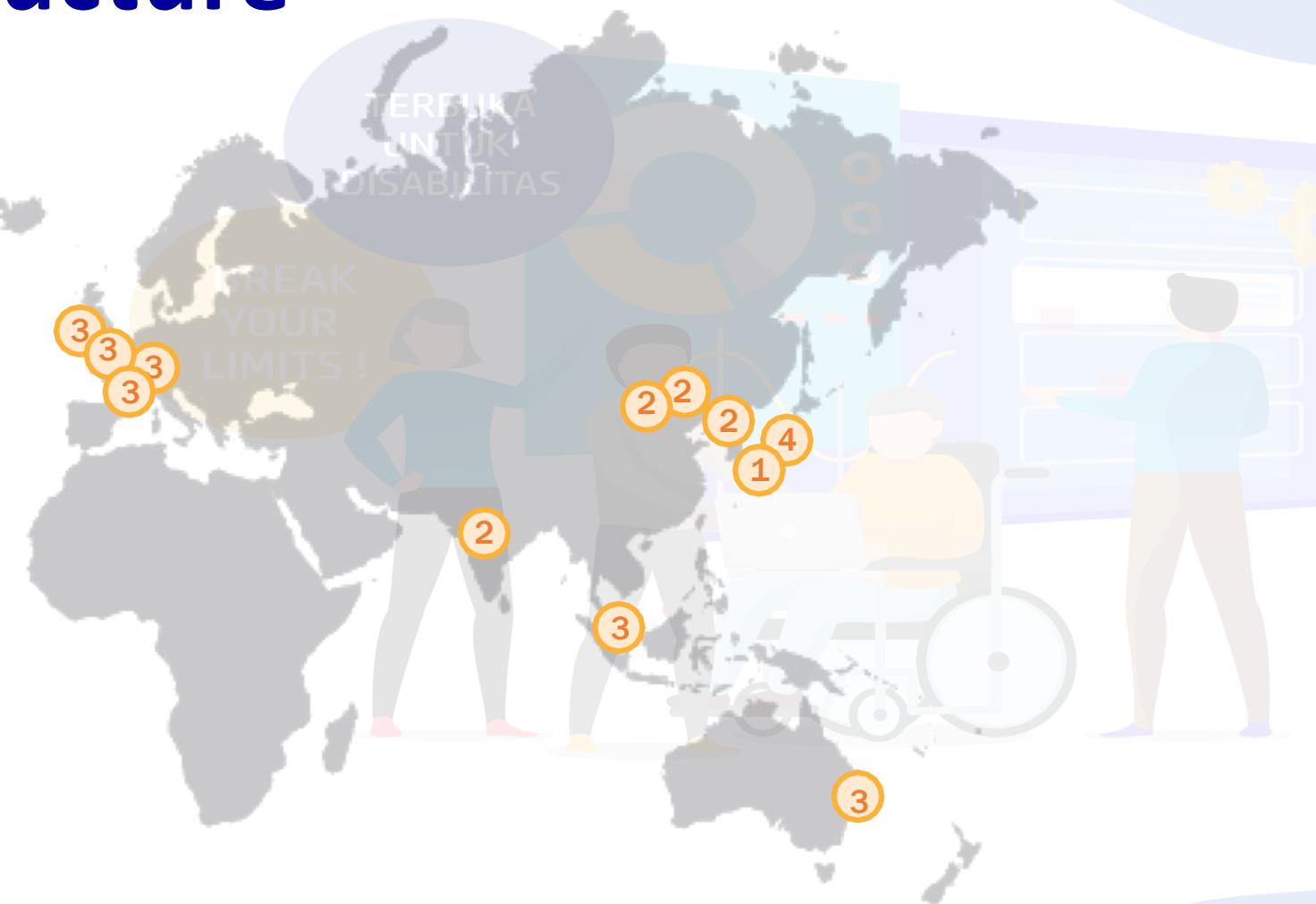
AWS Global Infrastructure



Regions

Availability Zones

Edge Locations

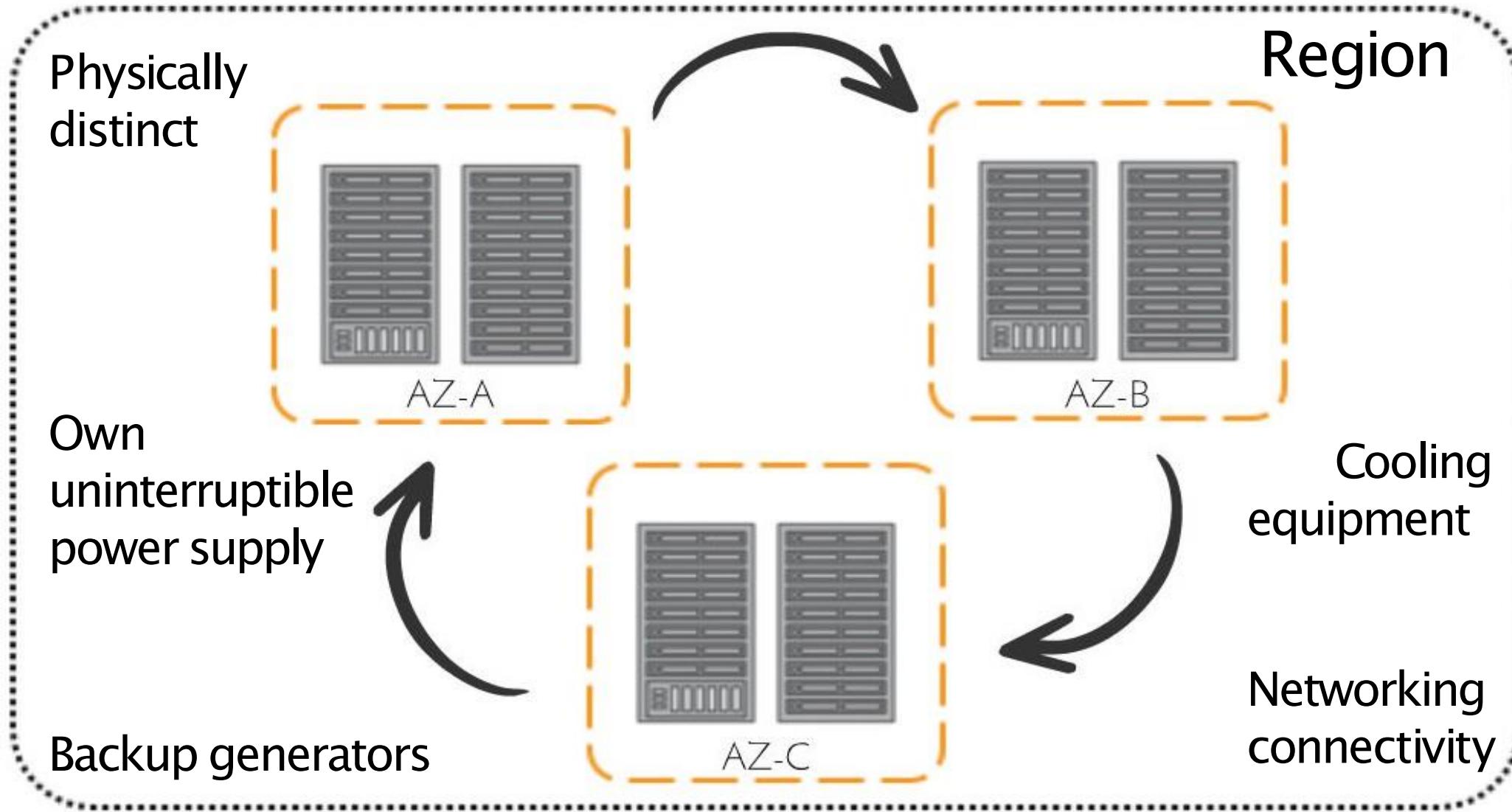


AWS Region Table

Last updated: December 20, 2017

Americas	Europe / Middle East / Africa	Asia Pacific					
Services Offered:		Northern	Ohio	Oregon	Northern	Montreal	São
		Virginia			California		Paulo GovCloud
Alexa for Business		✓					
Amazon API Gateway		✓	✓	✓	✓	✓	✓
Amazon AppStream		✓					
Amazon AppStream 2.0		✓		✓			
Amazon Athena		✓	✓	✓			
Amazon Aurora - MySQL-compatible		✓	✓	✓	✓	✓	
Amazon Aurora - PostgreSQL-compatible		✓	✓	✓		✓	
Amazon Chime		✓					
Amazon Cloud Directory		✓	✓	✓			

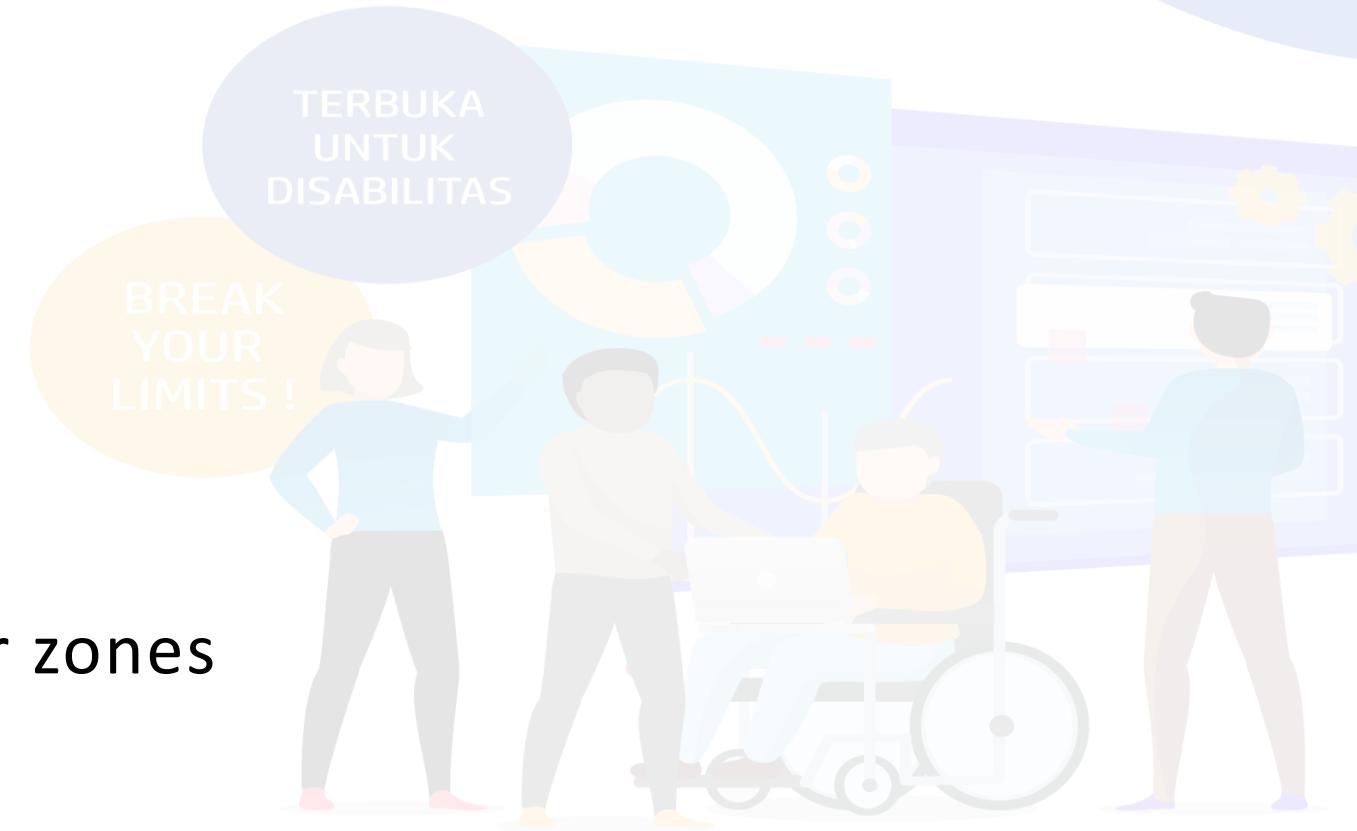
Availability Zones



Availability Zones

Isolating Availability Zones

- Protects zones from failure
- Designed for high availability
- Handles requests through other zones



Best practice: Implement multiple Availability Zones

Edge Locations

- Amazon CloudFront
- Amazon Route 53
- AWS Shield
- AWS Web Application Firewall
- Lambda@Edge Computing



Amazon Virtual Private Cloud (VPC)



TERBUKA
UNTUK
DISABILITAS

BREAK
YOUR
S

Introduction

- Private, virtual network in the AWS Cloud
- Similar constructs as on-premises network
- Customizable network configurations to your needs



Deployment

- Layer security controls in deployment
- Multiple AWS services that inherit the security deployed



Introduction



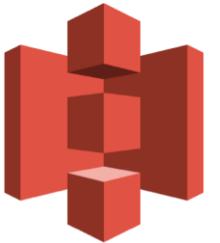
Amazon
VPC



Amazon
EC2



AWS
OpsWorks



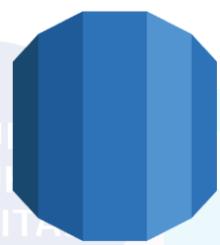
Amazon
S3



Amazon
EMR
YOUR
LIMITS!



Amazon
EFS



Amazon
RDS



AWS Elastic
Beanstalk



Amazon
DynamoDB



Amazon
WorkSpaces



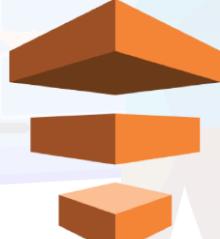
Amazon
Route 53



Amazon
ElastiCache



Elastic
Load
Balancing



AWS
Data
Pipeline

Features

Characteristics

- P Allows you to provision virtual networks

Logically isolated

Configurable key features

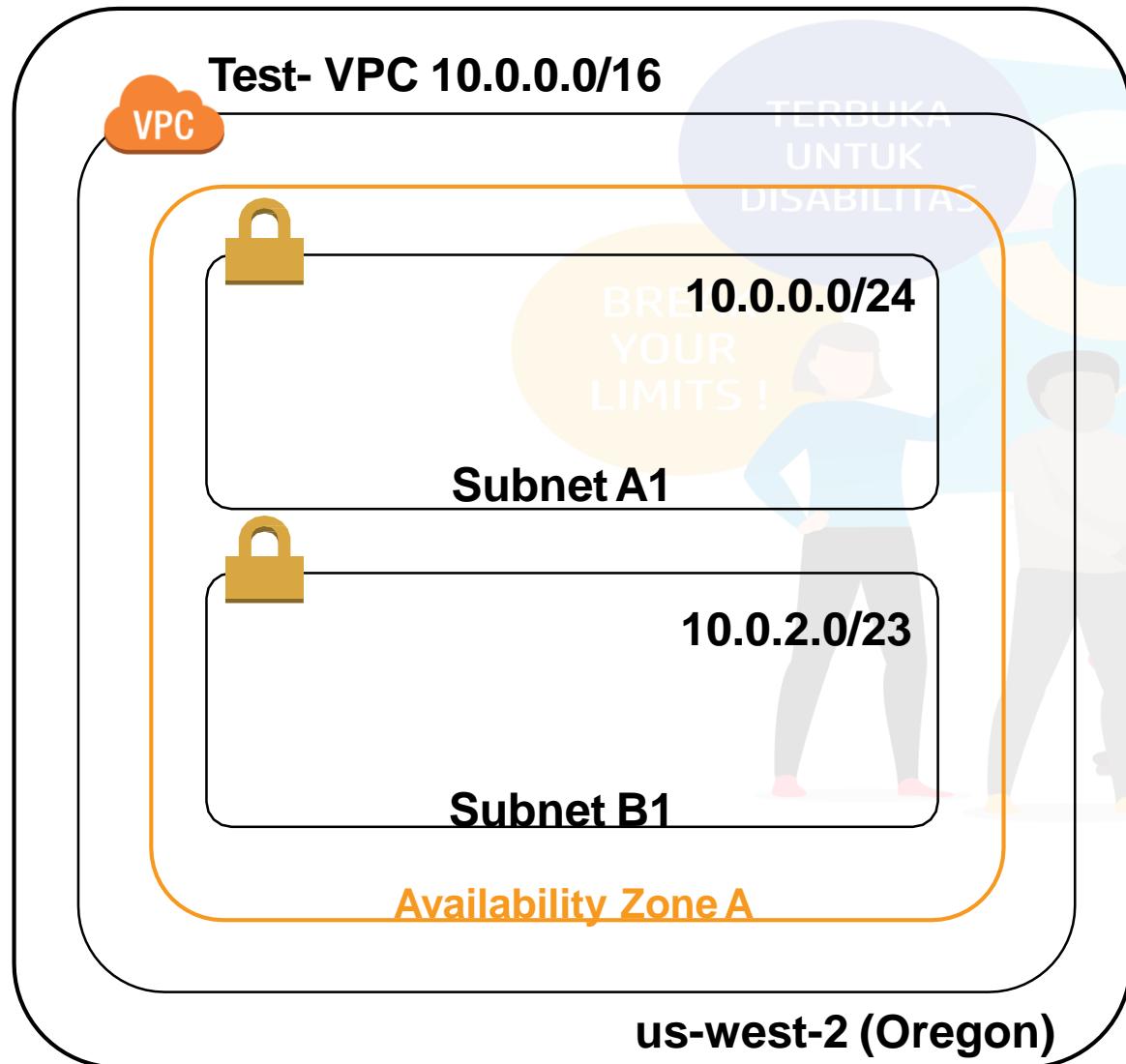
- P IP ranges
- P Routing
- P Network gateways
- P Security settings

Route Tables

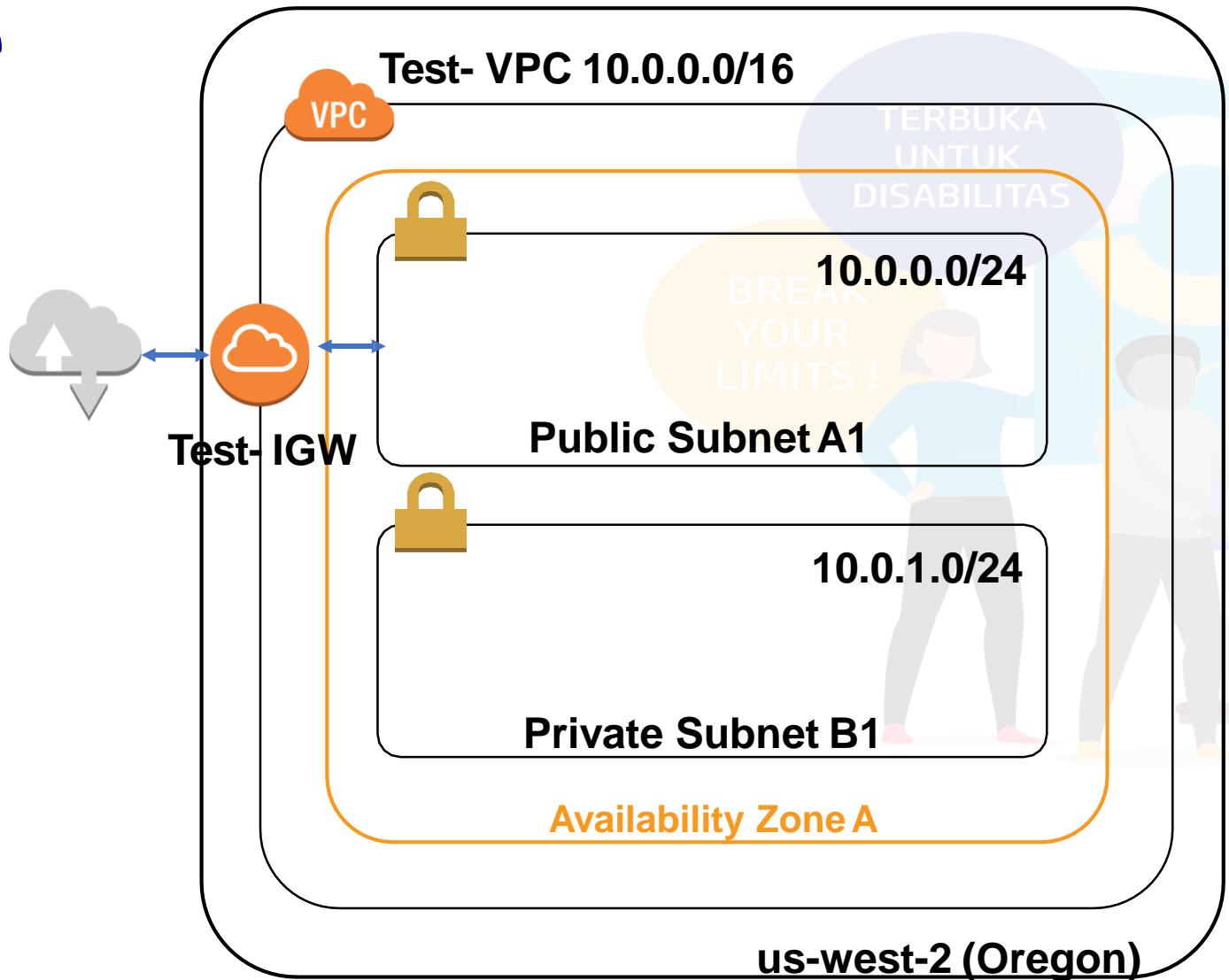
- P Control traffic going out of the subnets



Example



Example



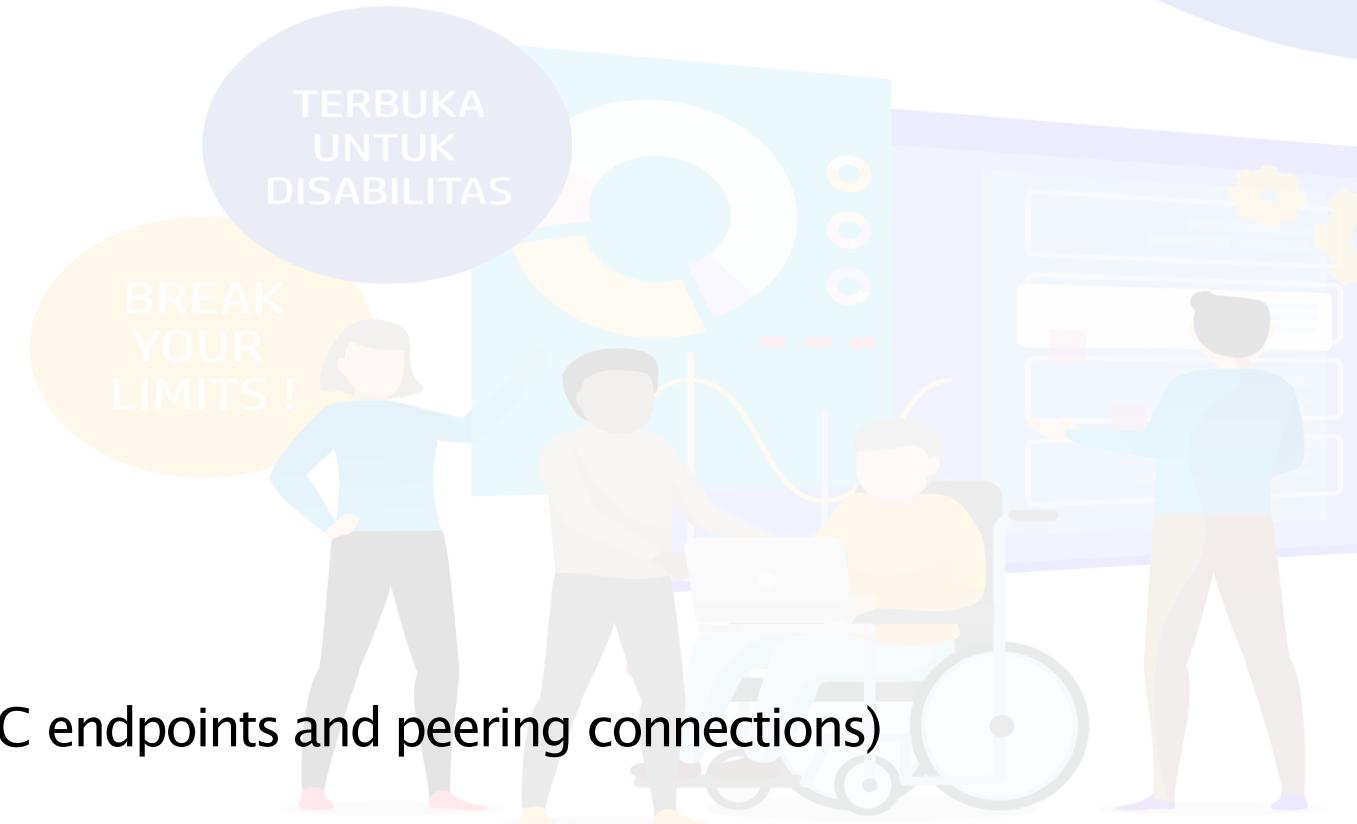
Summary

❖ You created:

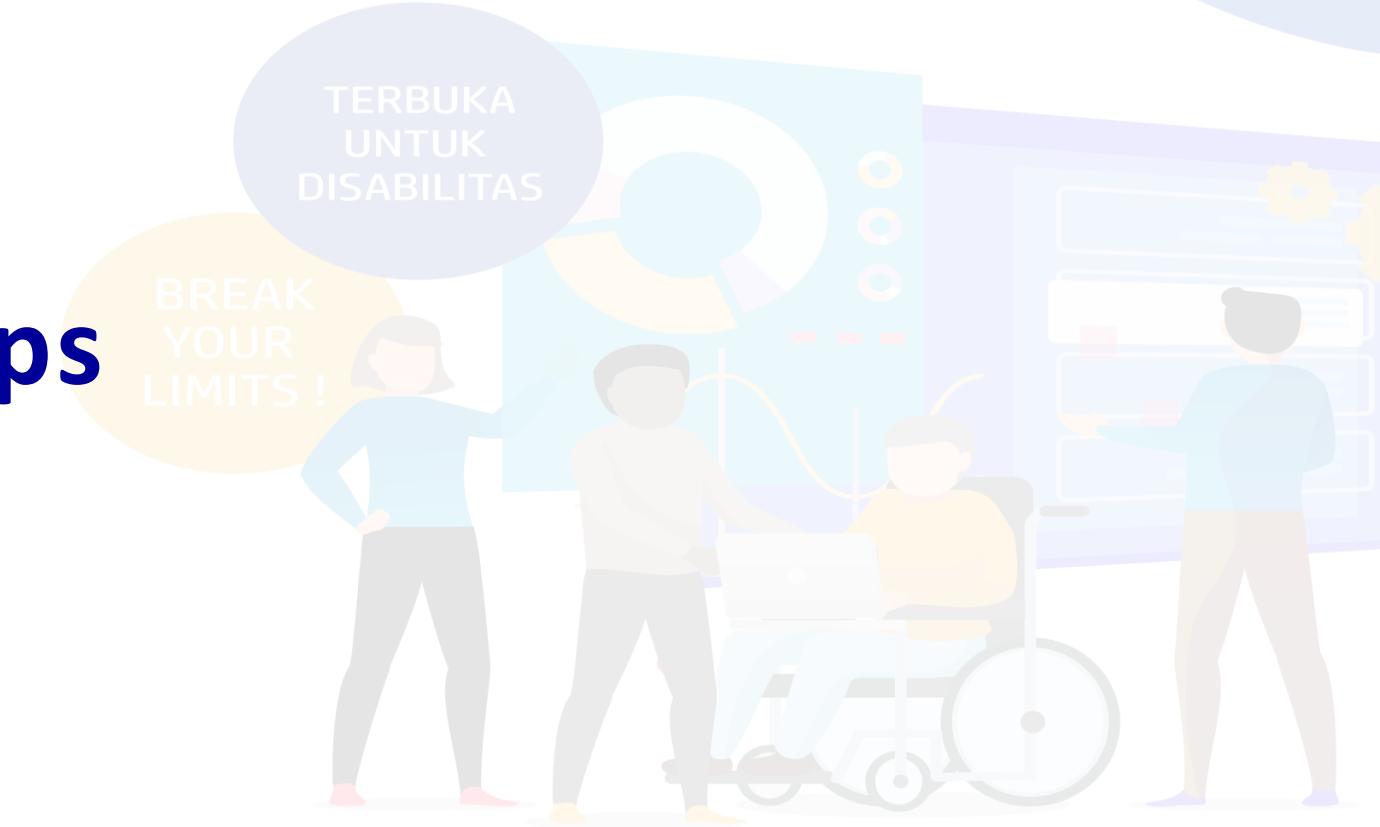
- VPC in the Oregon region
- An internet gateway
- One public subnet
- One private subnet

❖ Learn More

- Route tables and isolation methods
- Other Amazon VPC features (e.g., VPC endpoints and peering connections)
- Security groups
- Amazon Elastic Cloud Compute (EC2)
- Amazon Relational Database Service (RDS)



AWS Security Groups



AWS Security

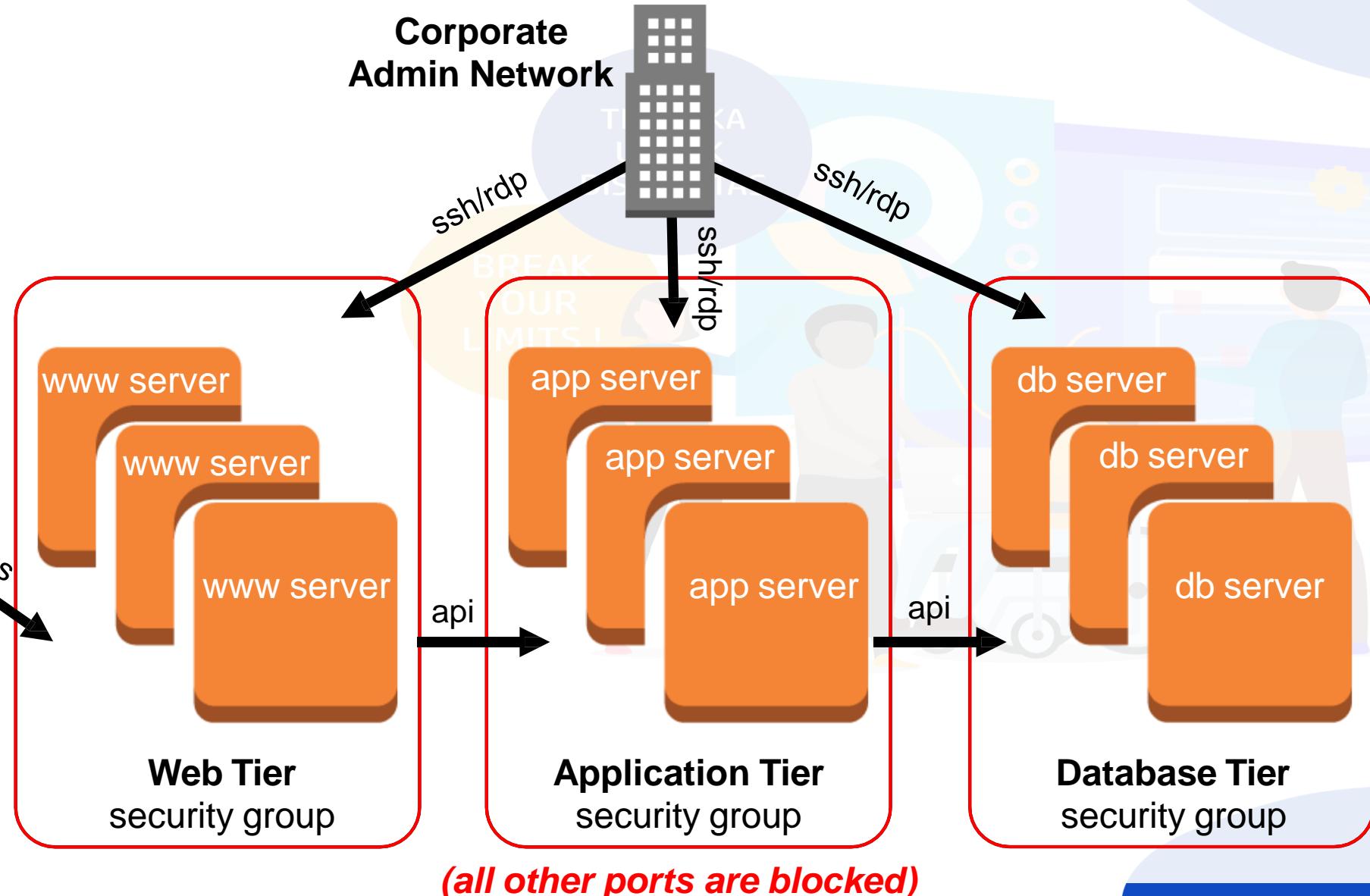
- Is the highest priorities
- Security groups
 - ▶ Act as built-in firewalls
 - ▶ Control accessibility to instances



AWS Security



internet



Summary

Amazon EC2 Security groups

- ▶ Provide virtual firewalls
- ▶ Control access to instances through rules
- ▶ Are managed through AWS management console



Compute Services



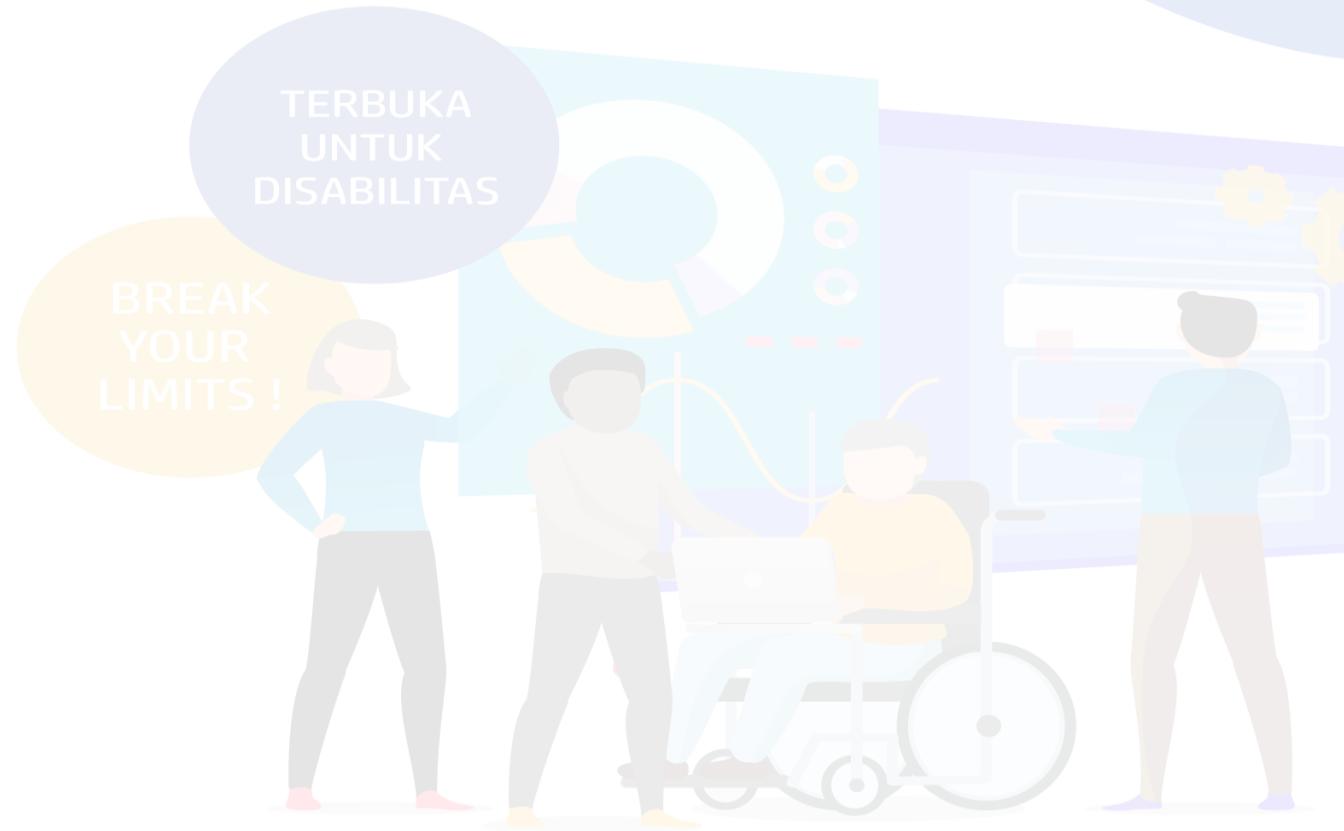
Compute Services

■ Broad catalog

■ Application services

■ Virtual private servers

■ Serverless computing



Compute Services

AWS

P Flexible

P Cost effective

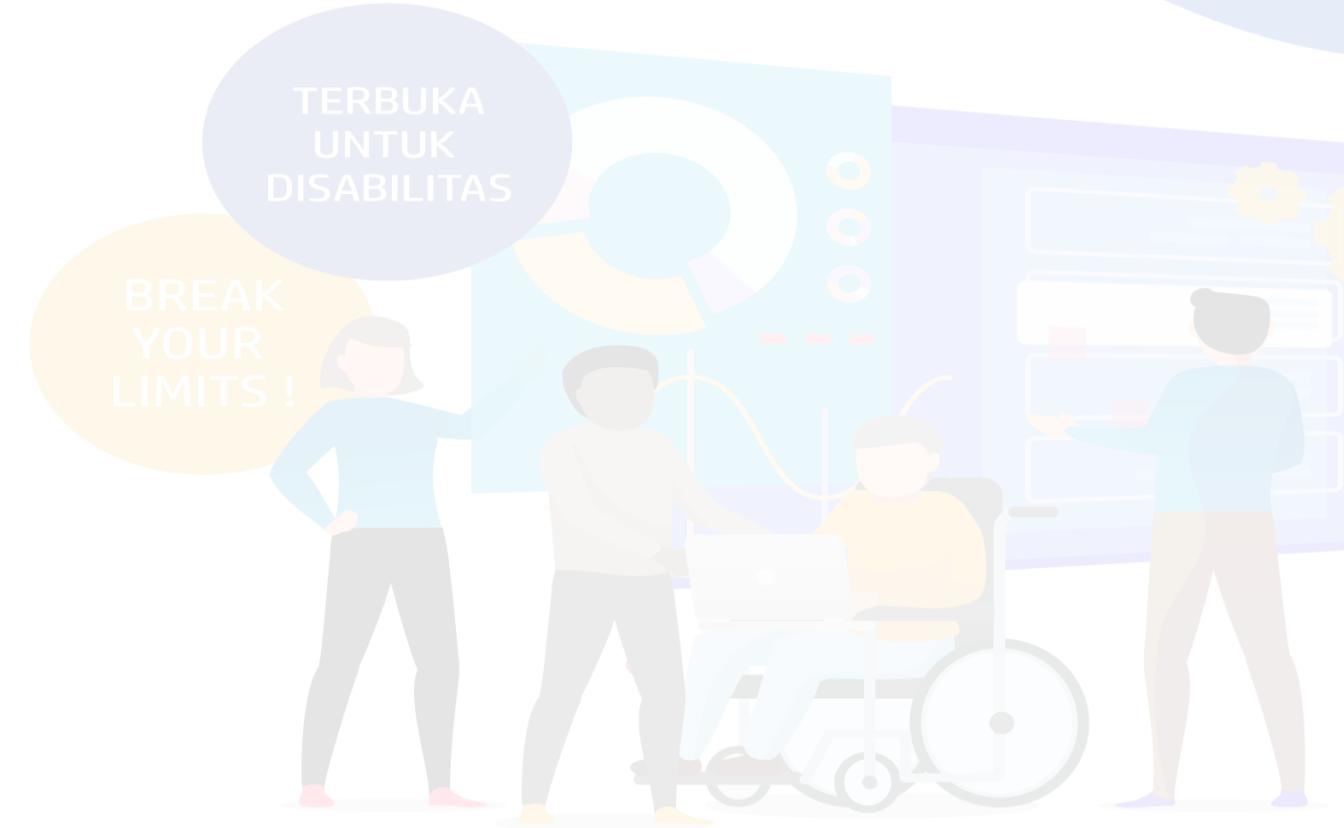
Amazon EC2

P Flexible configuration and control

AWS Lambda

P Pay only for what you use

P No administration



Compute Services

Amazon Lightsail

- ▶ Launch virtual private server
- ▶ Manage simple web and application servers

Amazon ECS

- ▶ Managed containers
- ▶ Highly scalable, high performance

AWS Fargate

Amazon EKS



Amazon Elastic Compute Cloud (EC2)



TERBUKA
UNTUK
DISABILITAS

BREAK
YOUR
LIMITS

EC2?

Elastic Compute Cloud



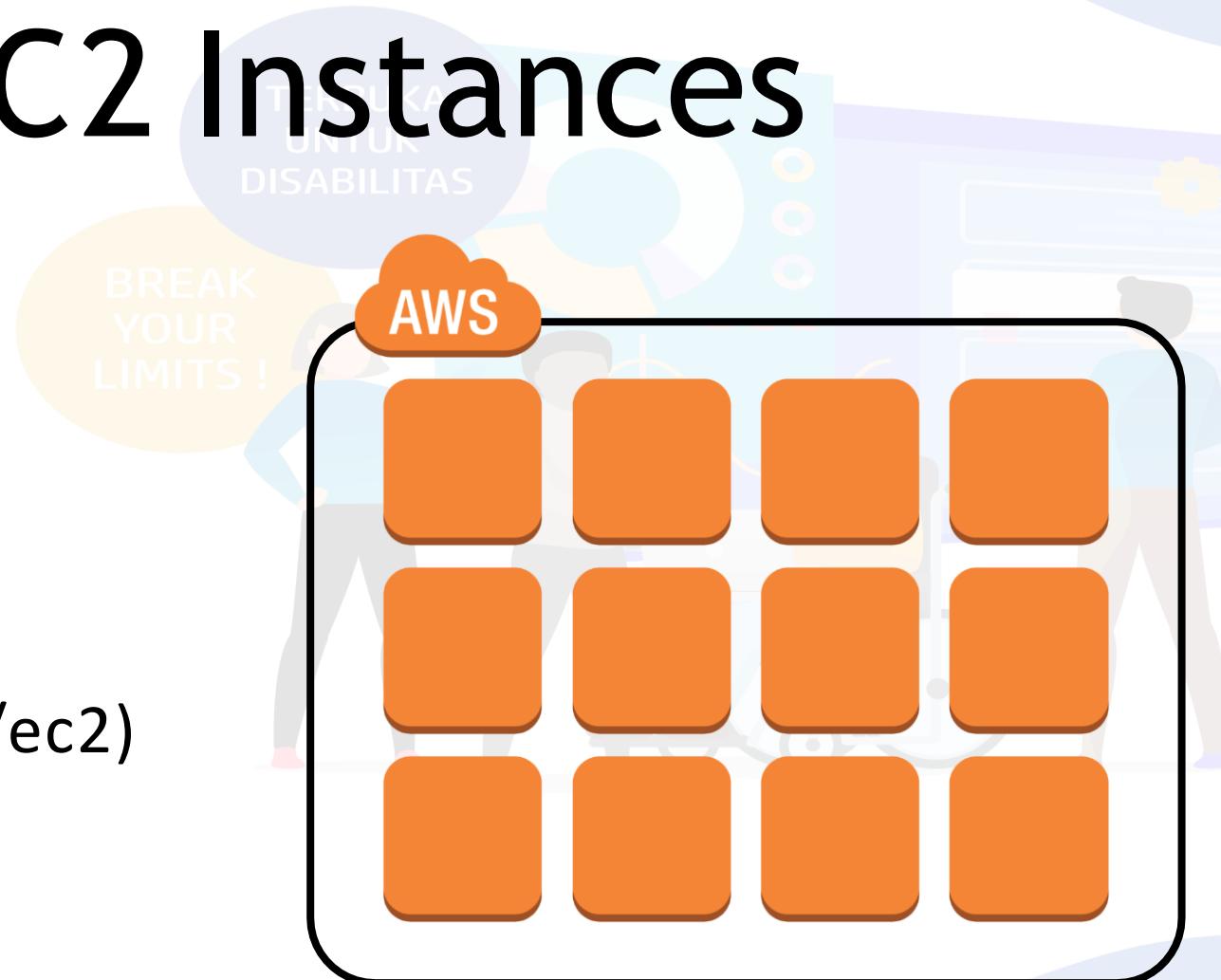
BREAK
YOUR
LIMITS

- Ü Application Server
- ü Web Server
- ü Database Server
- ü Game Server
- ü Mail Server ü
- Media Server
- ü Catalog Server
- ü File Server
- ü Computing Server
- ü Proxy Server

EC2?

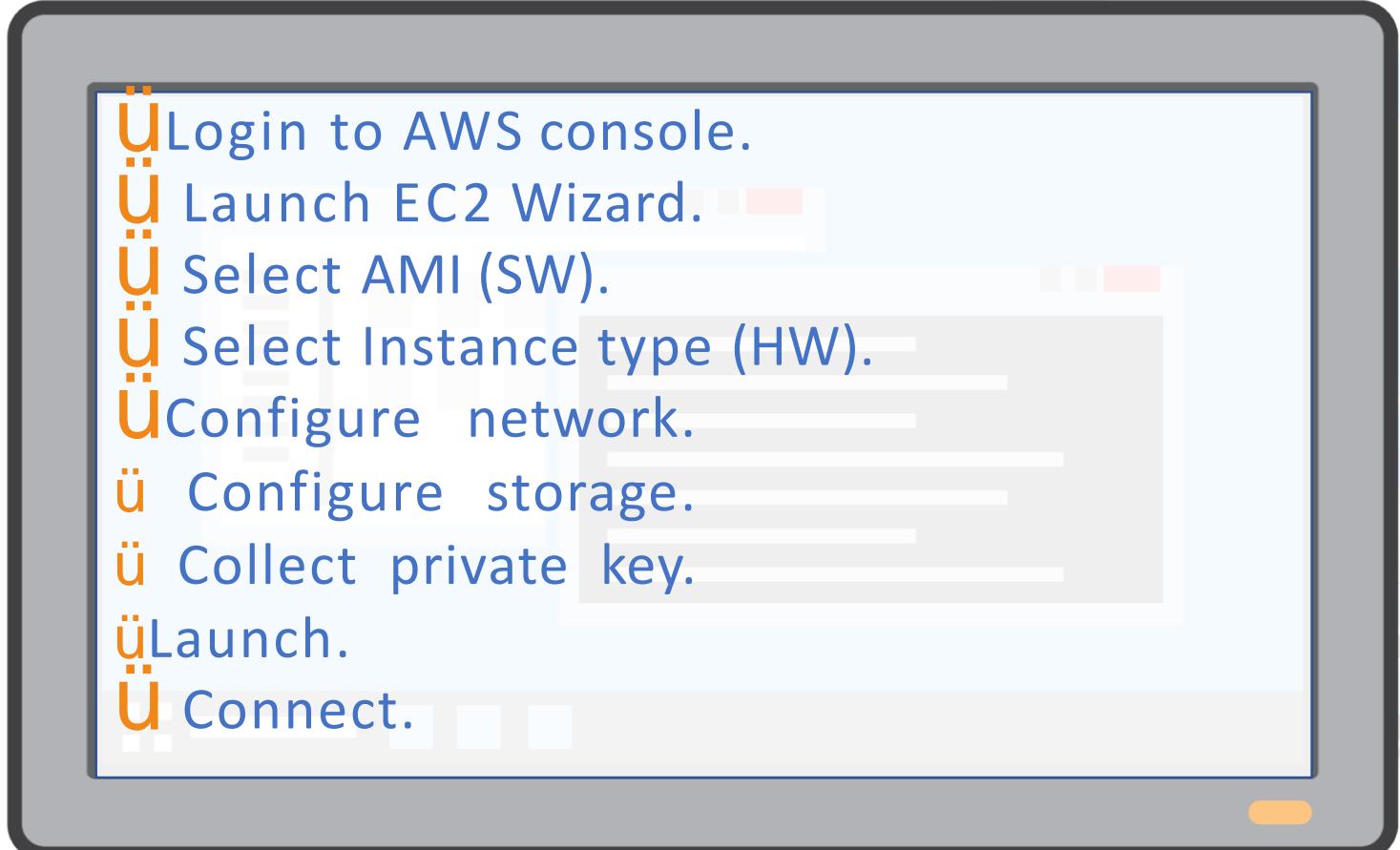
Amazon EC2 Instances

- cube Pay as you go
- cube Broad selection of HW/SW
- cube Global hosting
- cube *Much more (aws.amazon.com/ec2)*



Demonstration

- Ü Login to AWS console.
- Ü Launch EC2 Wizard.
- Ü Select AMI (SW).
- Ü Select Instance type (HW).
- Ü Configure network.
- Ü Configure storage.
- Ü Collect private key.
- Ü Launch.
- Ü Connect.





Families	Description	Example Use Cases
t2, m4, m3	General Purpose Balanced Performance	Websites, web applications, Dev, code repos, micro services, business apps
c3, c4, cc2	Compute Optimized High CPU Performance	Front-end fleets, web-servers, batch processing, distributed analytics, science and engineering apps, ad serving, MMO gaming, video-encoding
g2, p2	GPU Optimized High-end GPU	Amazon AppStream 2.0, video encoding, machine learning, high perf databases, science
r3, r4, x1, cr1	Memory Optimized Large RAM footprint	In-memory databases, data mining
d2, i2, i3, hi1, hs1	Storage Optimized High I/O, High density	NAS, data warehousing, NoSQL

Choosing the Right Amazon EC2 Instances



- EC2 Instance types are optimized for different use cases, workloads & come in multiple sizes. This allows you to optimally scale resources to your workload requirements.
- AWS utilizes Intel® Xeon® processors for EC2 Instances providing customers with high performance and value.
- Consider the following when choosing your instances: core count, memory size, storage size & type, network performance, I/O requirements & CPU technologies.
- Hurry Up & Go Idle - A larger compute instance can save you time and money, therefore paying more per hour for a shorter amount of time can be less expensive.

LOGO
UNIV/POLTEK

EC2 Instances Powered by Intel

DIGITAL
ALENT
SCHOLARSHIP

KOMINFO

aws

Technologies



TERBUKA

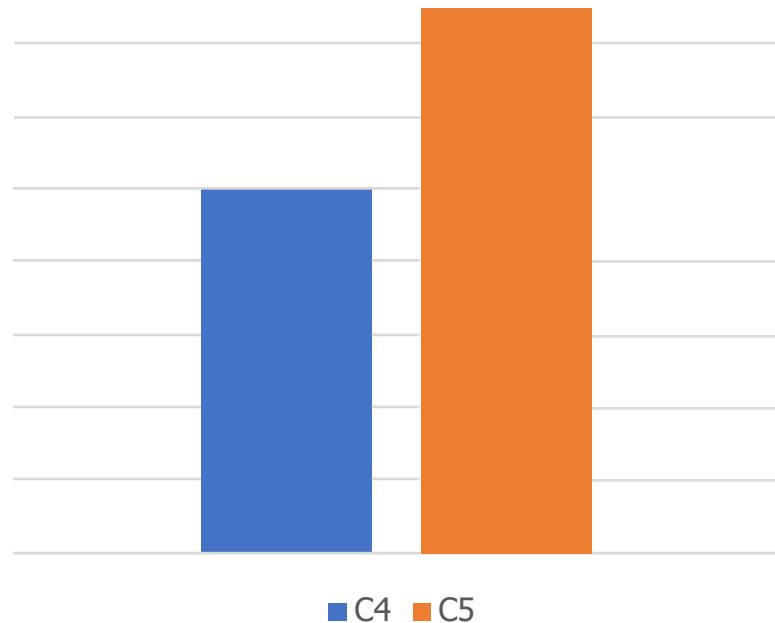
EC2 Instance Type	Compute Optimized		General Purpose			Memory Optimized			Storage Optimized		
	C5	C4	M5	M4	T2	X1	X1e	R4	H1	I3	D2
Intel Processor	Xeon Platinum 8175M	Xeon E5 2666 v3	Xeon Platinum 8175M	Xeon E5 2686 v4 2676 v3	Xeon Family	Xeon E7 8880 v3	Xeon E7 8880 v3	Xeon E5 2686 v4	Xeon E5 2686 v4	Xeon E5 2686 v4	Xeon E5 2676 v3
Intel Processor Technology	Skylake	Haswell	Skylake	Broadwell Haswell	Yes	Haswell	Haswell	Broadwell	Broadwell	Broadwell	Haswell
Intel AVX	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel AVX2	Yes	Yes	Yes	Yes	-	Yes	Yes	Yes	Yes	Yes	Yes
Intel AVX-512	Yes	-	Yes	-	-	-	-	-	-	-	-
Intel Turbo Boost	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Storage	EBS-only	EBS-only	EBS-only	EBS-only	EBS-only	SSD EBS-Opt	SSD EBS-Opt	-	HDD	SSD	HDD



C5: Compute Optimized Instances



25% price/performance improvement over C4



- Based on 3.0 GHz Intel Xeon Scalable Processors (Skylake)
- Up to 72 vCPUs and 144 GiB of memory (2:1 Memory:vCPU ratio)
- 25 Gbps NW bandwidth
- Support for Intel AVX-512



"We saw significant performance improvement on Amazon EC2 C5, with up to a 140% performance improvement in industry standard CPU benchmarks over C4."



GRAIL

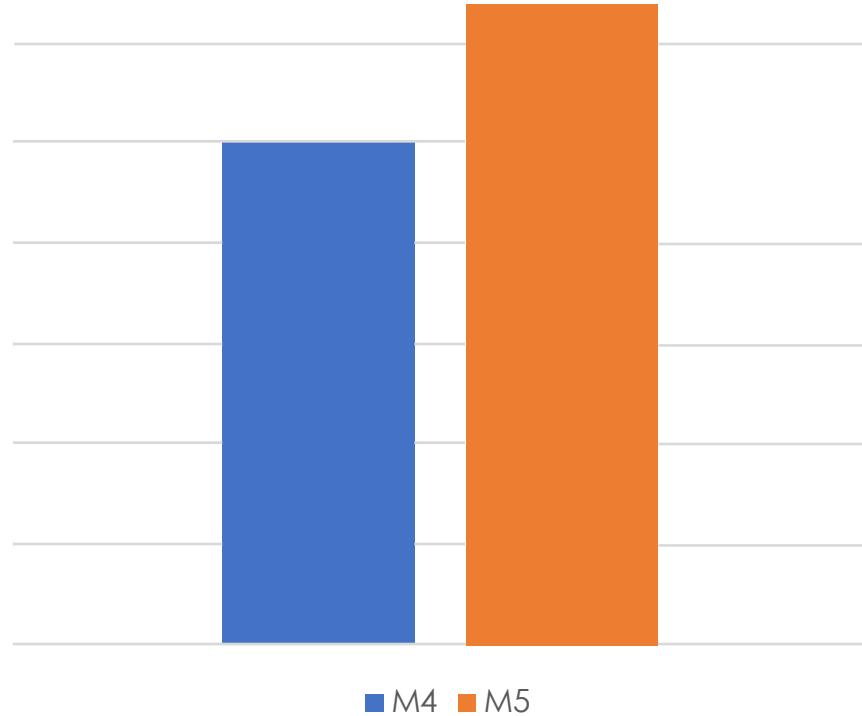
"We are eager to migrate onto the AVX-512 enabled c5.18xlarge instance size... . We expect to decrease the processing time of some of our key workloads by more than 30%."



M5: Next-Gen General Purpose instance



14% price/performance improvement With M5



- Powered by 2.5 GHz Intel Xeon Scalable Processors ([Skylake](#))
- New larger instance size—m5.24xlarge with [96 vCPUs](#) and [384 GiB of memory](#) (4:1 Memory:vCPU ratio)
- Improved network and EBS performance on smaller instance sizes
- Support for Intel [AVX-512](#) offering up to twice the performance for vector and floating point workloads

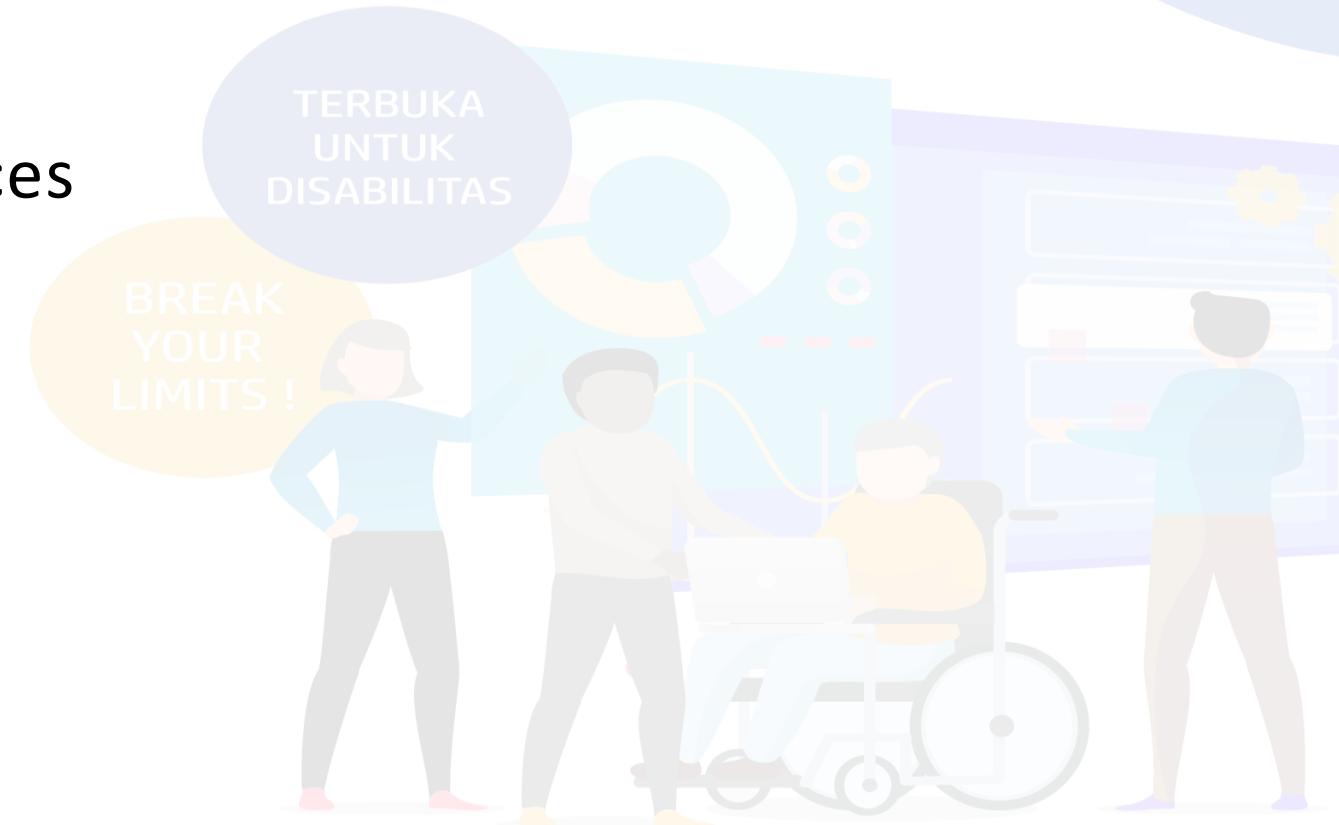


Elastic Load Balancing (ELB)

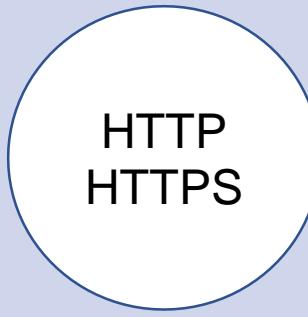
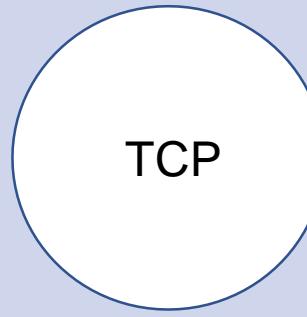


Balancing

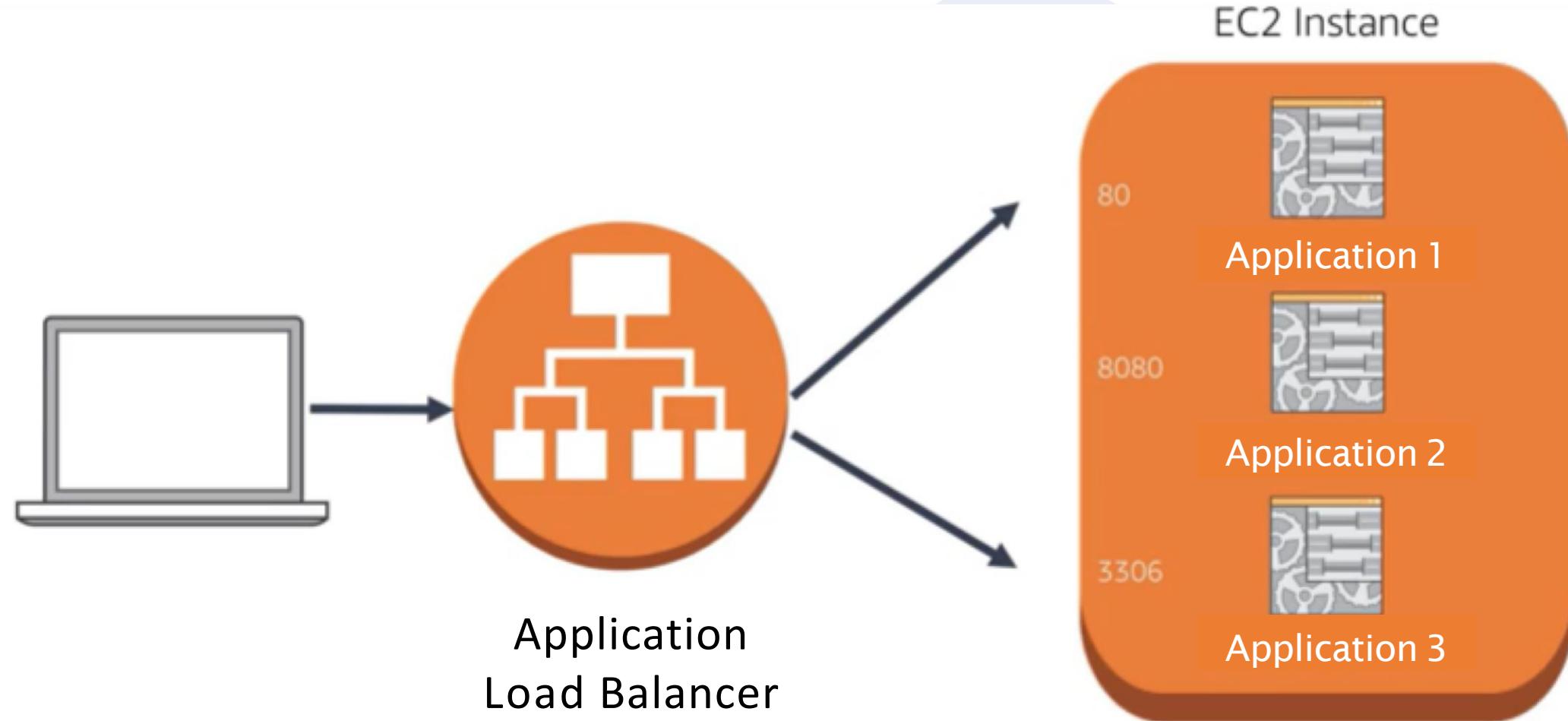
- Managed load balancing service
- Distributes loads between instances



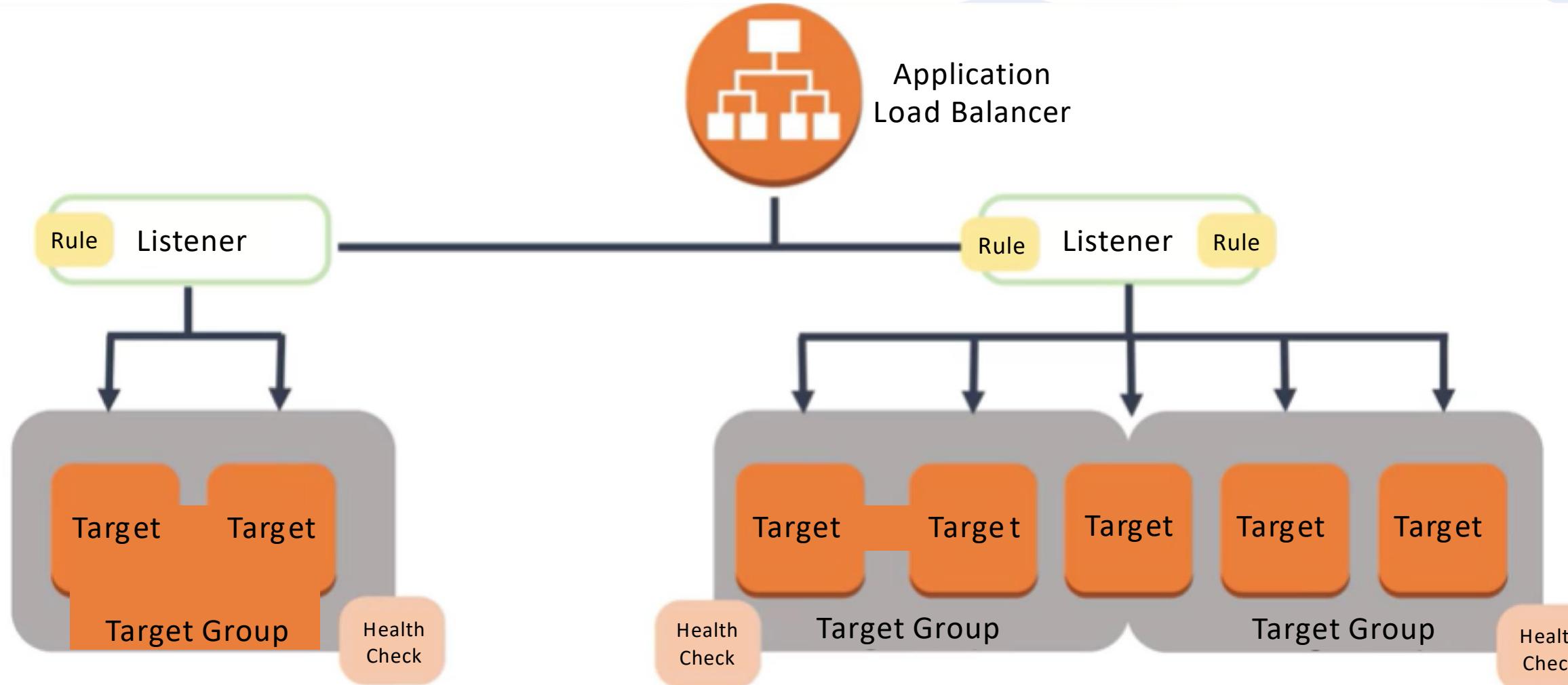
Products

Application Load Balancer (ALB)	Network Load Balancer (NLB)	Classic Load Balancer (CLB)
 HTTP HTTPS	 TCP	PREVIOUS GENERATION for HTTP, HTTPS, and TCP
<ul style="list-style-type: none">• Flexible application management• Advanced load balancing of HTTP and HTTPS traffic• Operates at the request level (Layer 7)	<ul style="list-style-type: none">• Extreme performance and static IP for your application• Load balancing of TCP traffic• Operates at the connection level (Layer 4)	<ul style="list-style-type: none">• Existing application that was built within the EC2-Classic network• Operates at both the request level and connection level

Cases



Cases



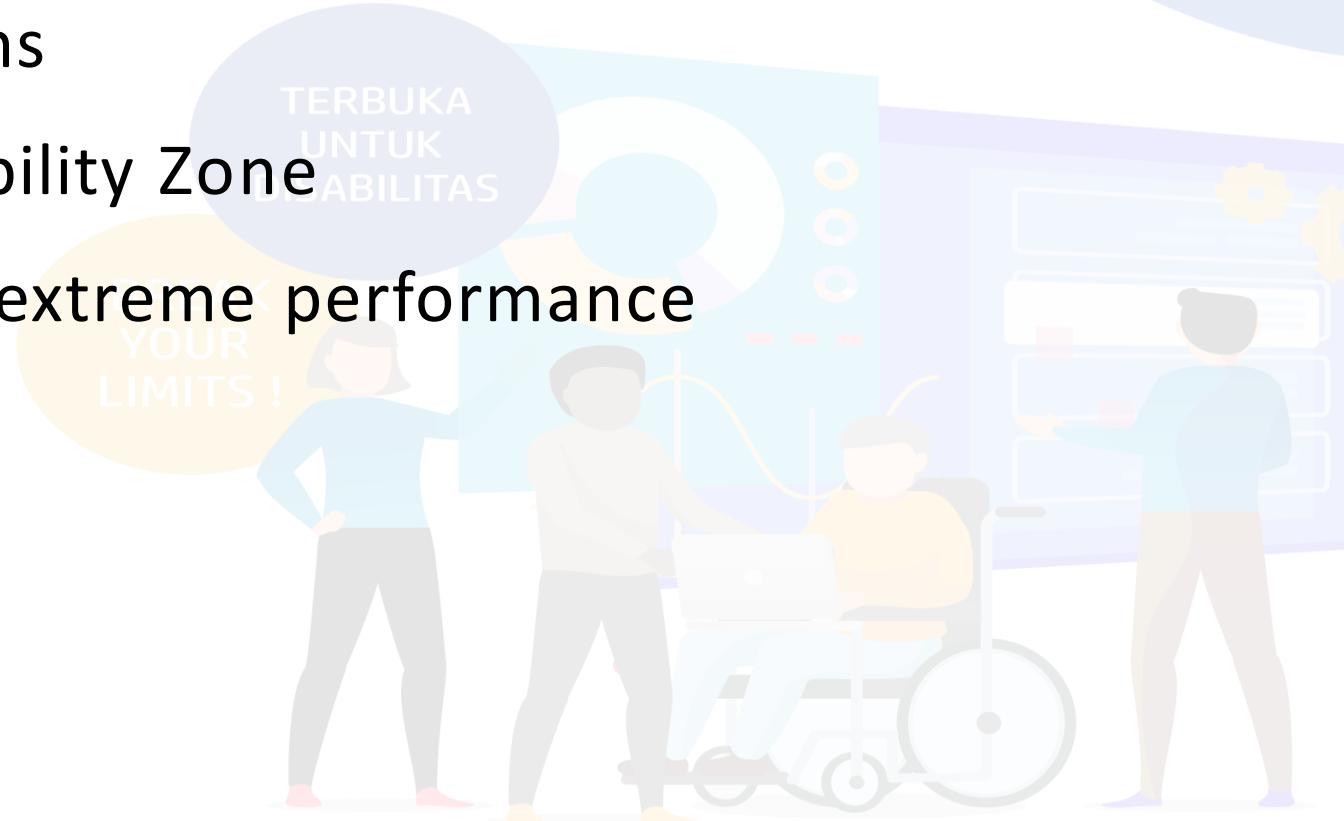
Cases

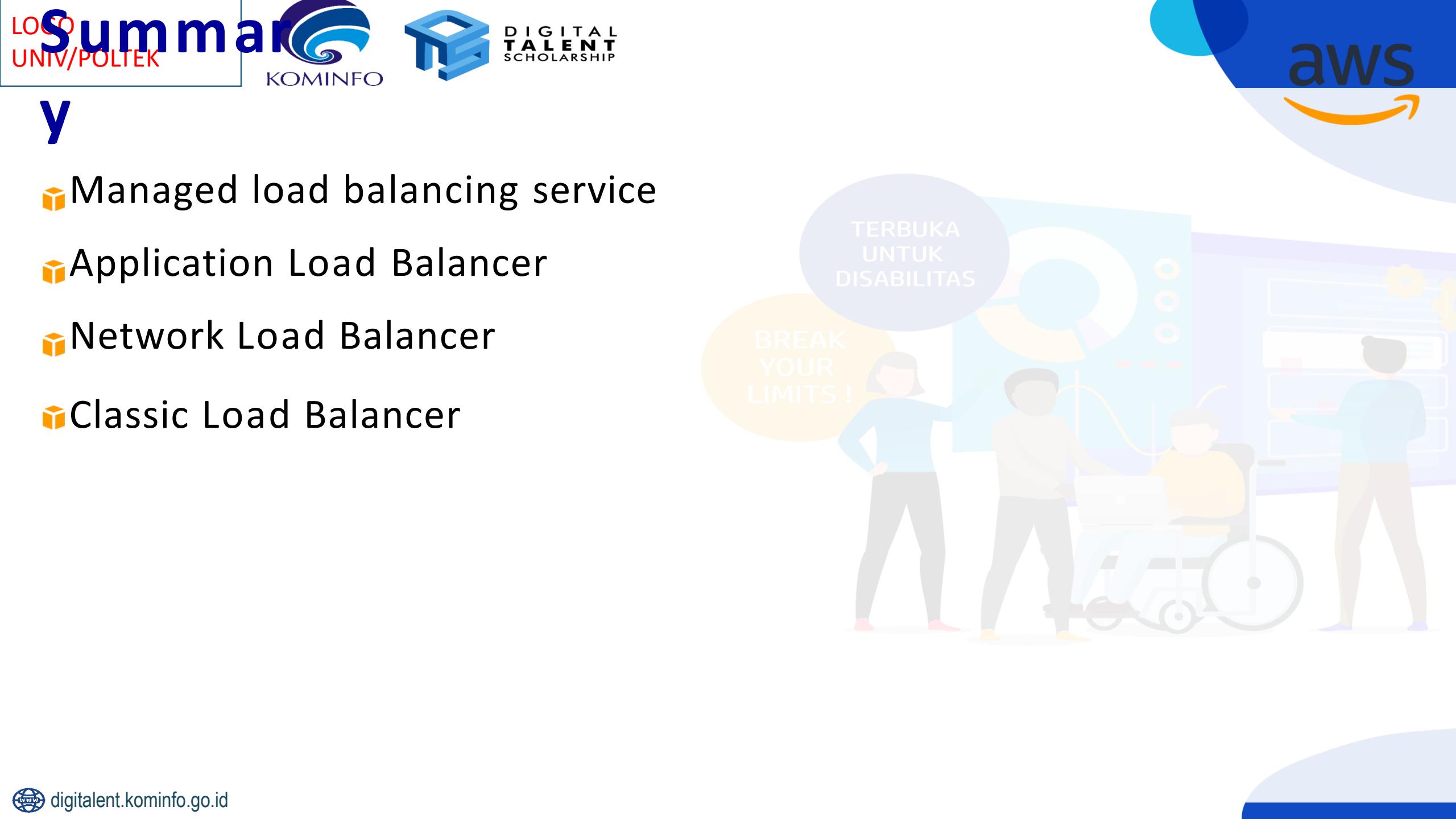
- Access servers through single point
- Decouple the application environment
- Provide high availability and fault tolerance
- Increase elasticity and scalability



Cases

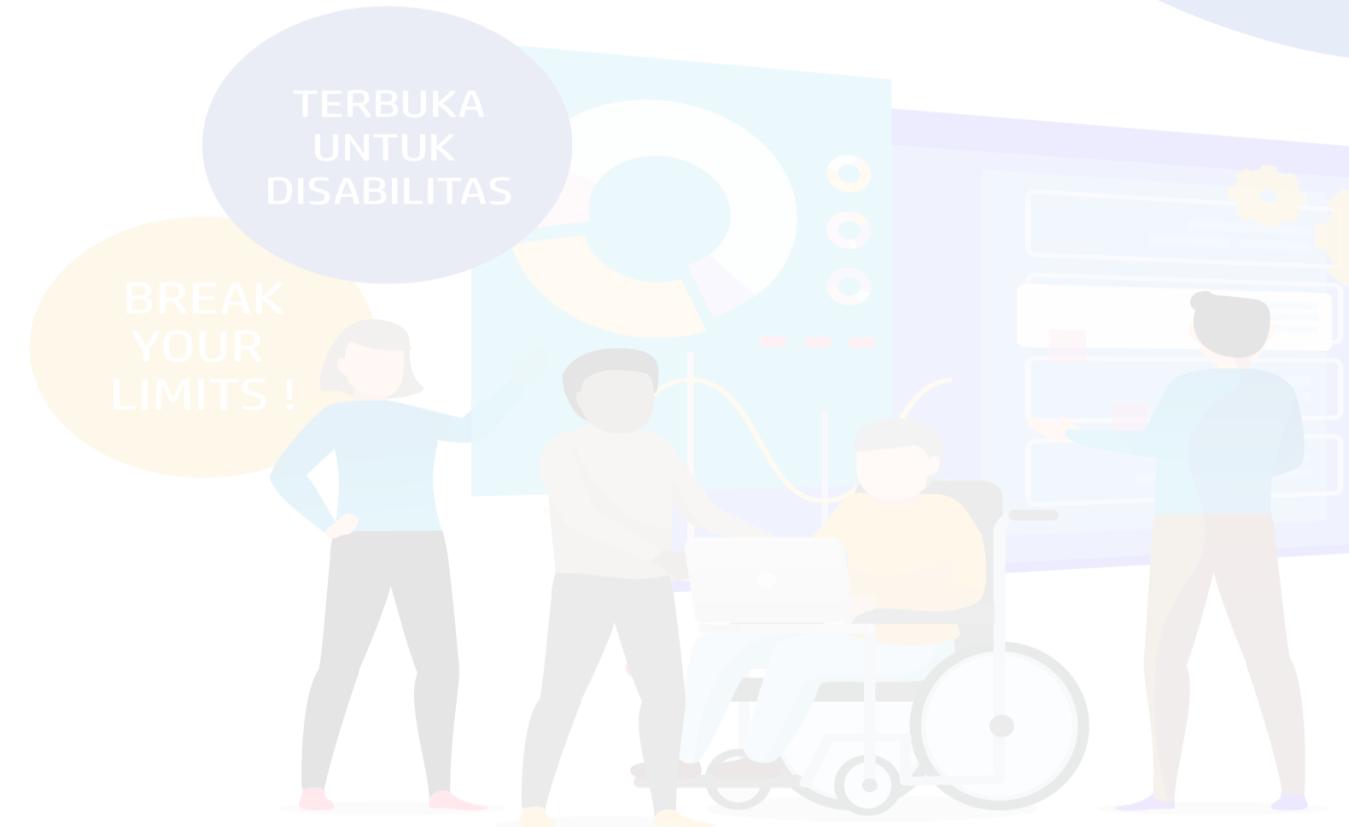
- Sudden and volatile traffic patterns
- Single static IP address per Availability Zone
- Ideal for applications that require extreme performance





y

- Managed load balancing service
- Application Load Balancer
- Network Load Balancer
- Classic Load Balancer



Auto Scaling



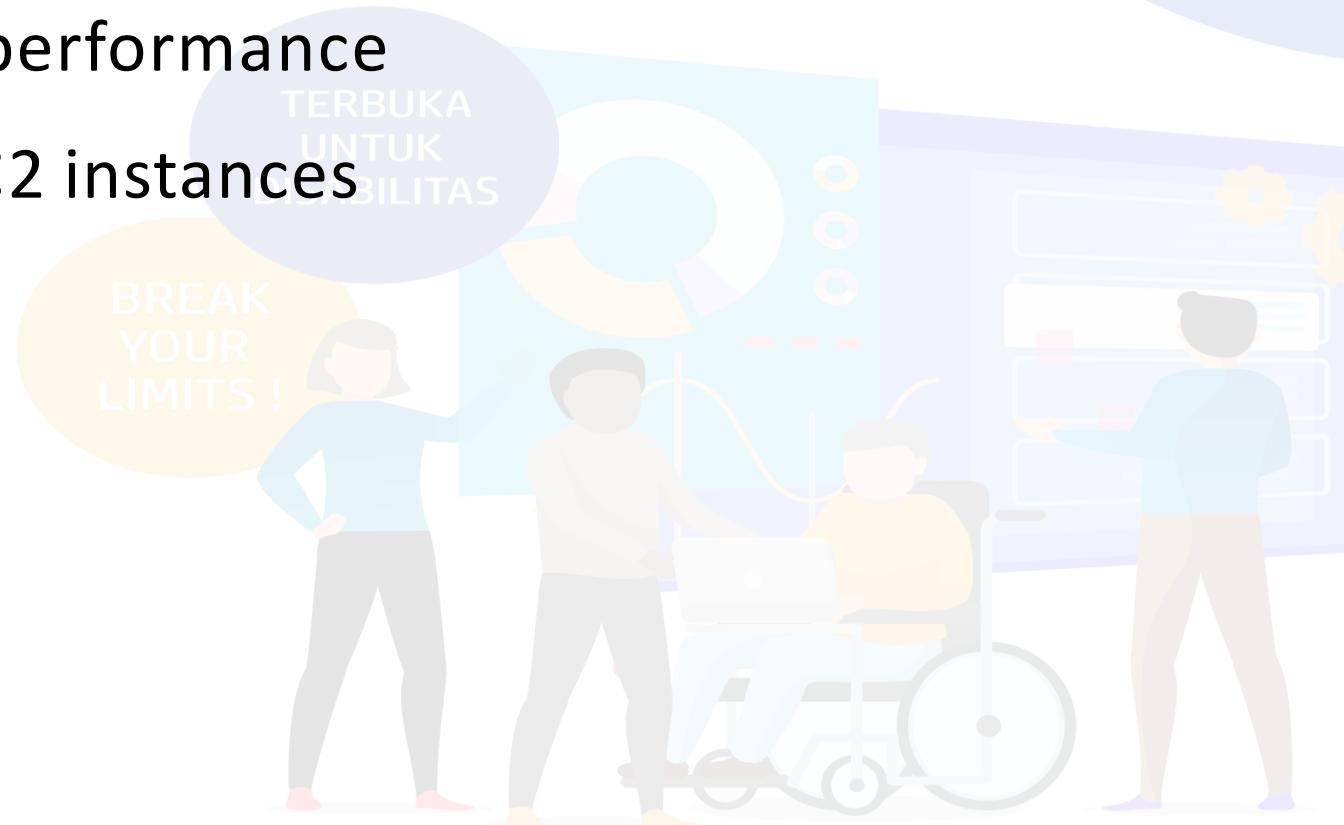
Helps you verify that you have the desired number of Amazon EC2 instances available to handle the load for your application



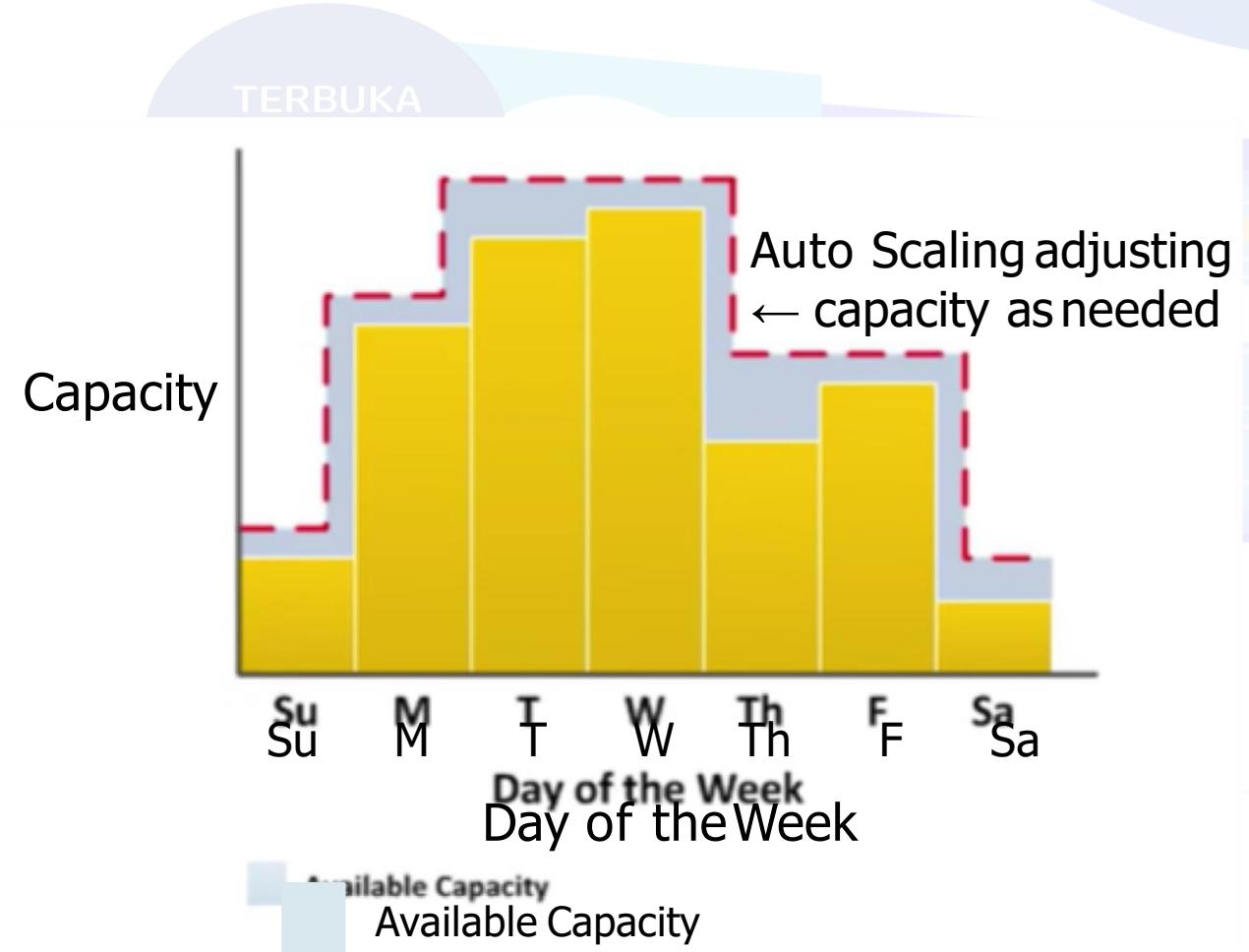
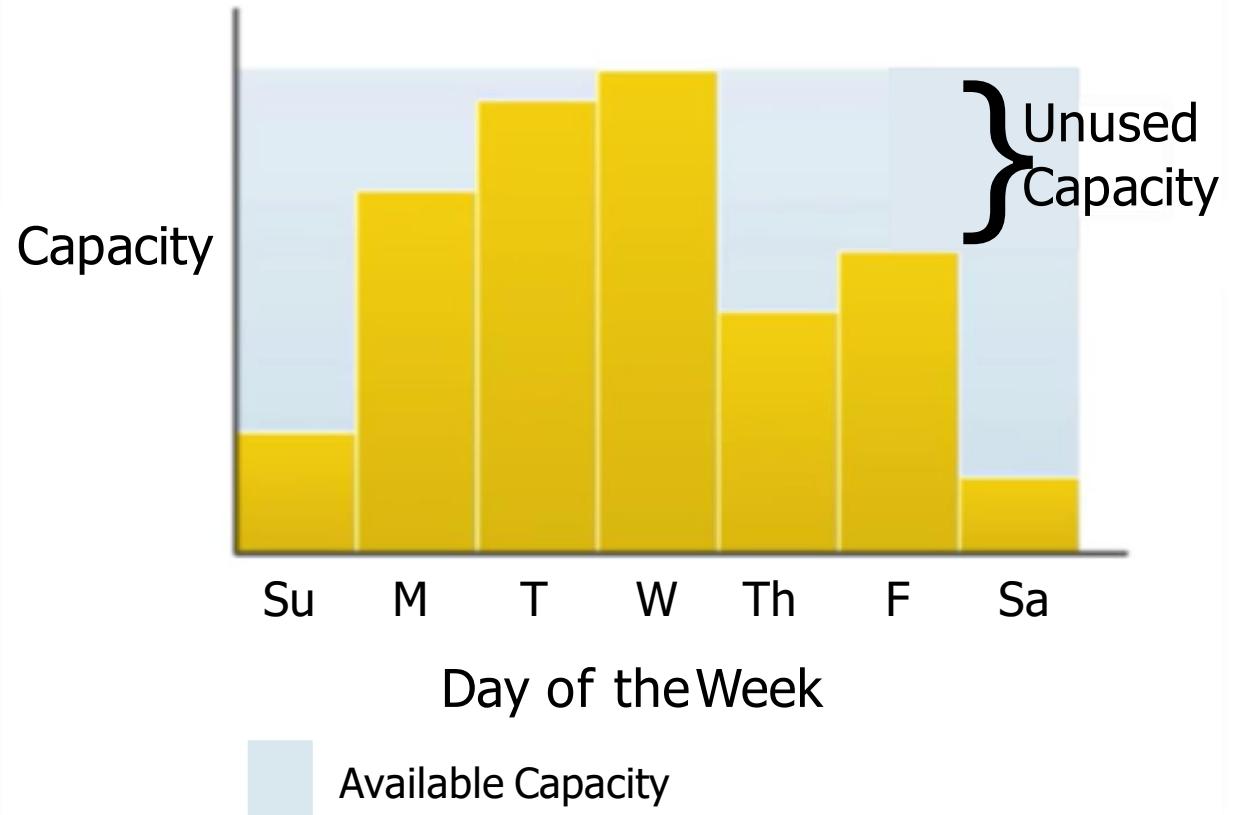


Performance

- Amazon CloudWatch to monitor performance
- Auto Scaling to add or remove EC2 instances



Capacity Management



Questions

💡 How can I make sure that my workload has enough EC2 resources to meet fluctuating performance requirements?

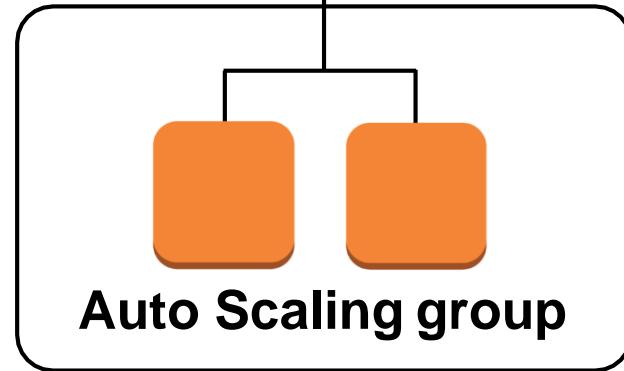
Scalability

💡 How can EC2 resource provisioning occur on-demand?

Automation

Scaling Out and Scaling In

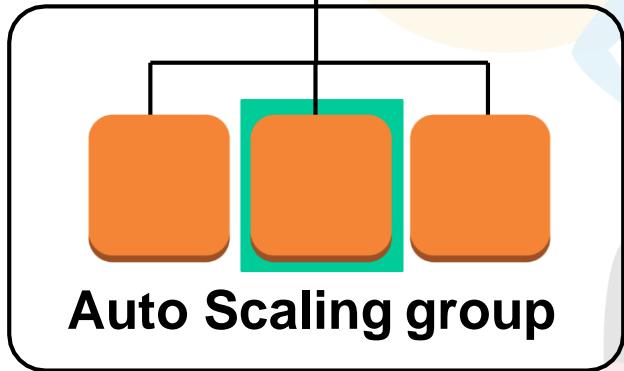
Elastic Load Balancing



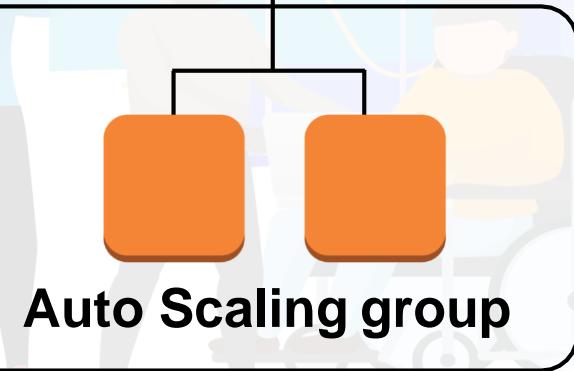
Base Configuration

TERBUKA
UNTUK
DISABILITAS

BREAK
YOUR
LIMITS!



Scaling Out



Scaling In

Launch Instances Terminate Instances

Components

- Launch Configuration
- Auto Scaling groups
- Auto Scaling Policy



Components

Launch Configuration: *What will be scaled?*

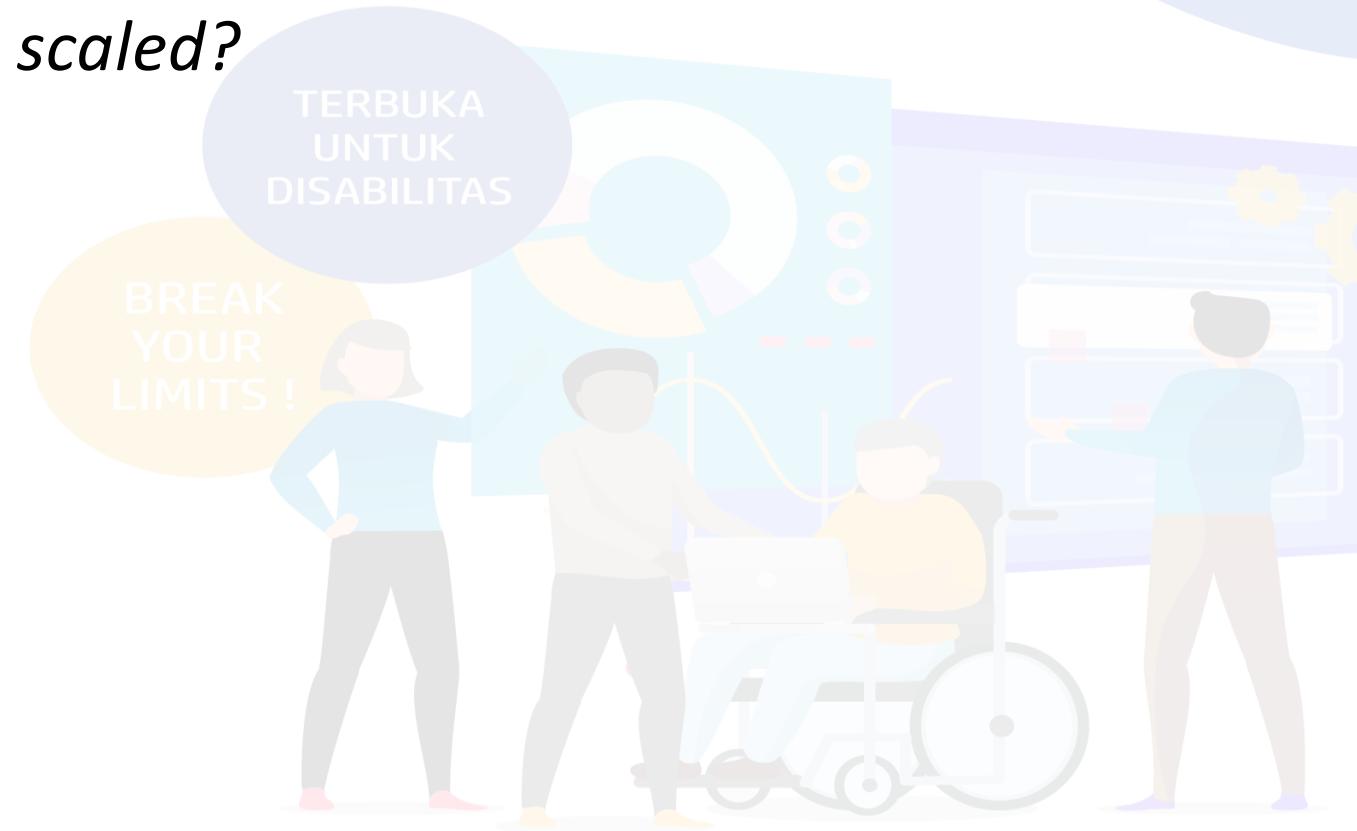
Launch settings

AMI

Instance type

Security groups

Roles



Components

Auto Scaling Group: *Where will it take place?*

■ Deployment settings

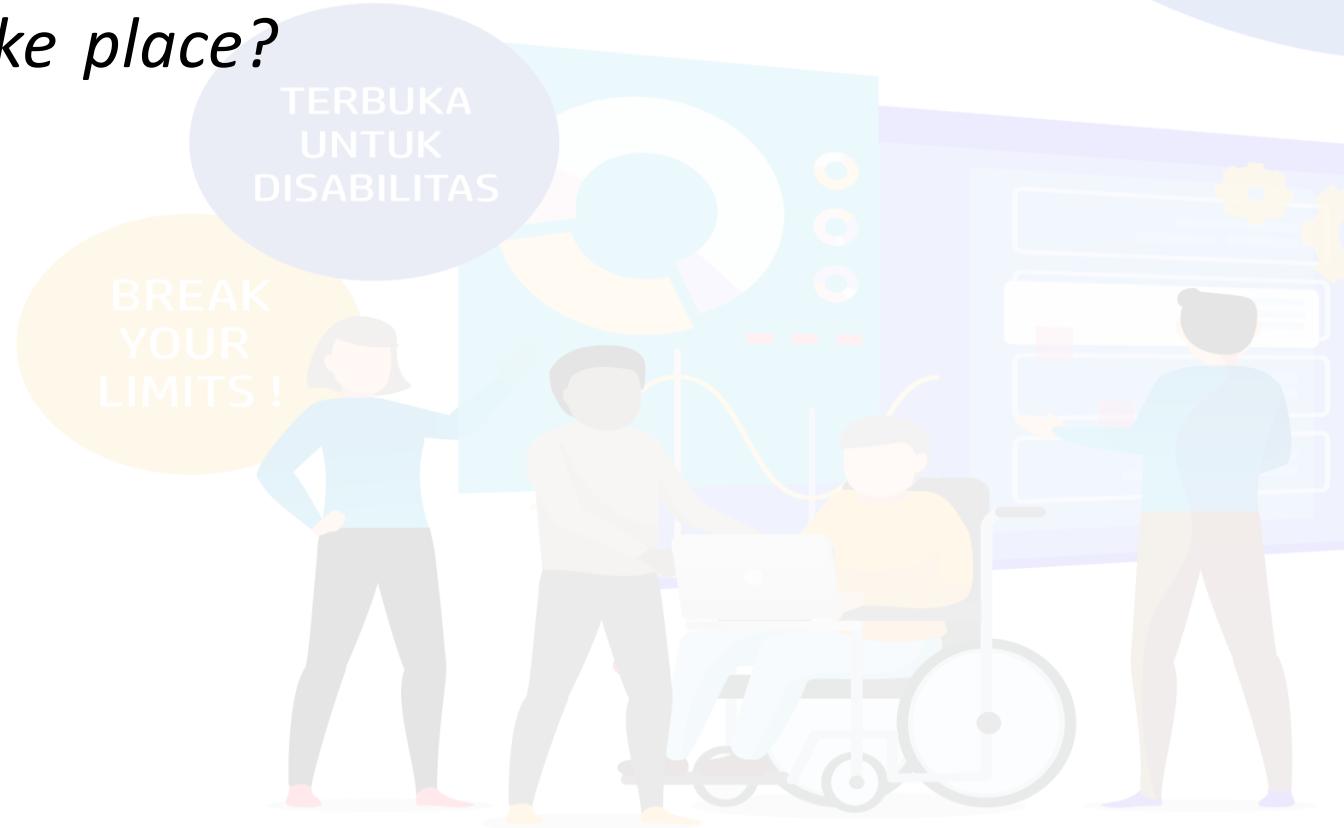
■ VPC and subnets

■ Load balancer

■ Minimum instances

■ Maximum instances

■ Desired capacity





Auto Scaling Components



Auto Scaling Policy: *When will it take place?*

Policy settings

P Scheduled

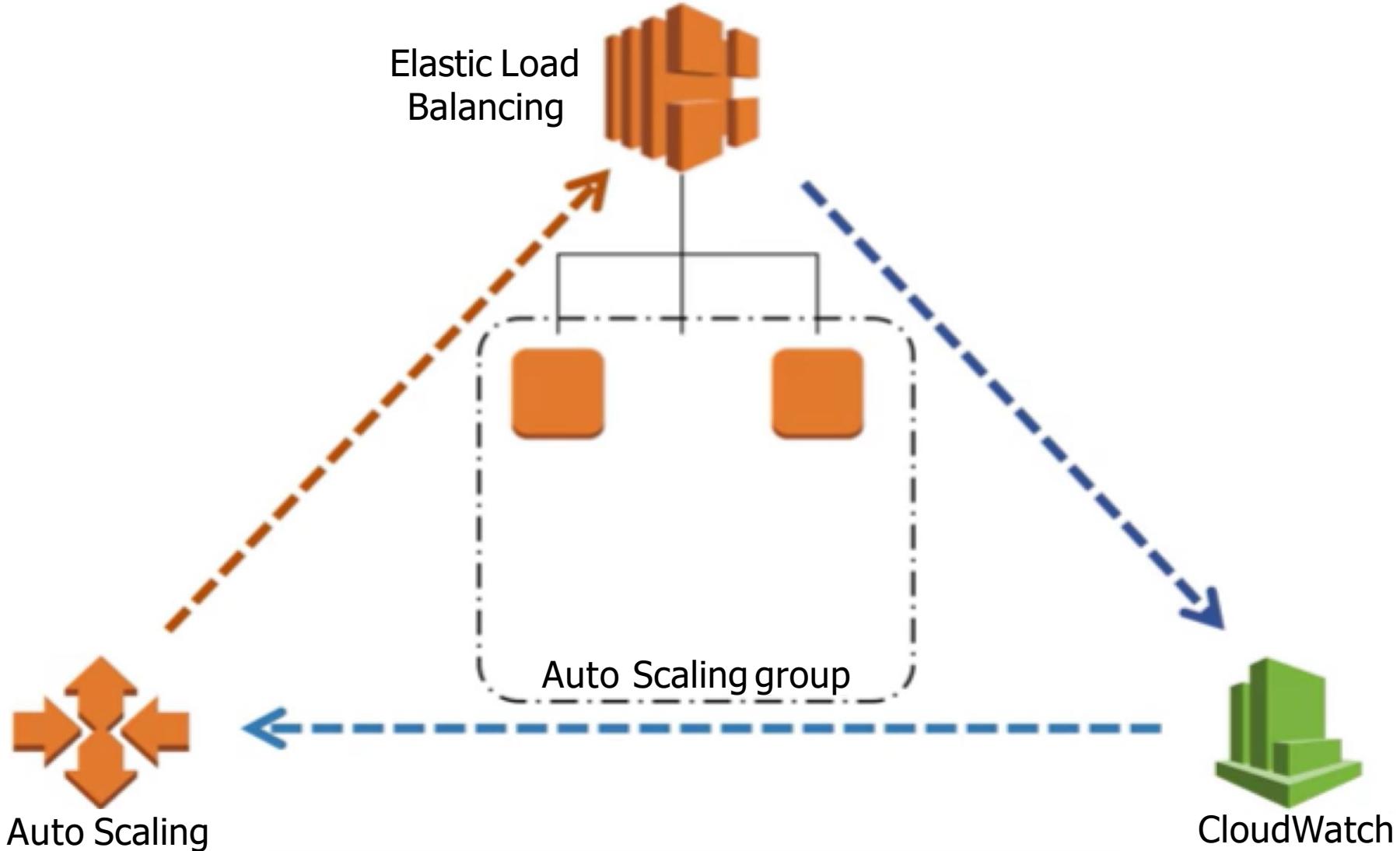
P On-demand

P Scale-out policy

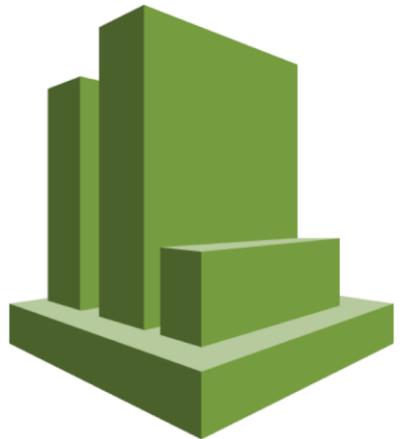
P Scale-in policy



Scaling



Scaling



Whenever: CPUUtilization

is: \geq

80

for: 1 consecutive period(s)

AutoScaling Action

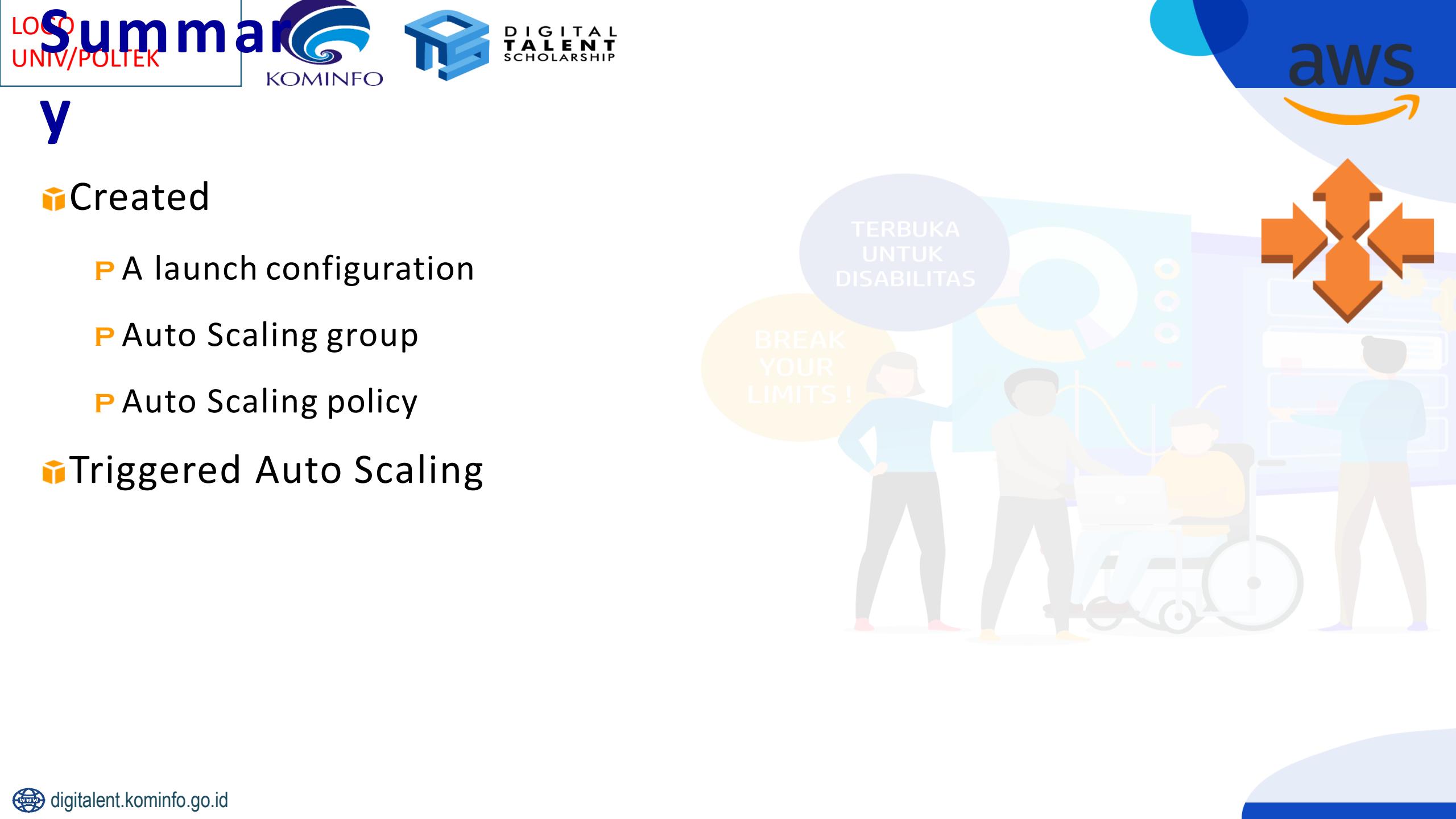
[Delete](#)

Whenever this alarm: State is ALARM

From resource type: AutoScaling

From the: IREASG

Take this action: Increase Group Size – Add 2 instances



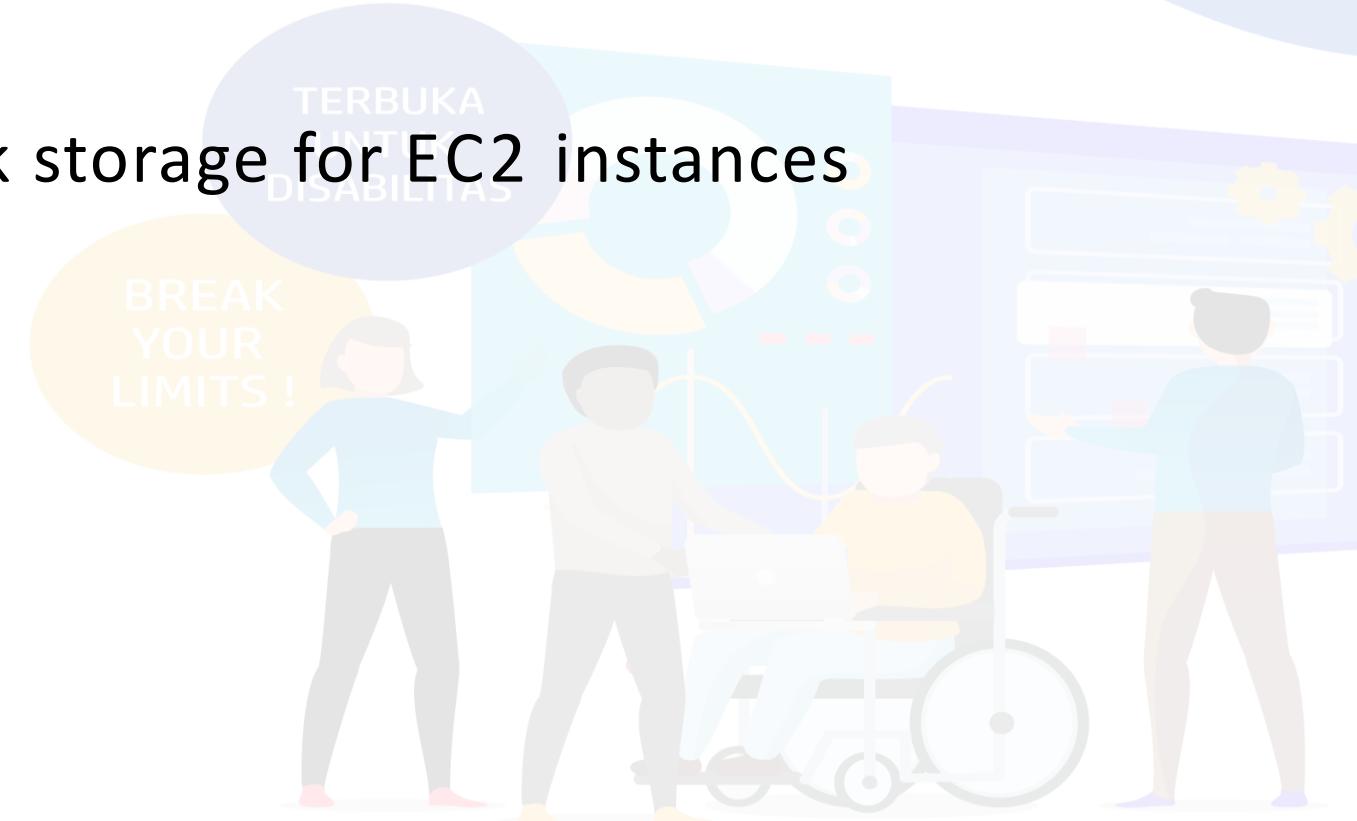
Amazon Elastic Block Store (EBS)



Volumes

Characteristics

- cube Persistent and customizable block storage for EC2 instances
- cube HDD and SSD types
- cube Use Snapshots for backups
- cube Easy and transparent encryption
- cube Elastic



Volumes

Availability

- Durable and automatically replicated

Drive Types

- Storage that best fits your needs
- Magnetic or SSD
- Performance and price requirements



EBS

Snapshots

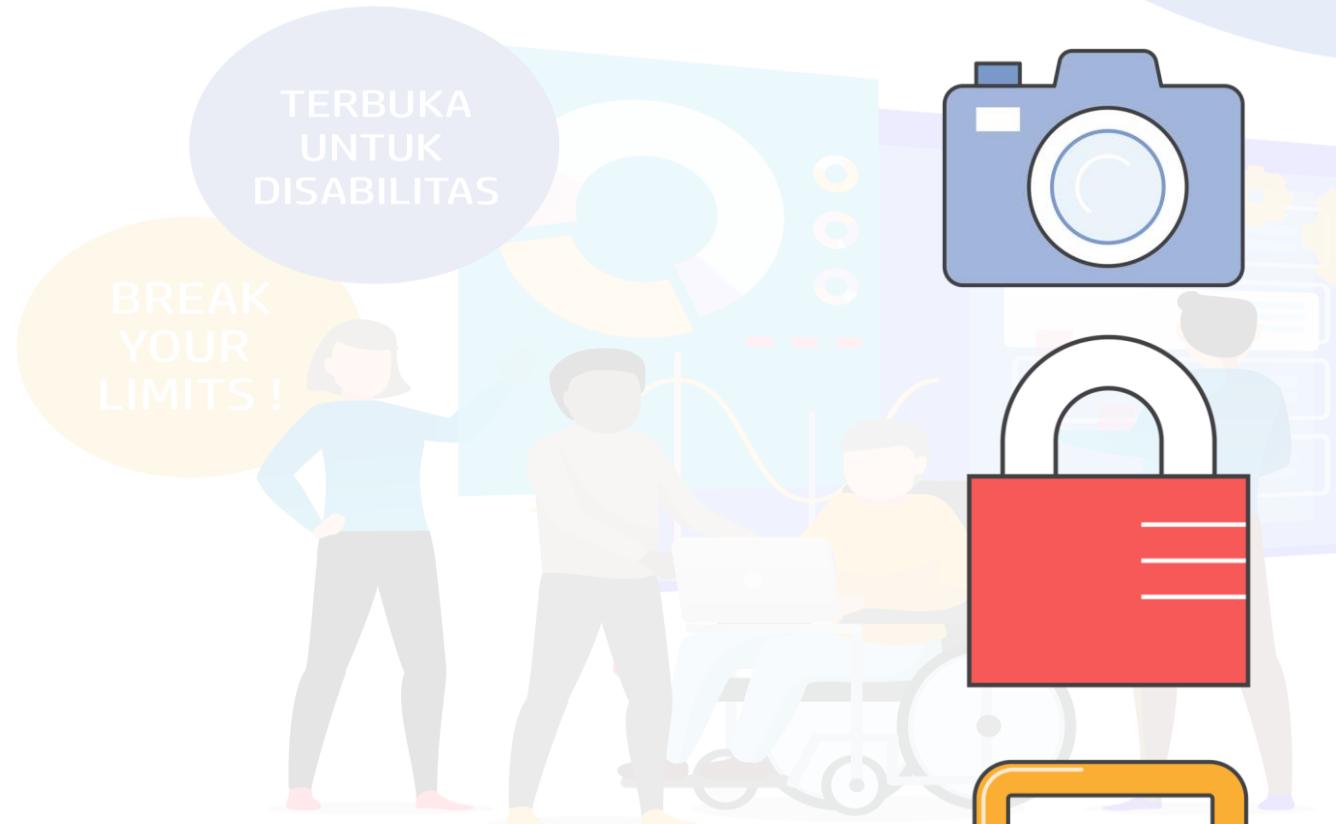
- Point-in-time snapshots
- Recreate a new volume at any time

Encryption

- Encrypted EBS volumes
- No additional cost

Elasticity

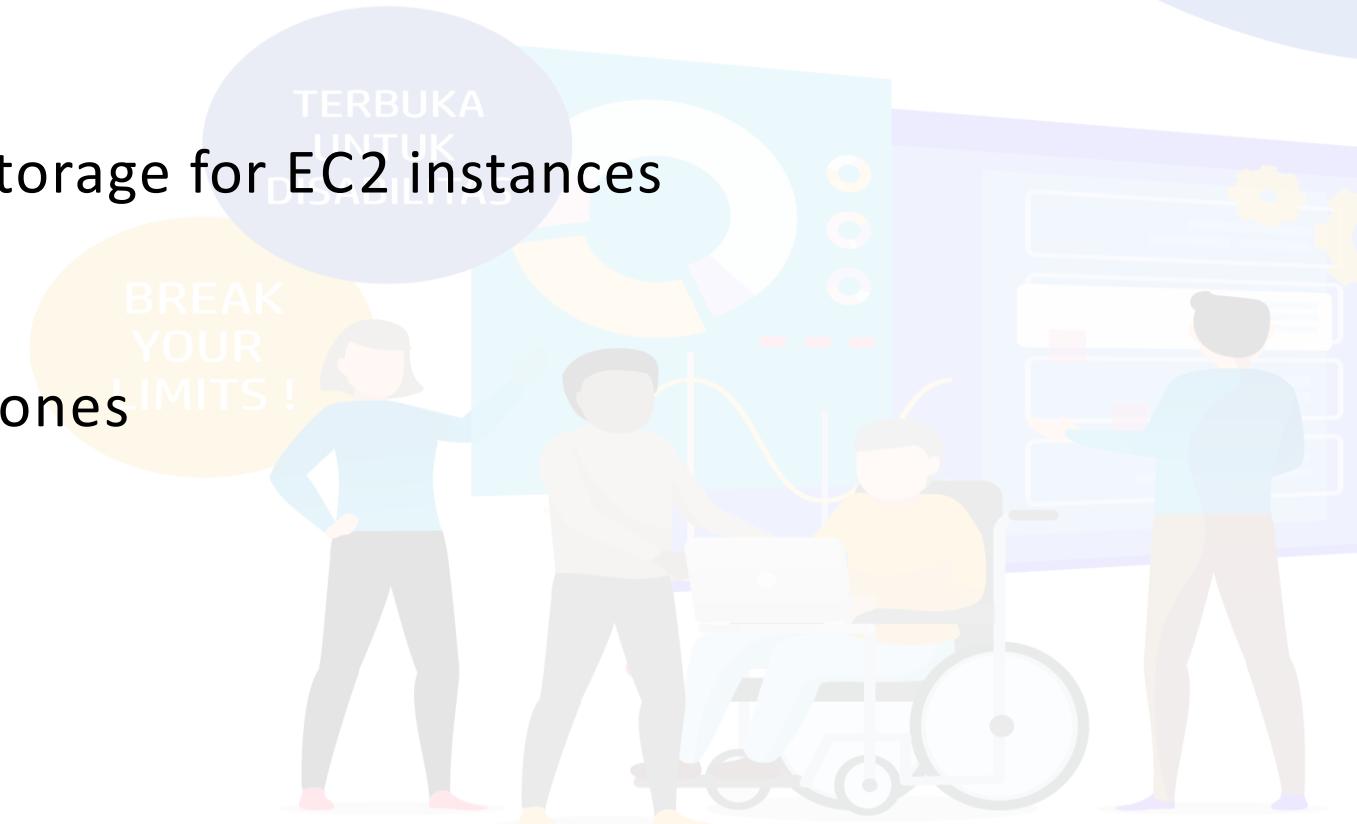
- Increase capacity
- Change to different types



y

Features

- P Persistent and customizable block storage for EC2 instances
- P HDD and SSD types
- P Replicated in the same Availability Zones
- P Easy and transparent encryption
- P Elastic volumes
- P Back up using snapshots



Amazon Simple Storage Service (S3)



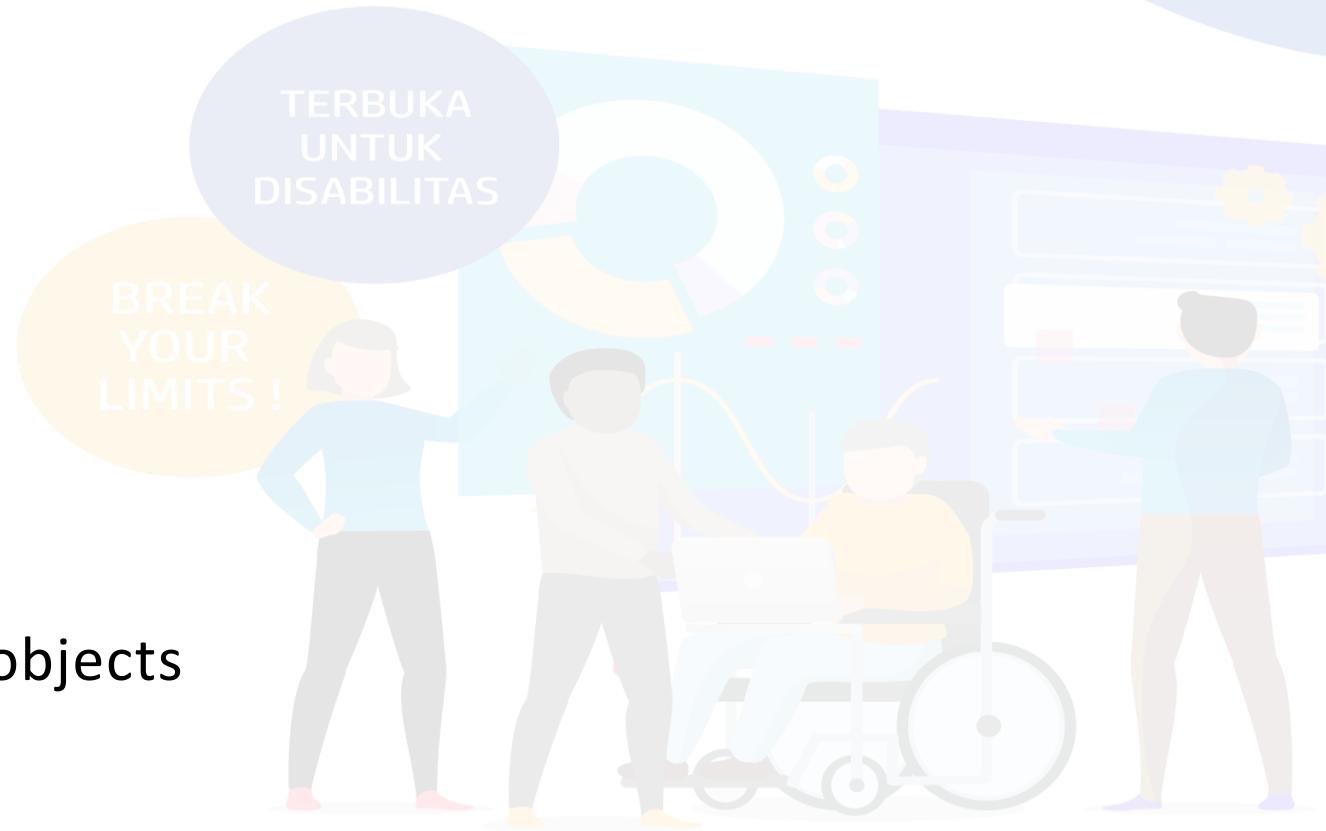
S3

Features

- P Fully managed cloud storage service
- P Rich security controls

Functionality

- P Store virtually unlimited number of objects
- P Access any time, from anywhere



Getting Started with S3



media/welcome.mp4



my-bucket-name

media/welcome.mp4



Key

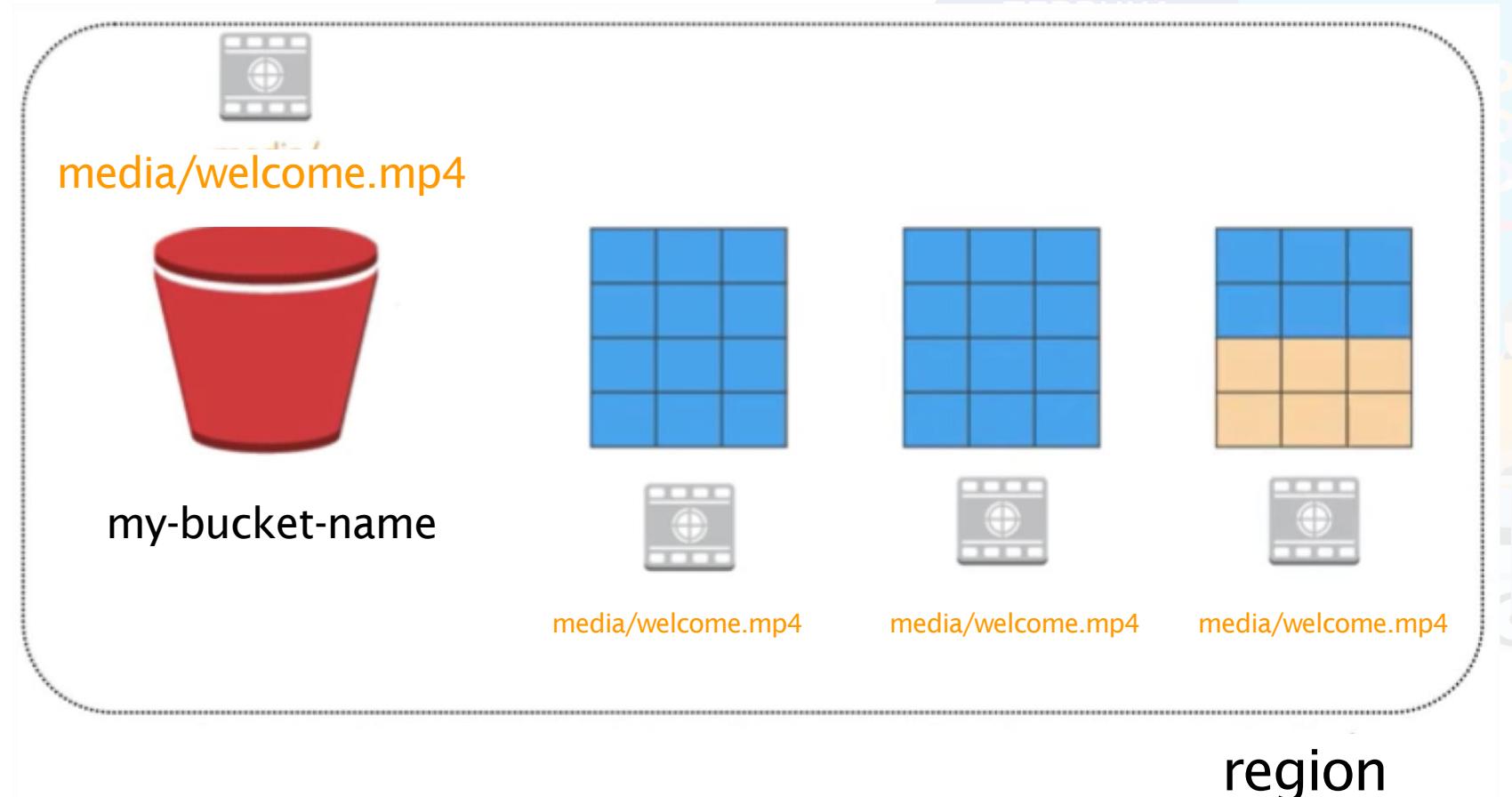


Object

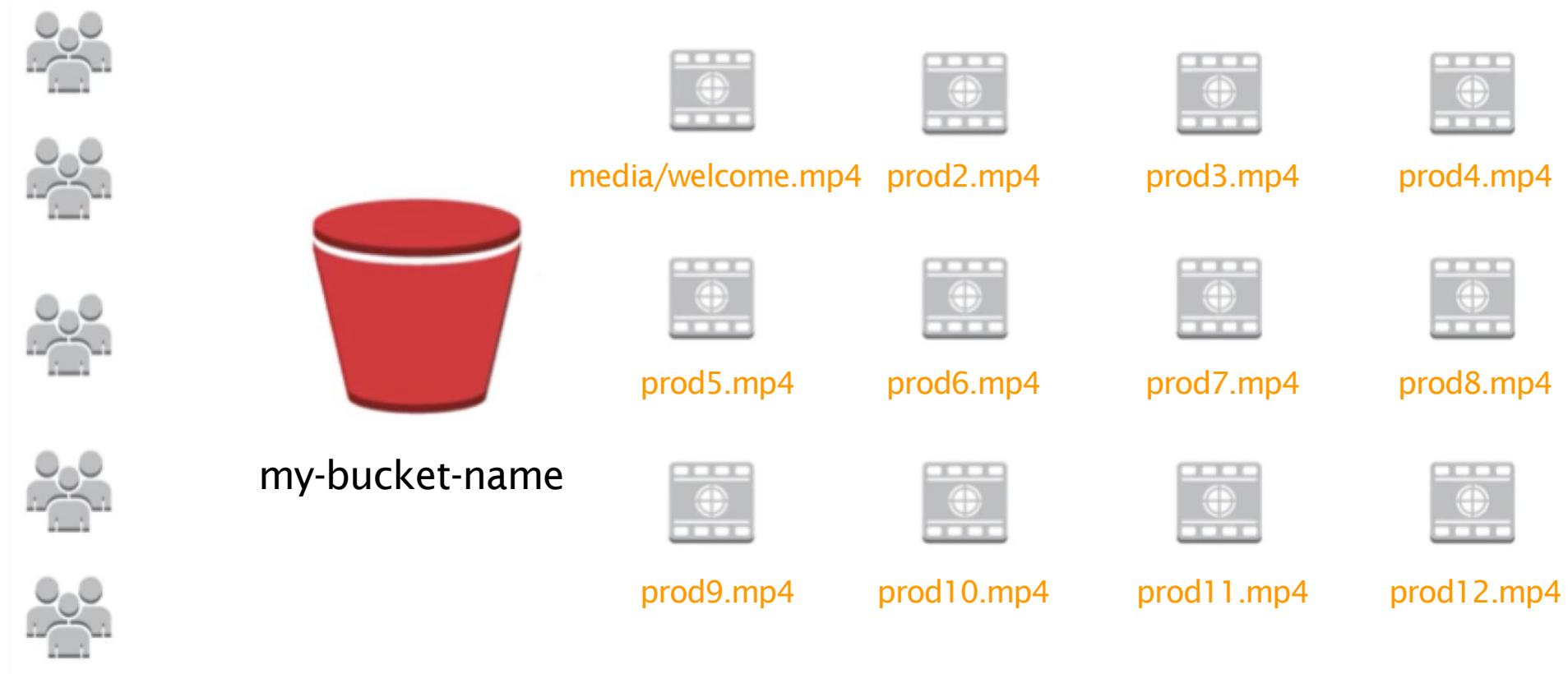


my-bucket-name

Data redundantly stored in region



Designed for seamless scaling



Anywhere

- AWS Management Console
- AWS command line interface
- AWS software development kits



Cases

- Storing application assets
- Static web hosting
- Backup and disaster recovery (DR)
- Staging area for big data



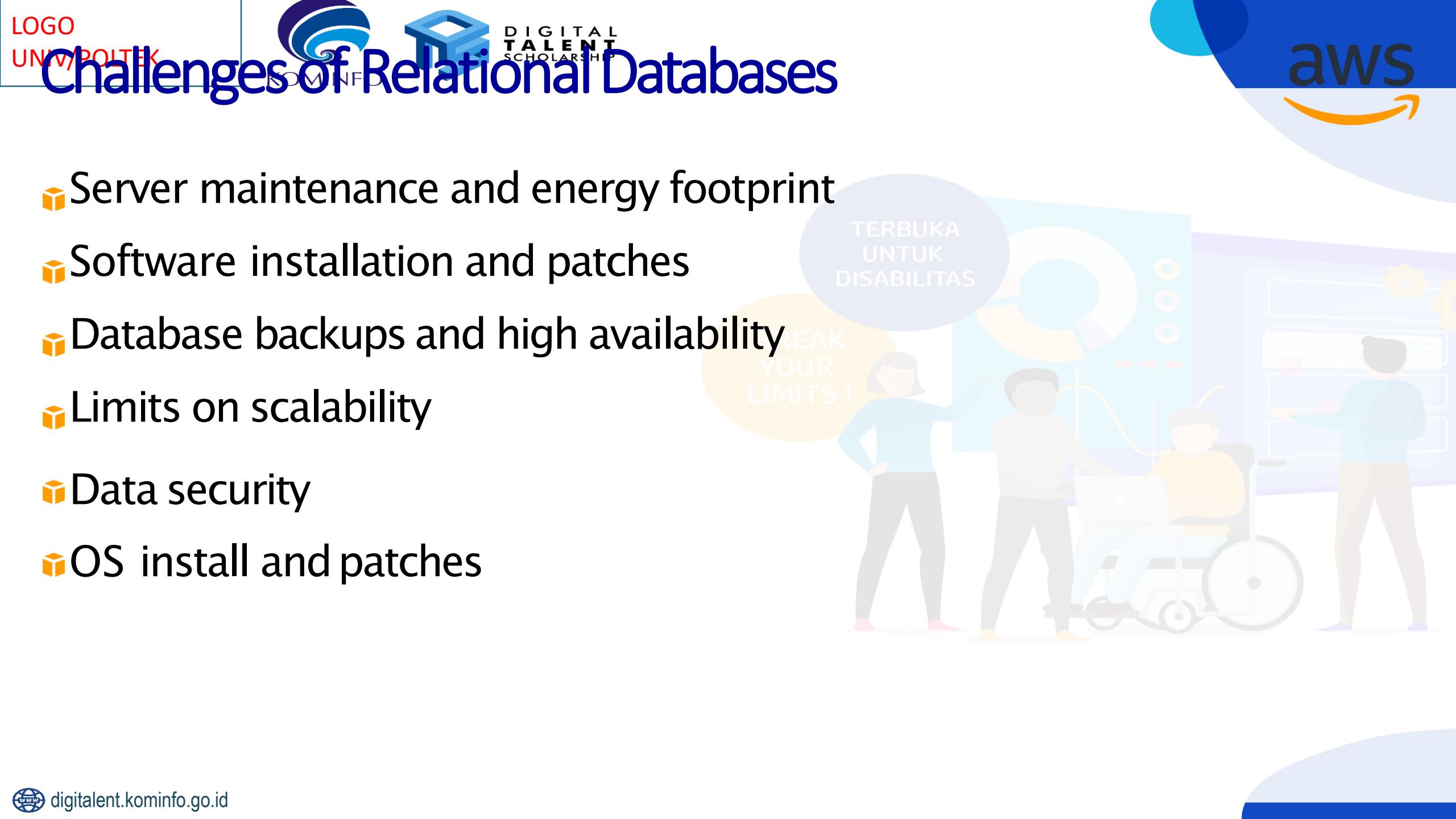
y

- Fully managed cloud storage service
- Store virtually unlimited number of objects
- Access any time, from anywhere
- Rich security controls
- Common use cases



Amazon Relational Database Service (RDS)



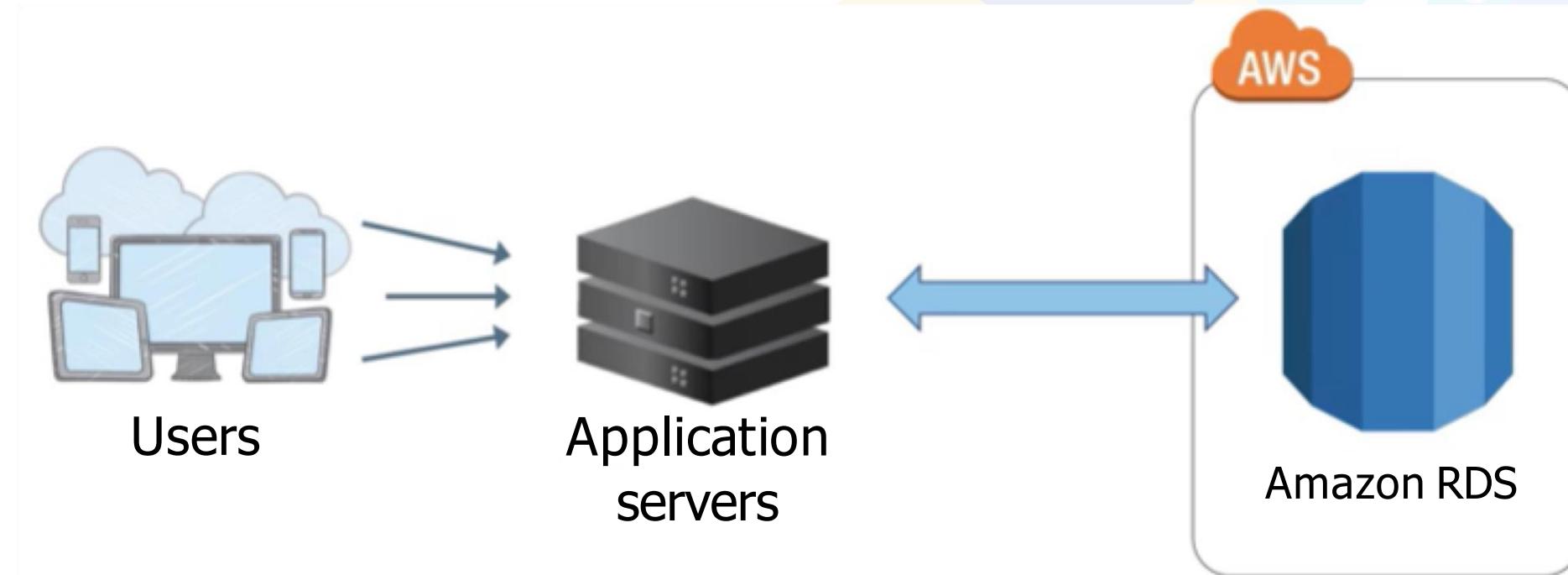


Challenges of Relational Databases

- Server maintenance and energy footprint
- Software installation and patches
- Database backups and high availability
- Limits on scalability
- Data security
- OS install and patches

RDS

Managed service that sets up and operates a relational database
in the Cloud



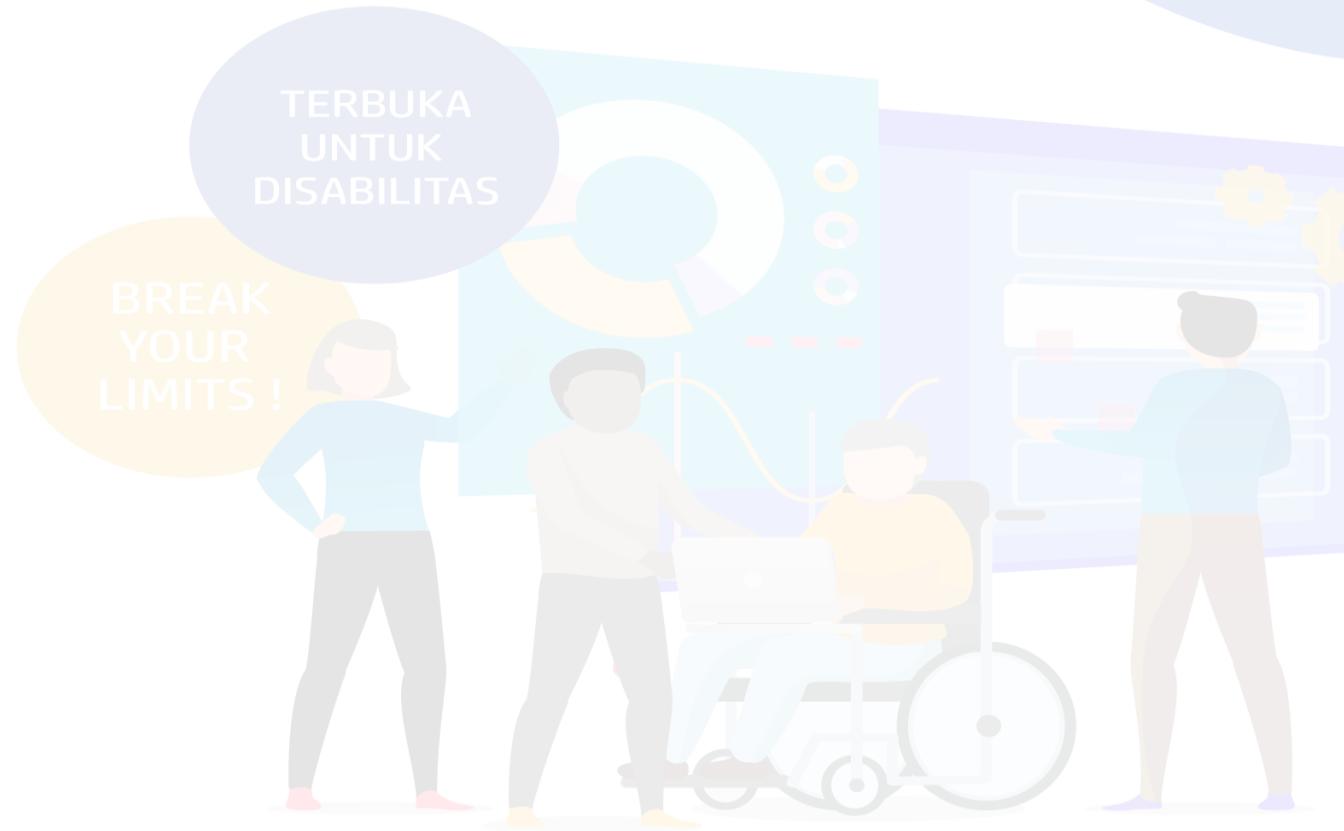
AWS Cloud

❖ Customer manages:

- ▶ Application Optimization
- ▶ Database schema
- ▶ Data

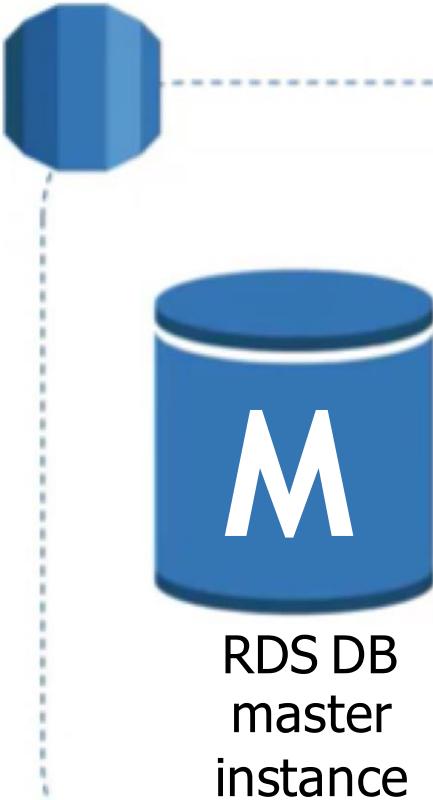
❖ AWS manages:

- ▶ OS installation and patches
- ▶ Database software installation and patches
- ▶ Database backups
- ▶ High availability
- ▶ Scaling
- ▶ Power, rack and stack
- ▶ Server maintenance



Instances

Amazon
RDS



DB Instance Class

- CPU
- Memory
- Network Performance

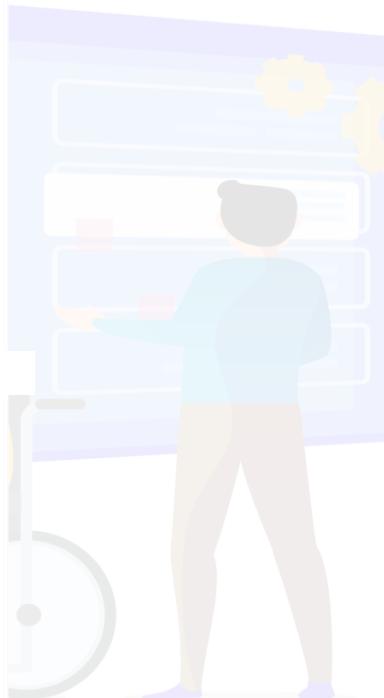
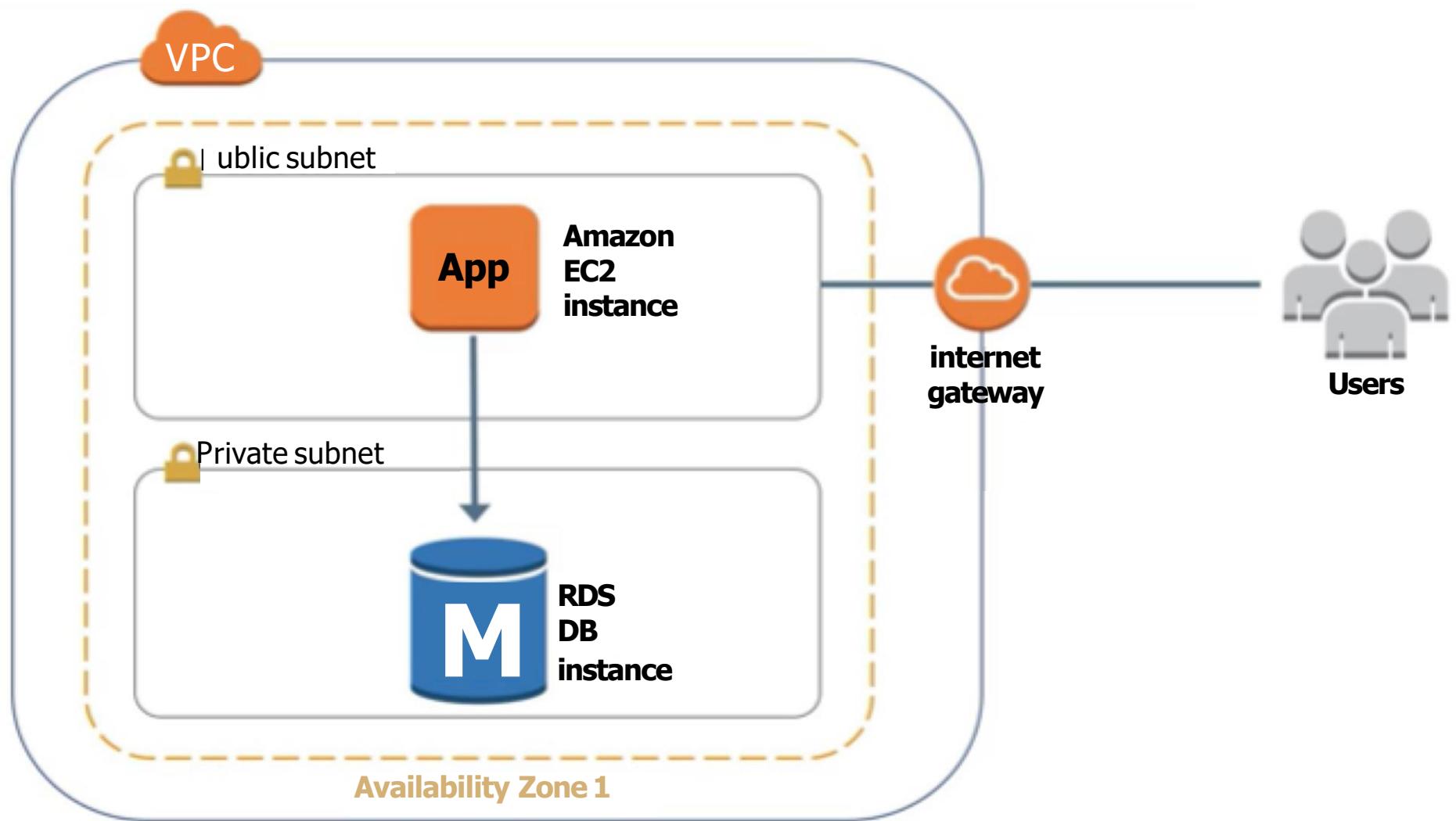
DB Instance Storage

- Magnetic
- General Purpose (SSD)
- Provisioned IOPS

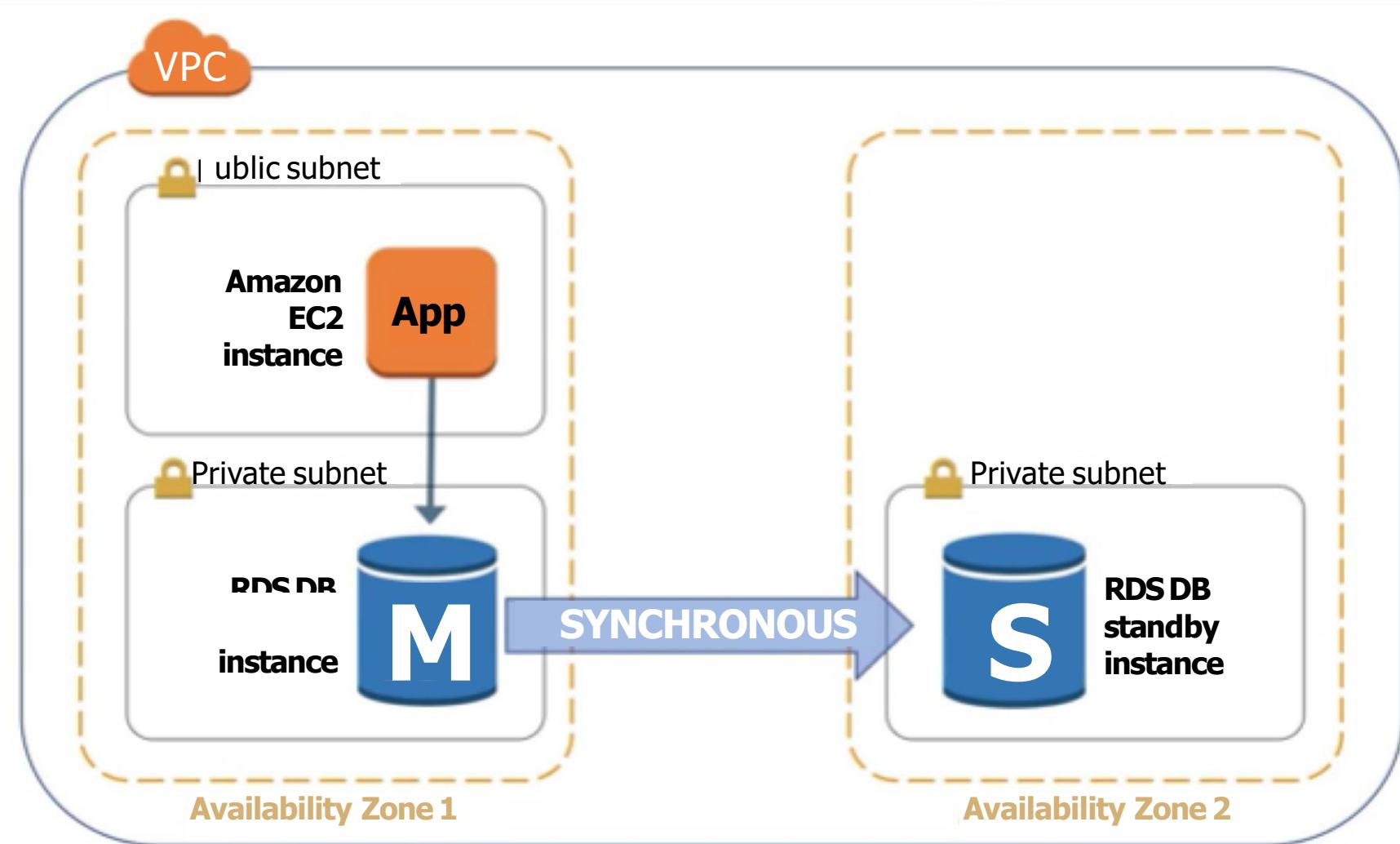


DB Engines

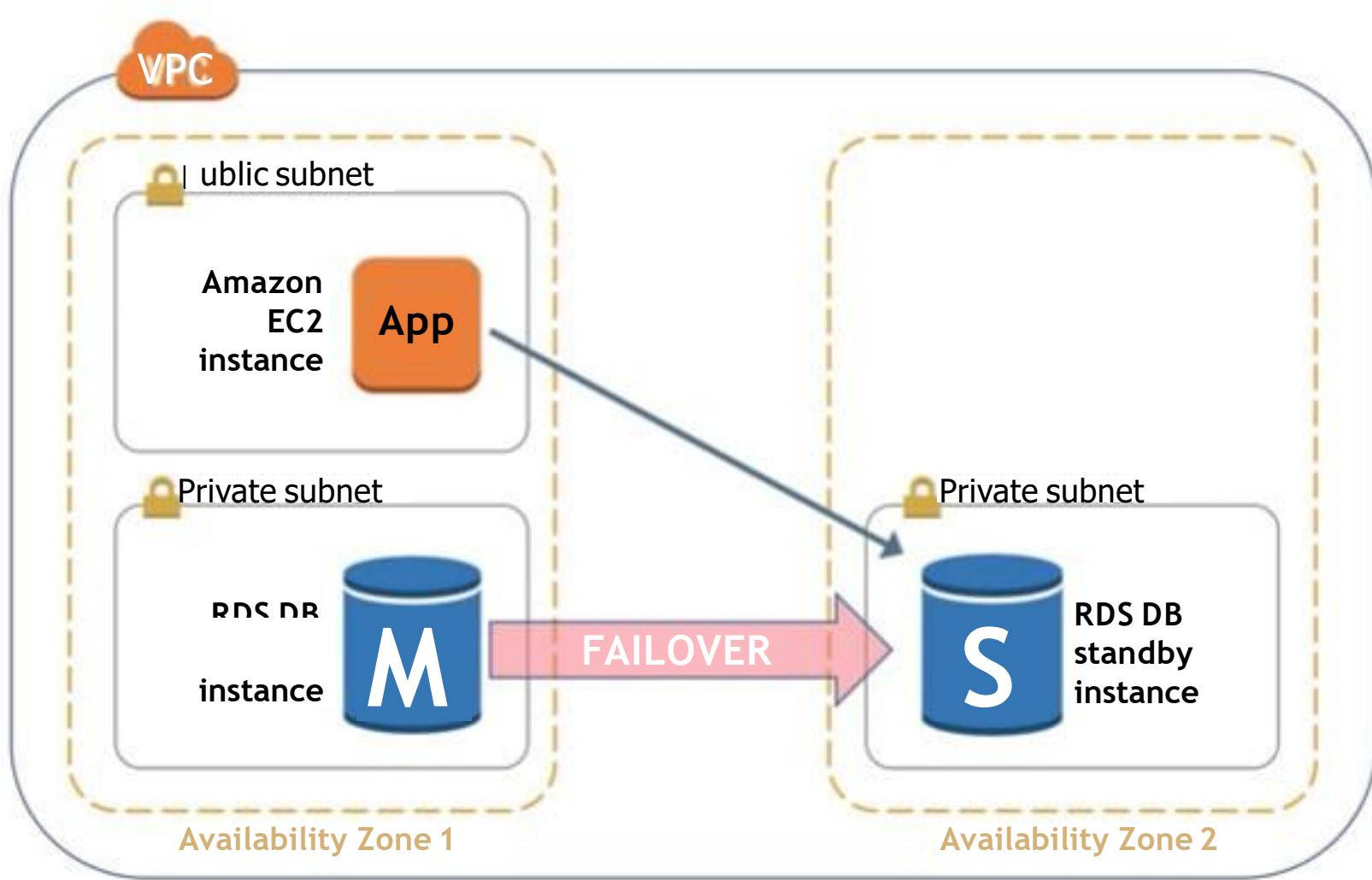
Amazon RDS Ina Virtual Private Cloud



High Availability with Multi-AZ



High Availability with Multi-AZ

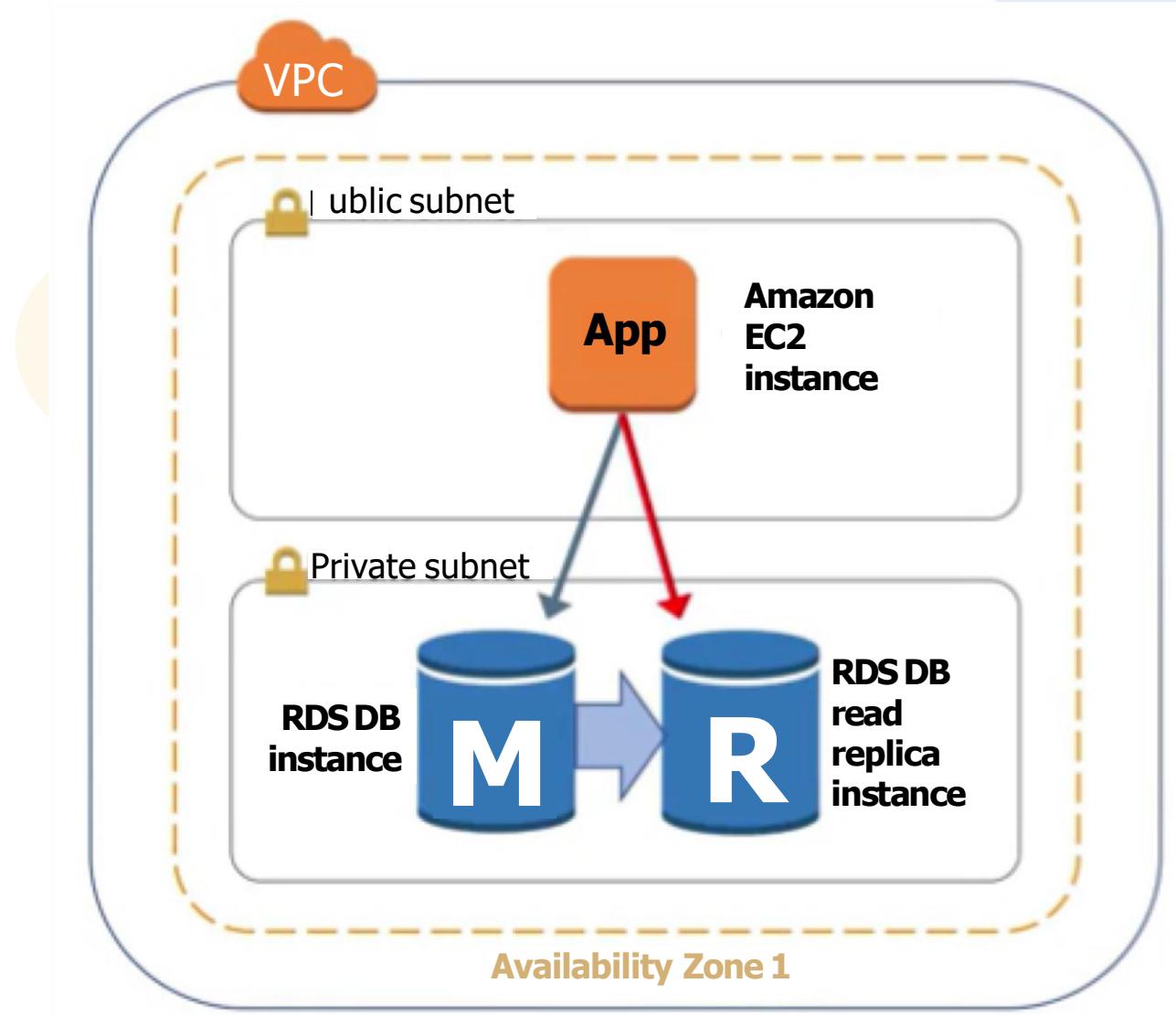


Features

- Asynchronous replication
- Promote to master if necessary

Functionality

- Read-heavy database workloads
- Offload read queries



Cases

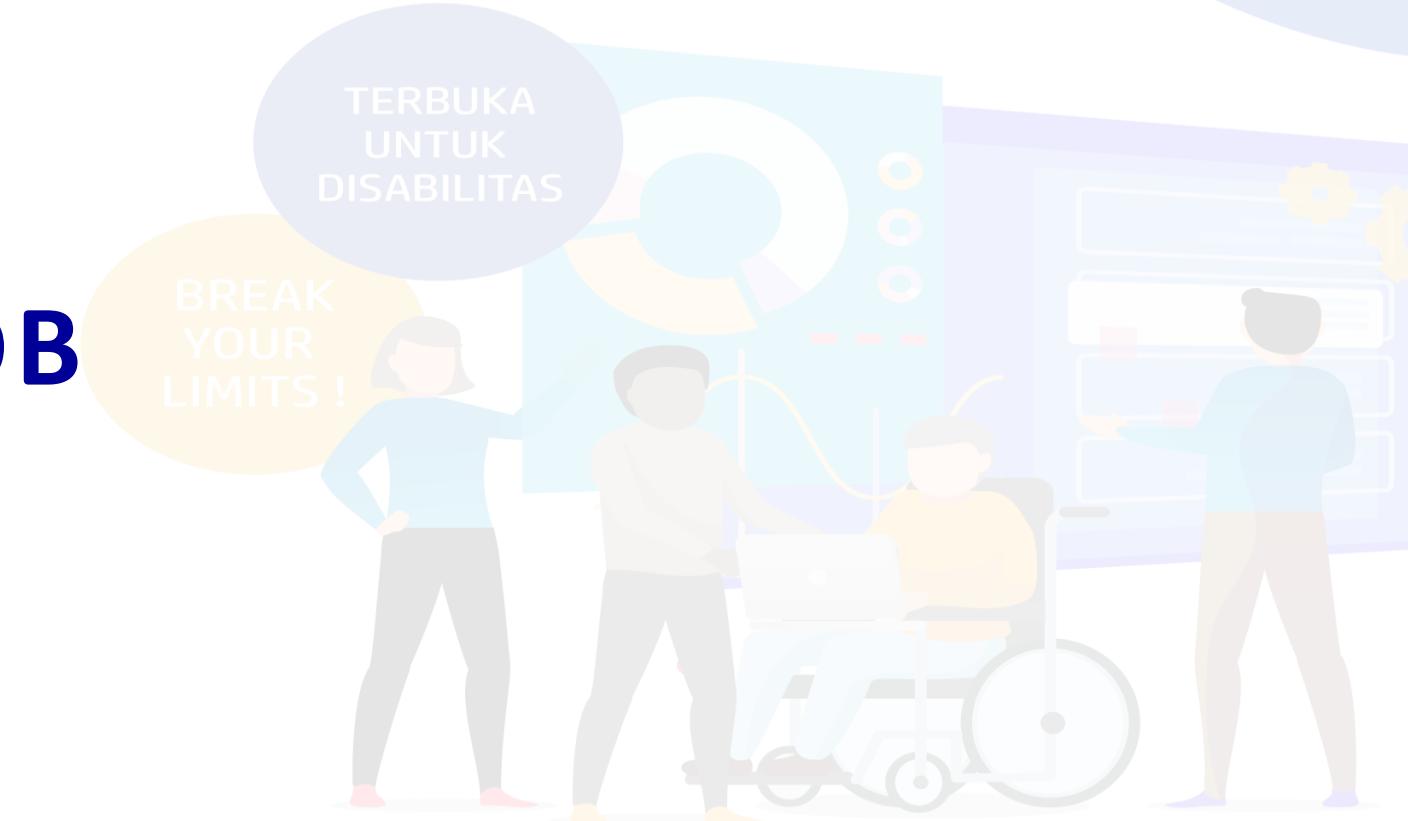
Web and Mobile Applications	ÜHigh throughput ÜMassive storage scalability ÜHigh availability
E-commerce Applications	ÜLow-cost database ÜData security ÜFully managed solution
Mobile and Online Games	ÜRapidly grow capacity ÜAutomatic scaling ÜDatabase monitoring

y

- Highly scalable
- High performance
- Easy to administer
- Available and durable
- Secure and compliant



Amazon DynamoDB



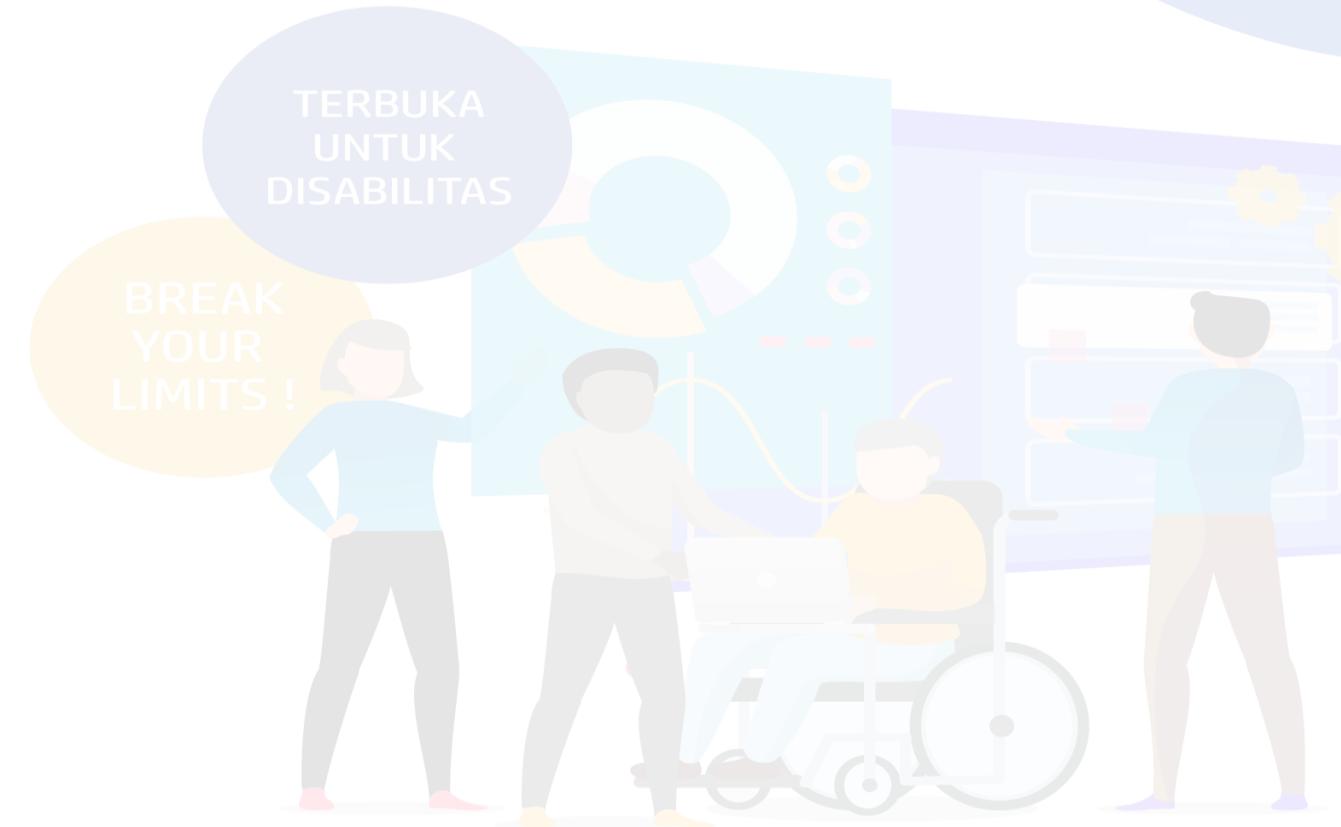
DynamoDB?

- NoSQL database tables
- Virtually unlimited storage
- Items may have differing attributes
- Low-latency queries
- Scalable read/write throughput



Cases

- Web
- Mobile apps
- Internet of Things
- Ad tech
- Gaming



g



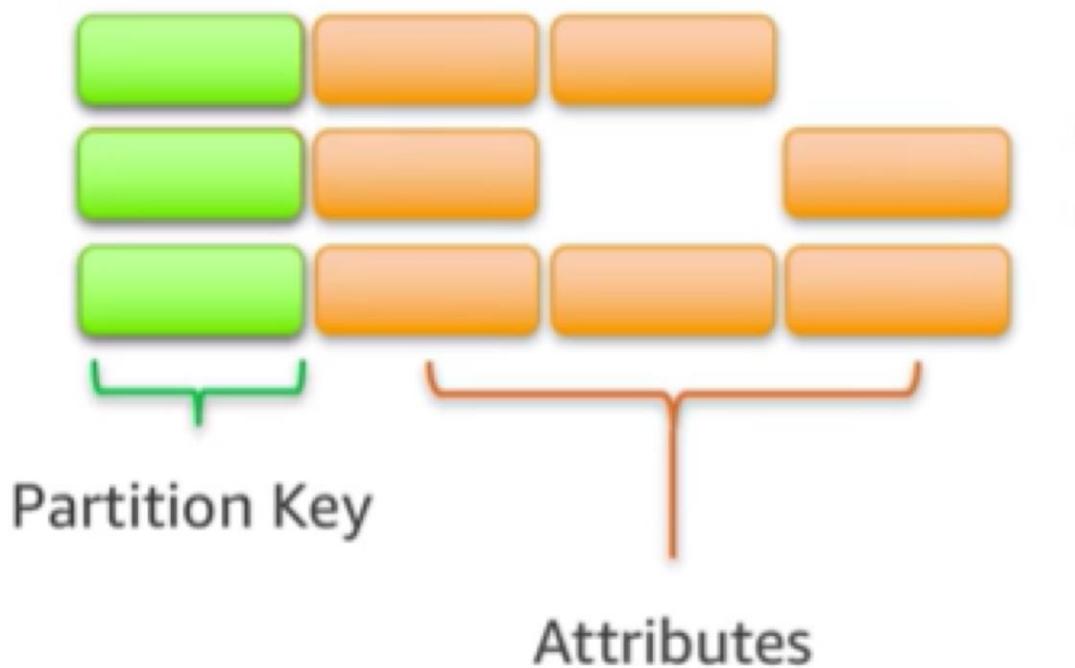
As data grows, table partitioned by key

QUERY by Key to find items efficiently
SCAN to find items by any attribute

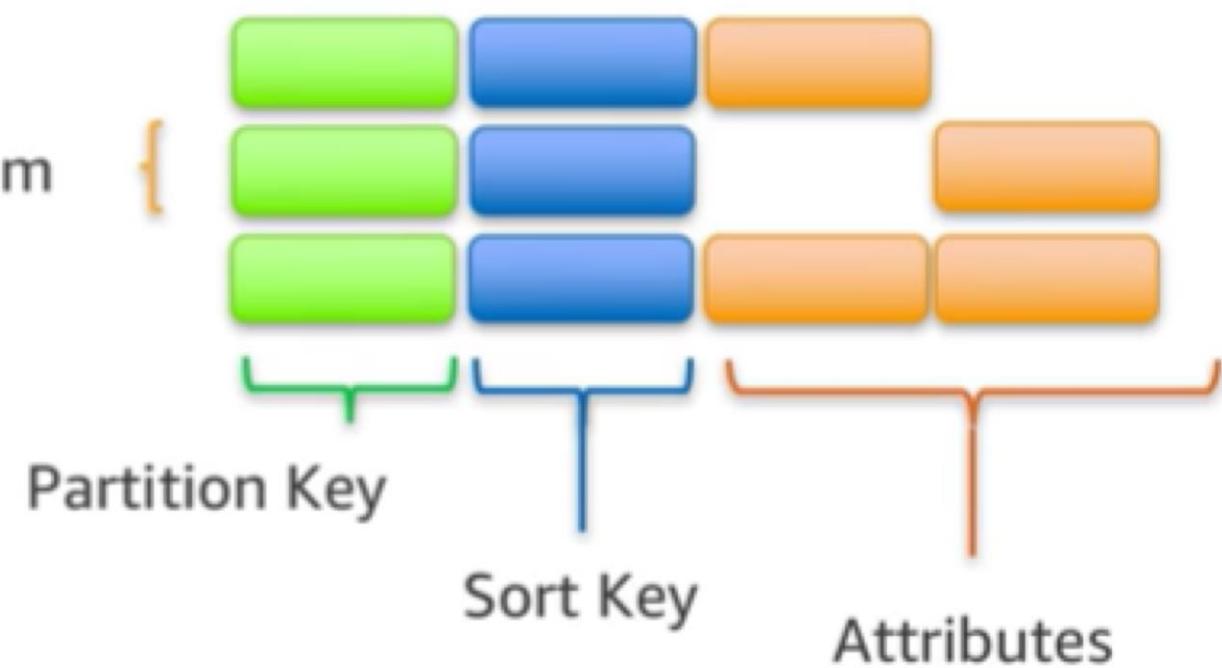
Items in a Table Must Have a Key

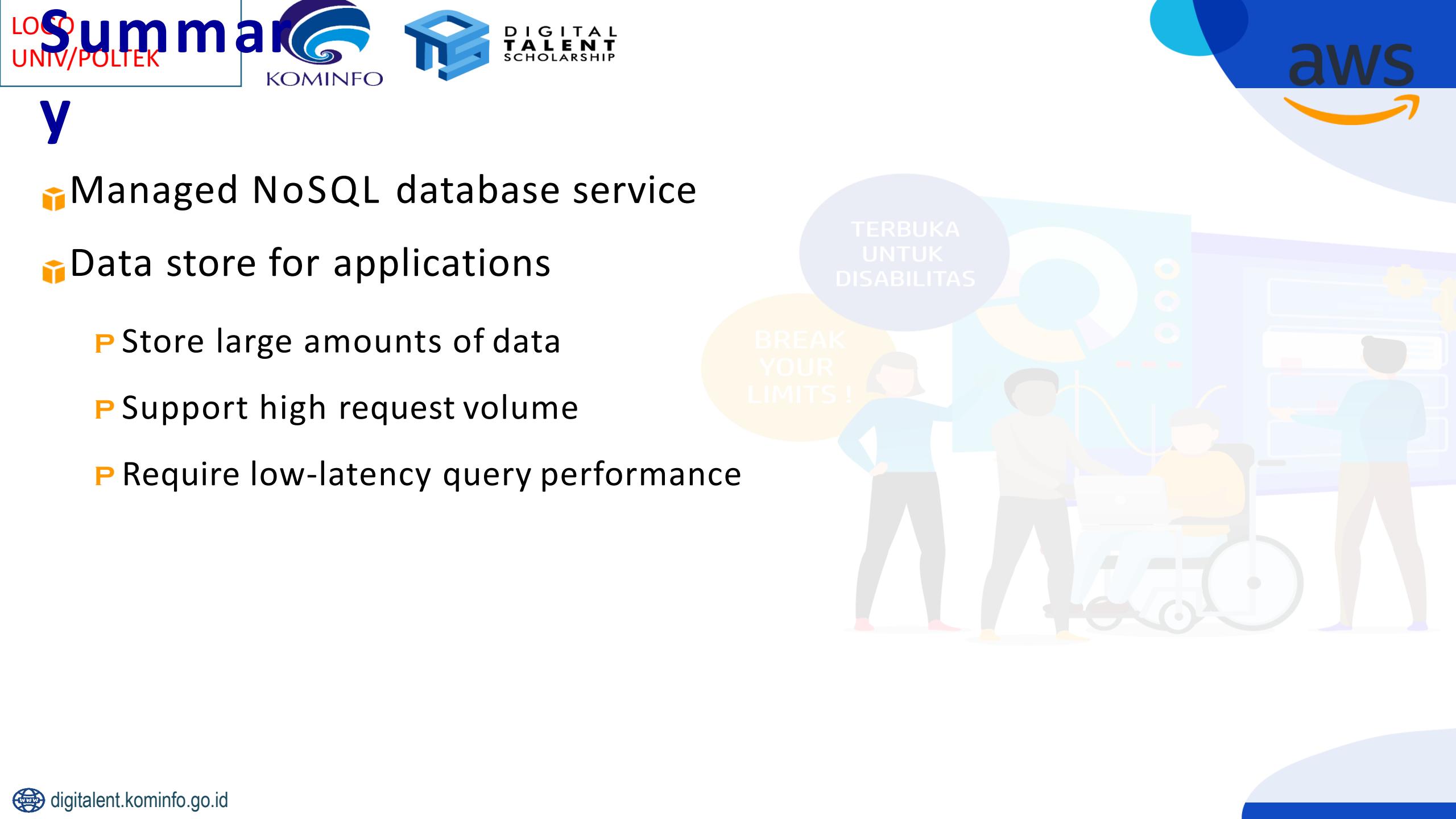


Single Key



Compound Key





y

- Managed NoSQL database service
- Data store for applications
 - ▶ Store large amounts of data
 - ▶ Support high request volume
 - ▶ Require low-latency query performance



Module 3: Security Overview

- Introduction to AWS Security
- The AWS Shared Responsibility Model
- AWS Access Control and Management
- AWS Security Compliance Programs



Introduction to AWS Security

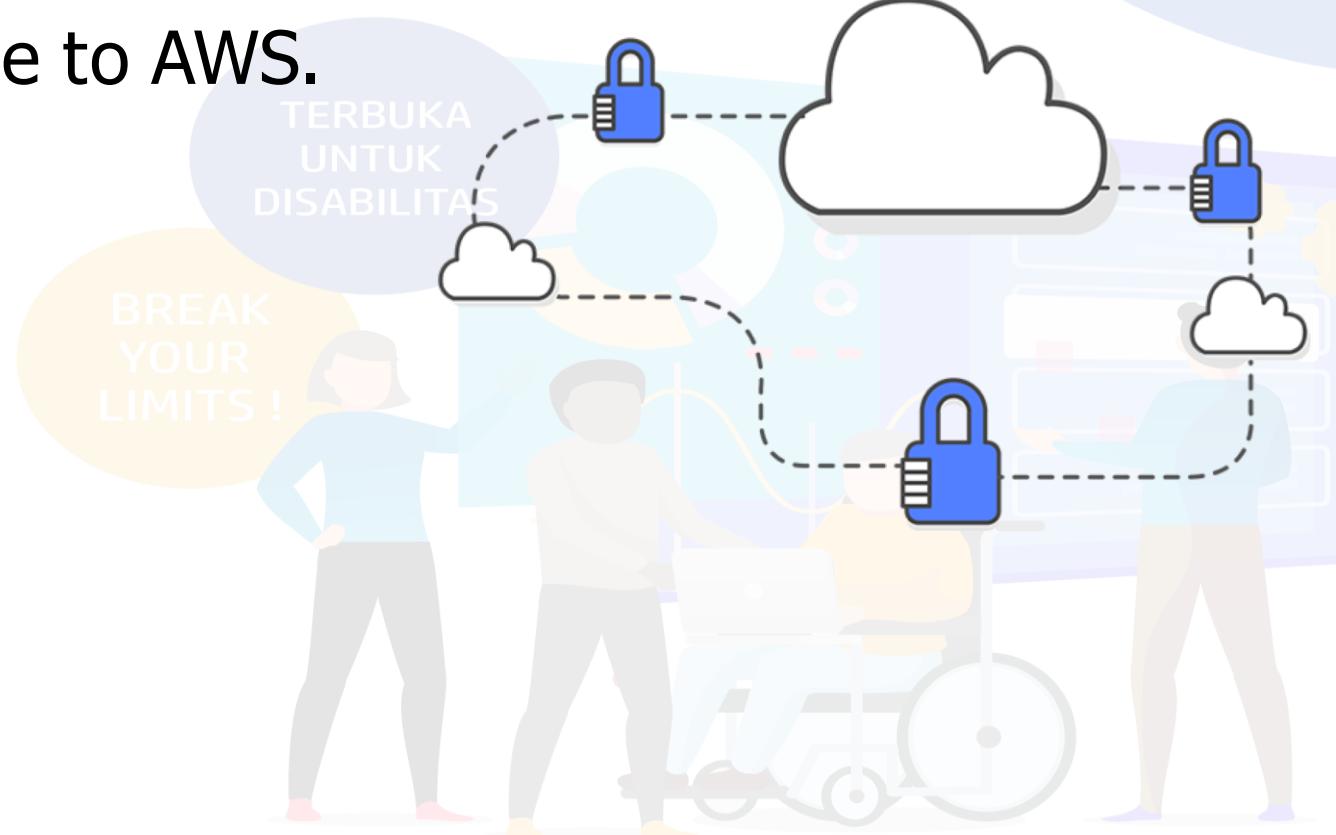
TERBUKA
UNTUK
DISABILITAS

BREAK
LIMITS

Security

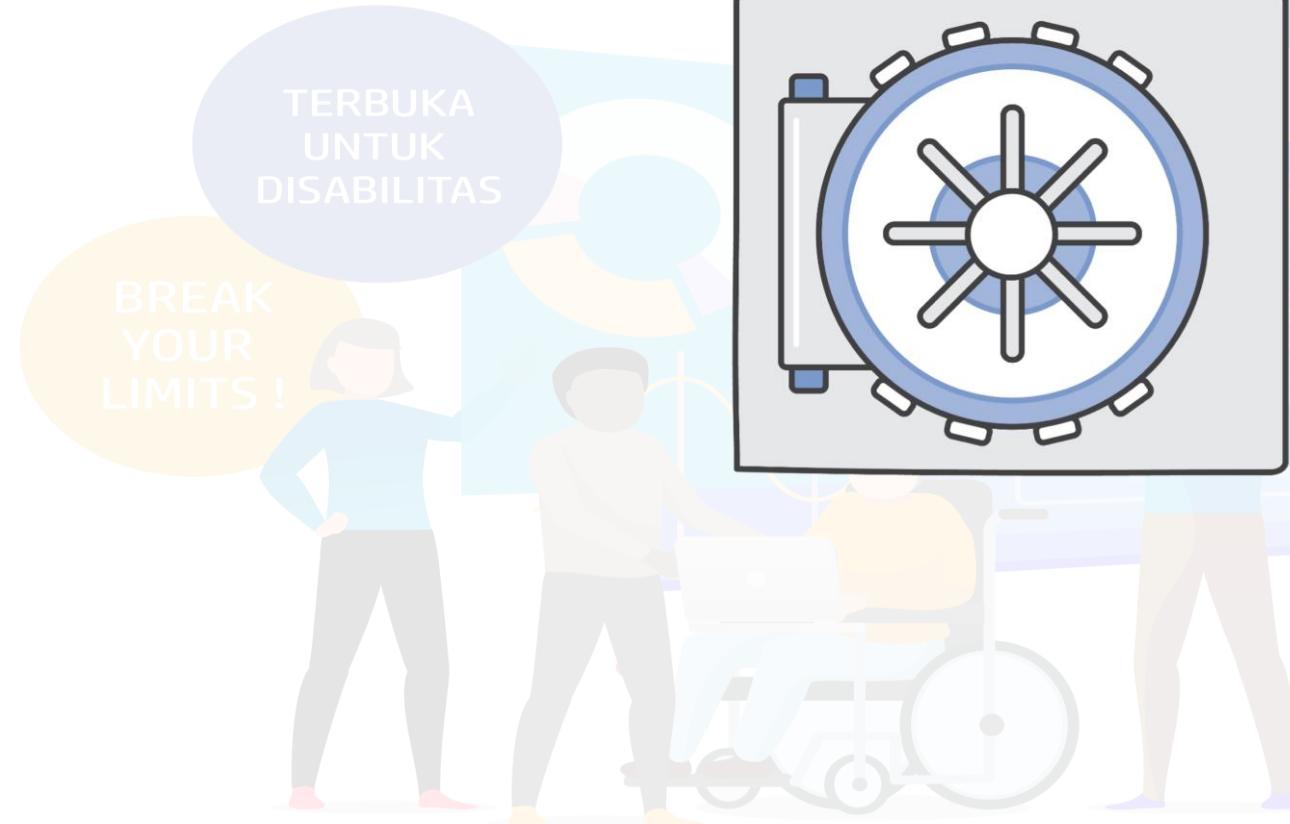
Security is of the utmost importance to AWS.

- Approach to security
- AWS environment controls
- AWS offerings and features



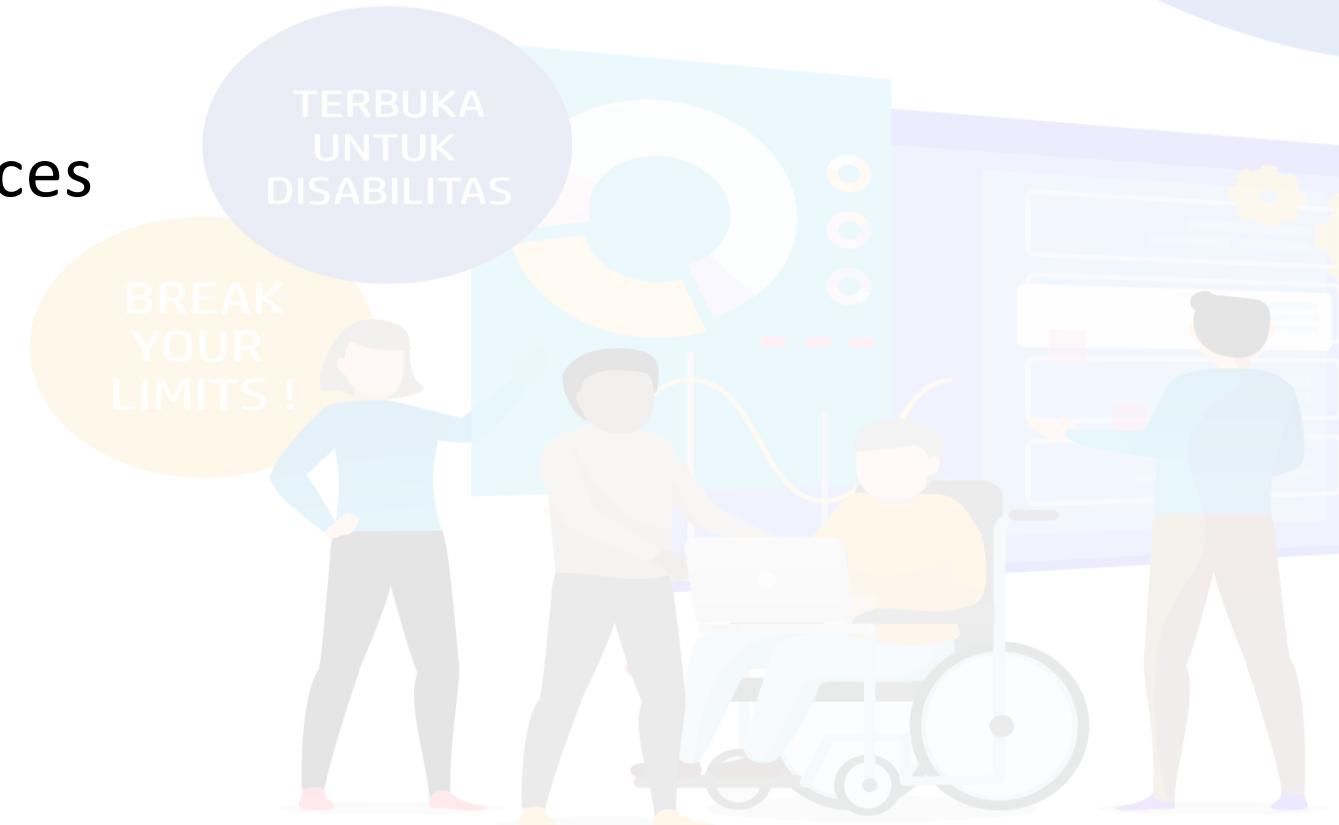
Safe

- Resilient infrastructure
- High security
- Strong safeguards



Improvement

- Rapid innovation
- Constantly evolving security services

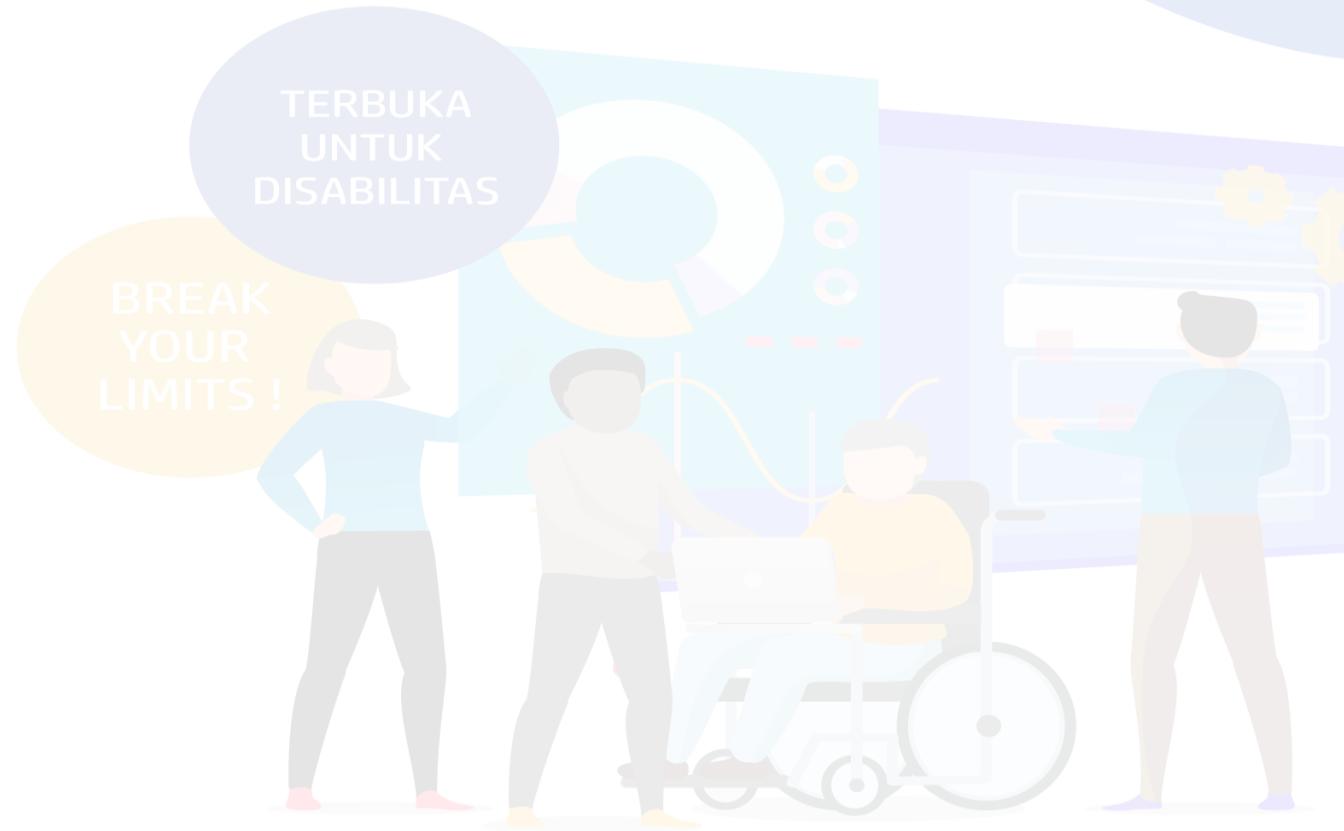




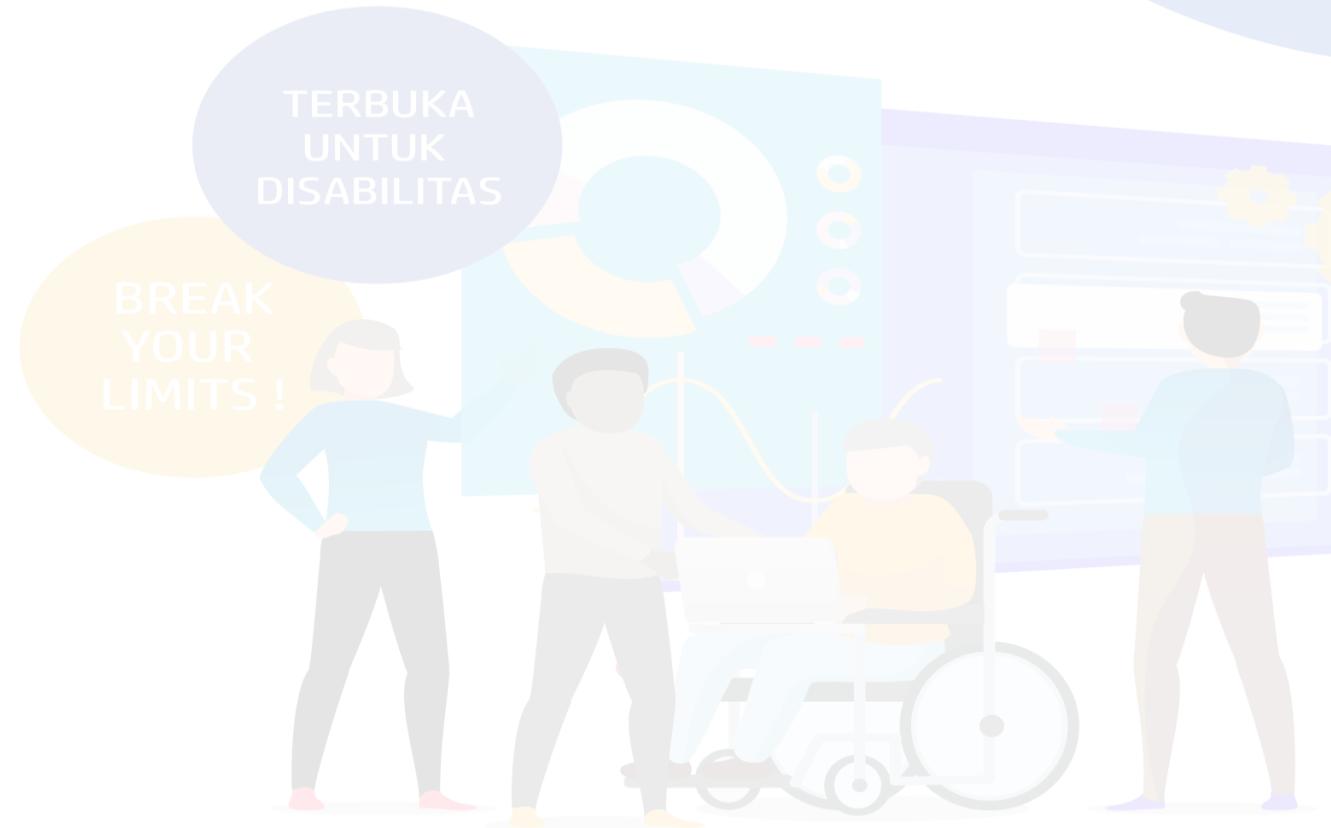
Requirements

治理功能

- P Additional oversight
- P Security control
- P Central automation



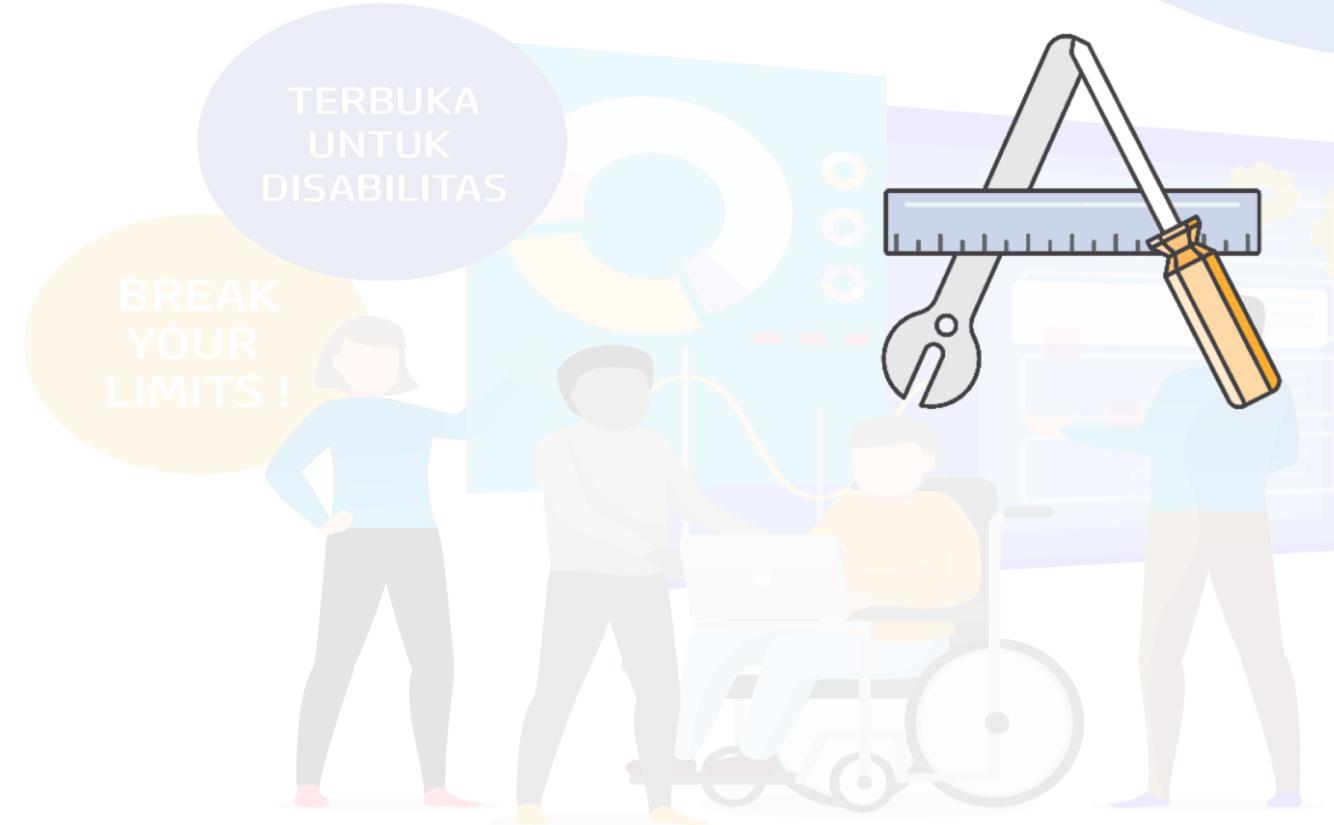
- Inherit AWS security controls
- Layer your controls



Features

Tools

- ▶ Access from AWS and partners
- ▶ Use for monitoring and logging



Security

- Built-in firewalls
- Encryption in transit
- Private/dedicated connections
- Distributed denial of service (DDoS) mitigation



LOGO
UNIV/POLTEK

Inventory and Configuration
Management

KOMINFO

2020-2021
SCHOLARSHIP

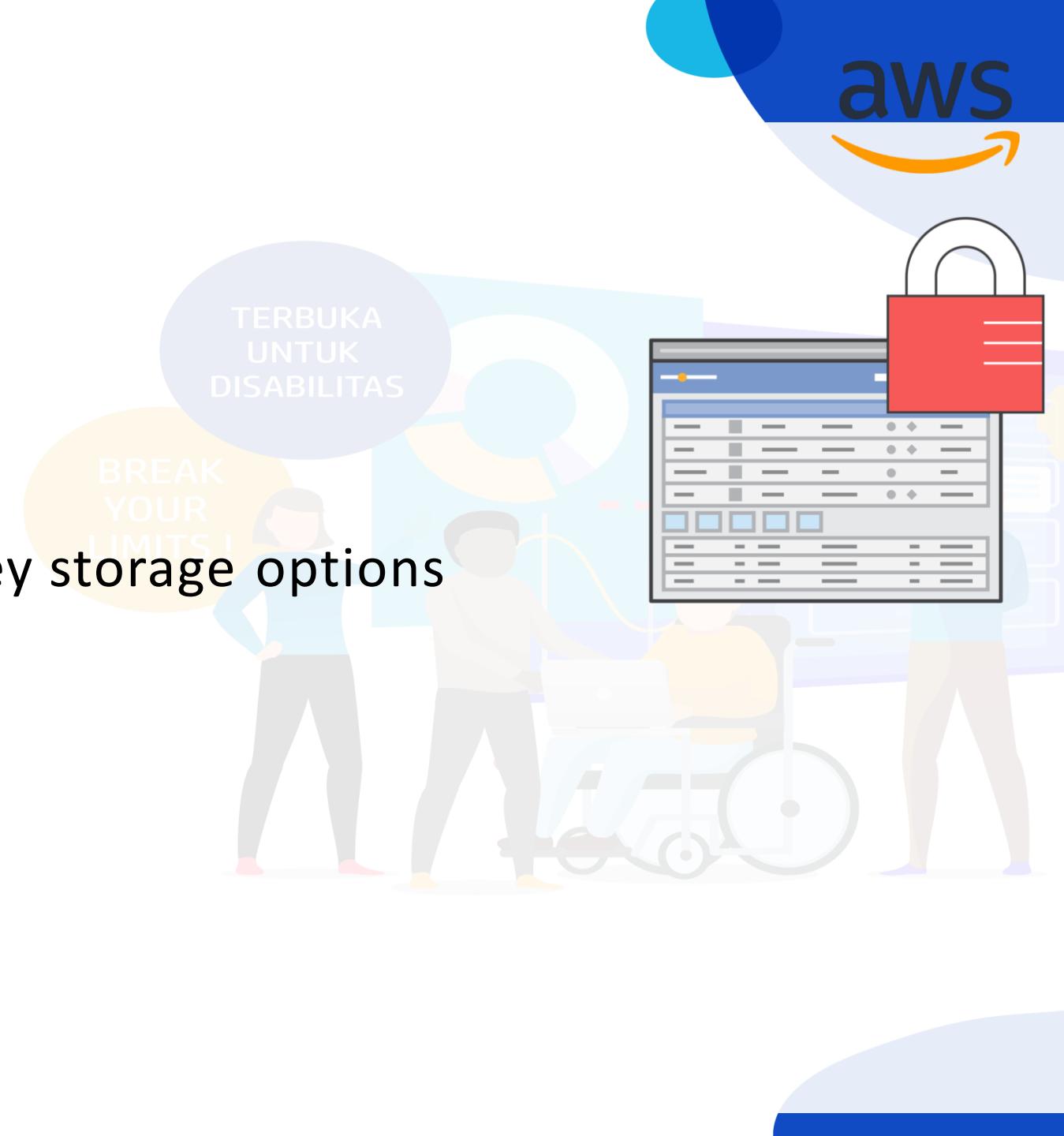
aws

- Deployment tools
- Inventory and configuration tools
- Template definition and management tools



Encryption

- Encryption capabilities
- Key management options
 - AWS Key Management Service
- Hardware-based cryptographic key storage options
 - AWS CloudHSM



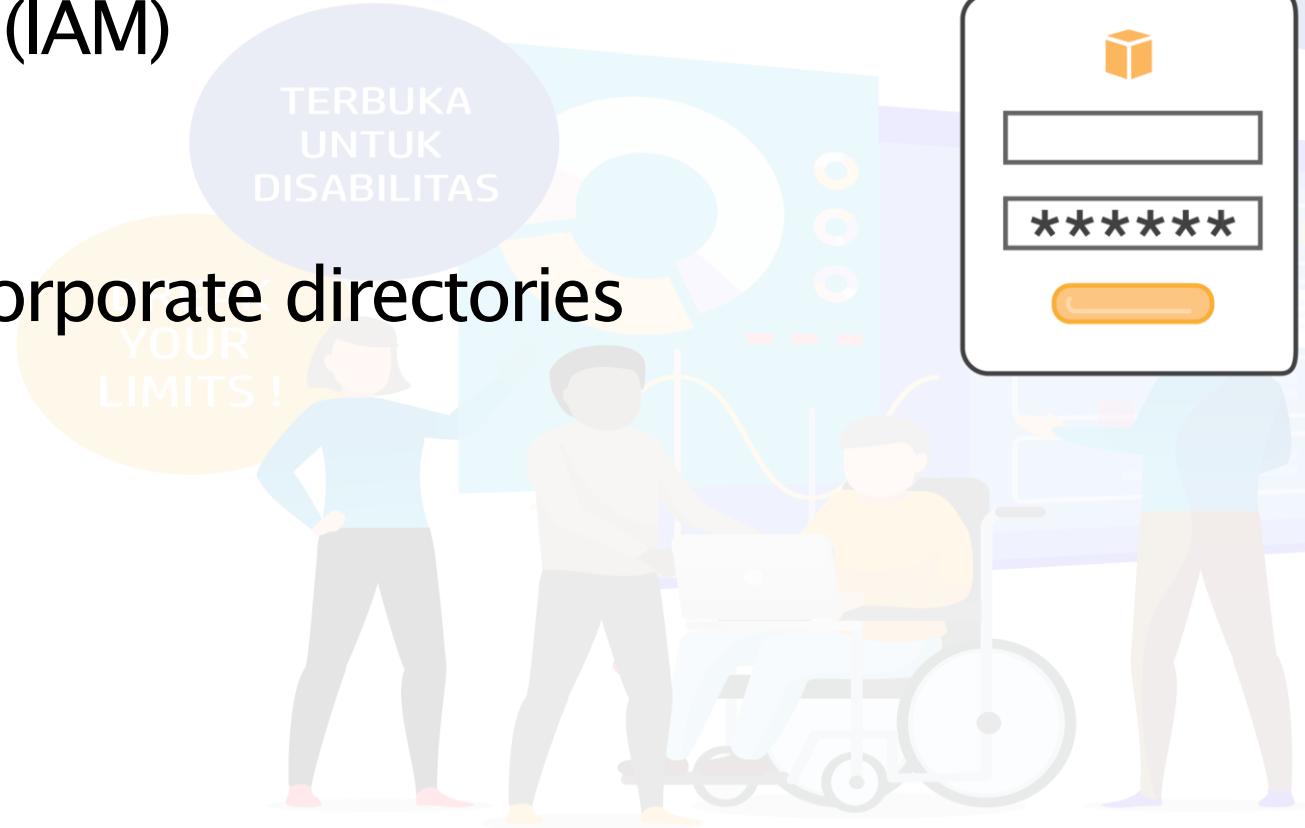
LOGO
UNIV/POITEK

DIGITAL
TALENT
SCHOLARSHIP

Access Control and Management



- Identity and Access Management (IAM)
- Multi-factor authentication (MFA)
- Integration and federation with corporate directories
- Amazon Cognito
- AWS Single Sign-On

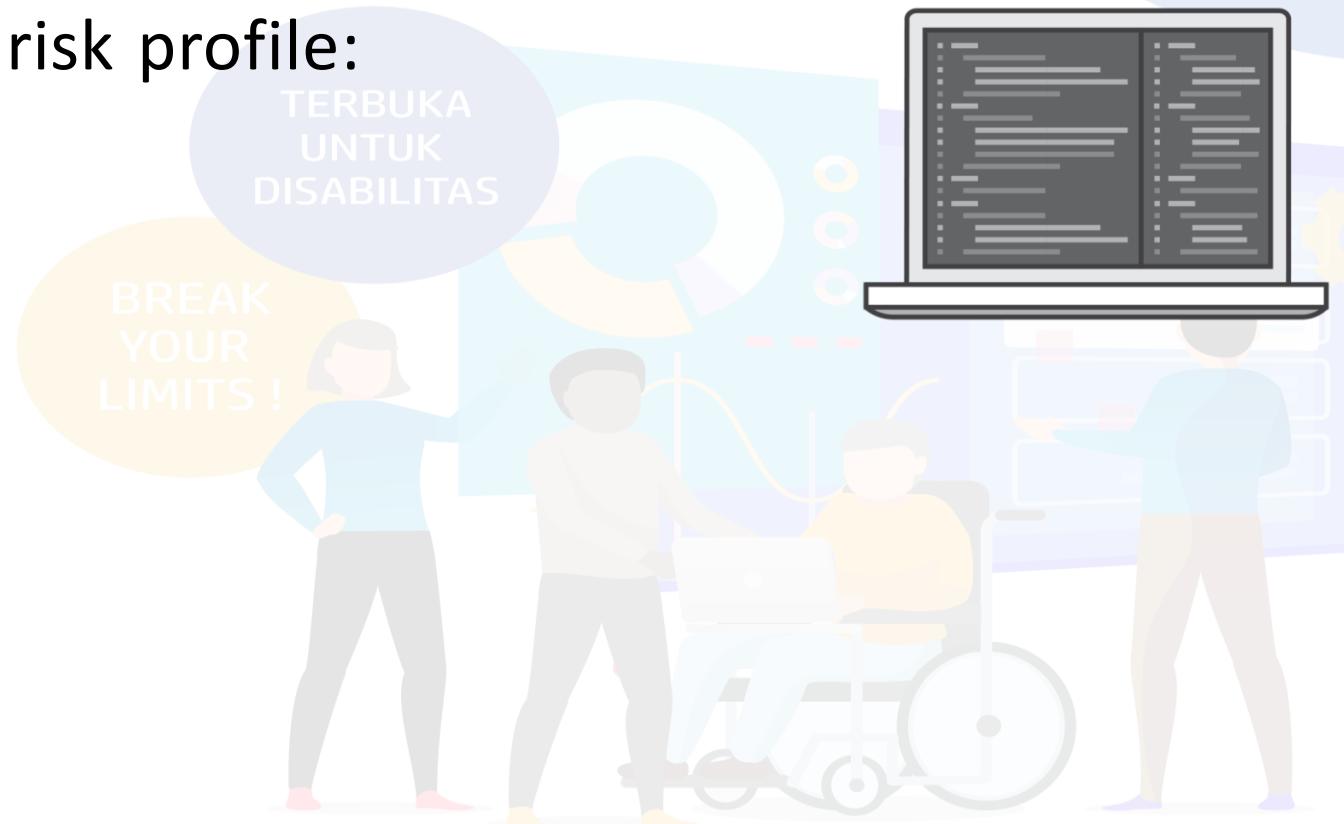




Logging

Tools and features to reduce your risk profile:

- ▶ Deep visibility into API calls
- ▶ Log aggregation and options
- ▶ Alert notifications





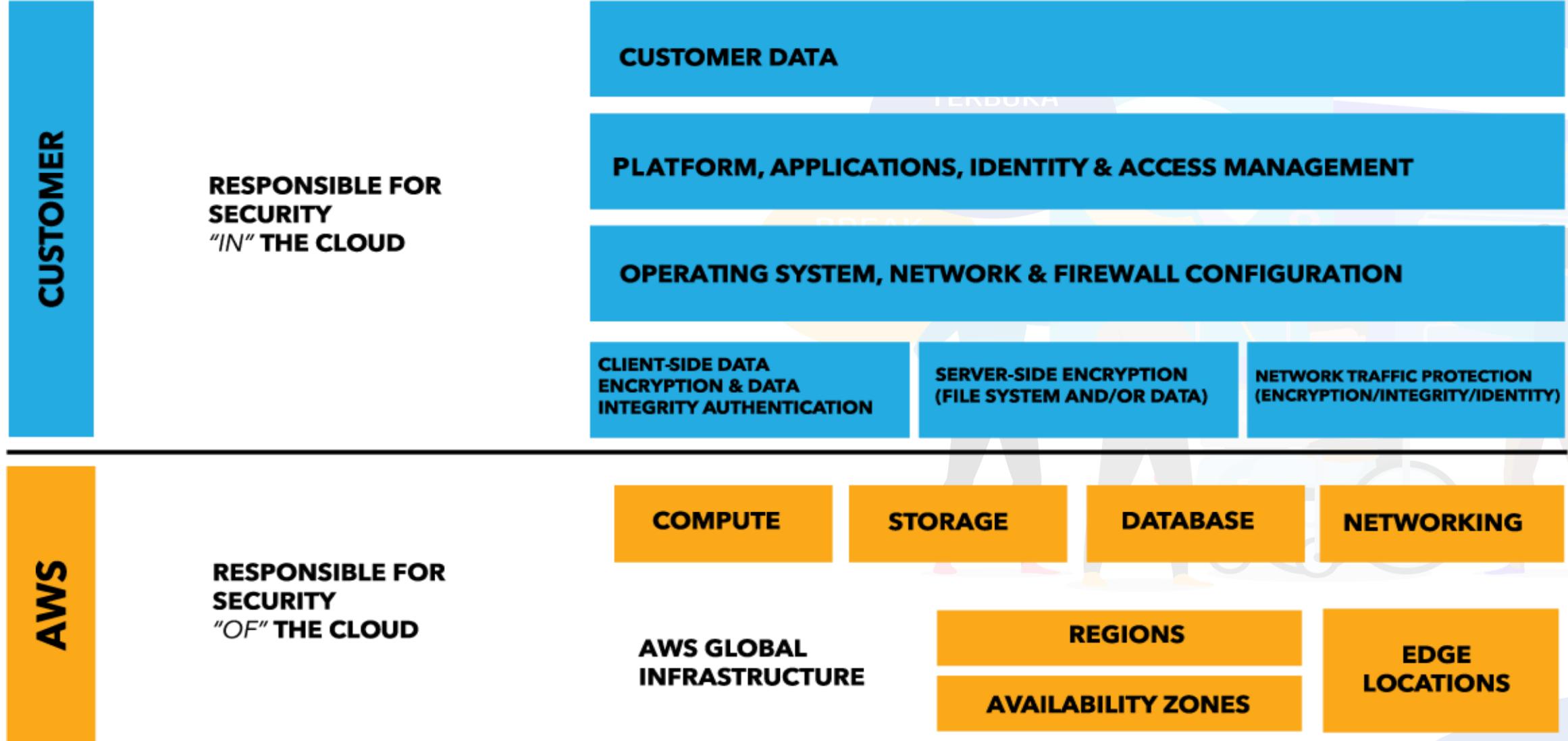
- Qualified partners to market/sell software to AWS customers
- Online software store that can run on AWS



The AWS Shared Responsibility Model



Model



Security of the Cloud



AWS

**RESPONSIBLE FOR
SECURITY
"OF" THE CLOUD**



- Protection of the AWS global infrastructure is top priority
- Availability of third-party reports

Cloud

- AWS Foundation Services

cube icon Amazon EC2

cube icon Amazon EBS

- Managed Services

cube icon Amazon DynamoDB

cube icon Amazon RDS

cube icon Amazon Redshift

cube icon Amazon EMR

cube icon Amazon WorkSpaces

Cloud

Inherited Controls

P Physical

P Environmental

Shared Controls

P Patch Management

P Configuration Management

P Awareness and Training

Customer Specific

P Service/Communication Protection

P Zone Security

Cloud

CUSTOMER

**RESPONSIBLE FOR
SECURITY
"IN" THE CLOUD**

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

**CLIENT-SIDE DATA
ENCRYPTION & DATA
INTEGRITY AUTHENTICATION**

**SERVER-SIDE ENCRYPTION
(FILE SYSTEM AND/OR DATA)**

**NETWORK TRAFFIC PROTECTION
(ENCRYPTION/INTEGRITY/IDENTITY)**

- ─ What to store
- ─ Which AWS services
- ─ In what location

- ─ In what content format and structure
- ─ Who has access

CUSTOMER

RESPONSIBLE FOR
SECURITY
"IN" THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA
ENCRYPTION & DATA
INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION
(FILE SYSTEM AND/OR DATA)

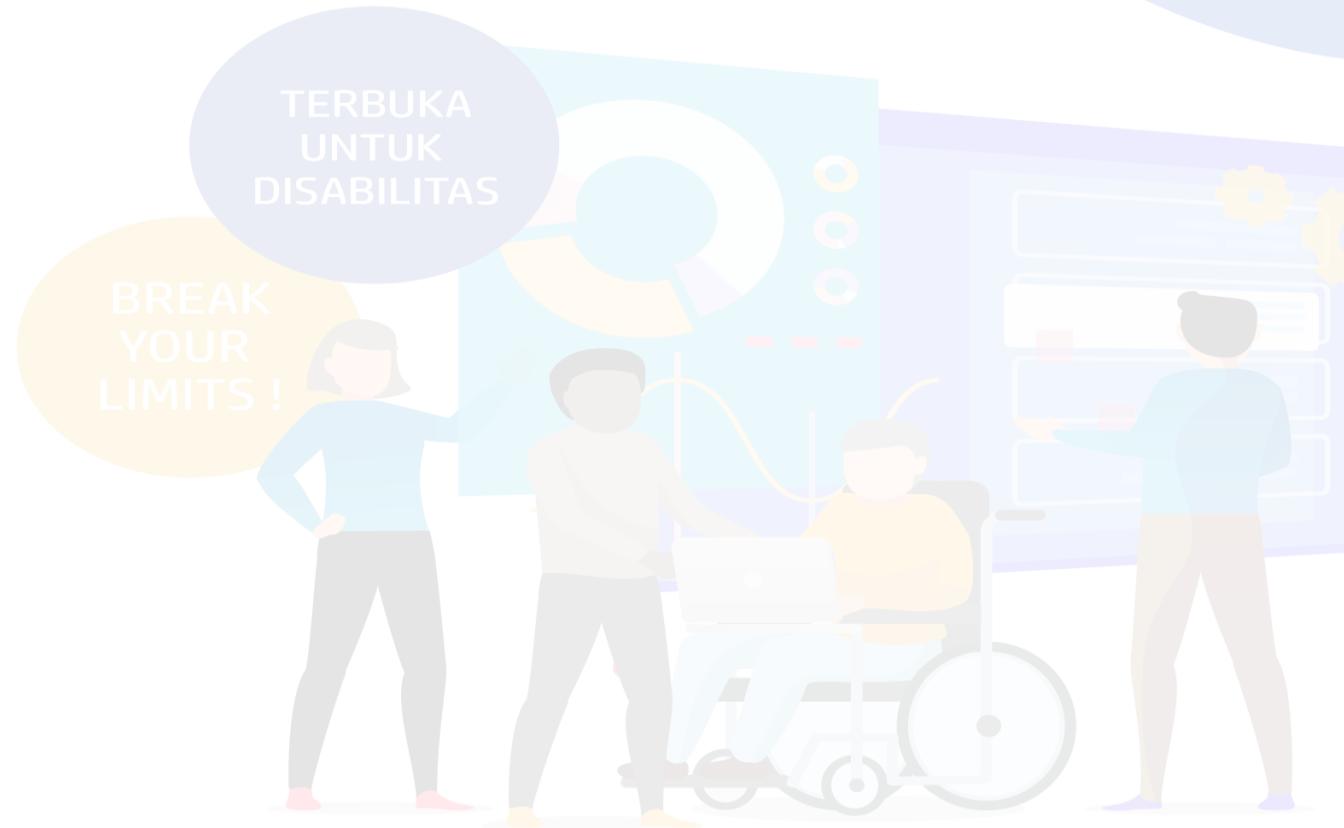
NETWORK TRAFFIC PROTECTION
(ENCRYPTION/INTEGRITY/IDENTITY)

- Customers retain control
- Changes to model depend on services

Cloud

AWS Service Catalog

- Virtual Machine Images
- Servers
- Software
- Databases



Cloud

Benefits

- Centrally manage common IT services
- Achieve consistent governance
- Meet compliance requirements
- Quickly deploy approved IT services

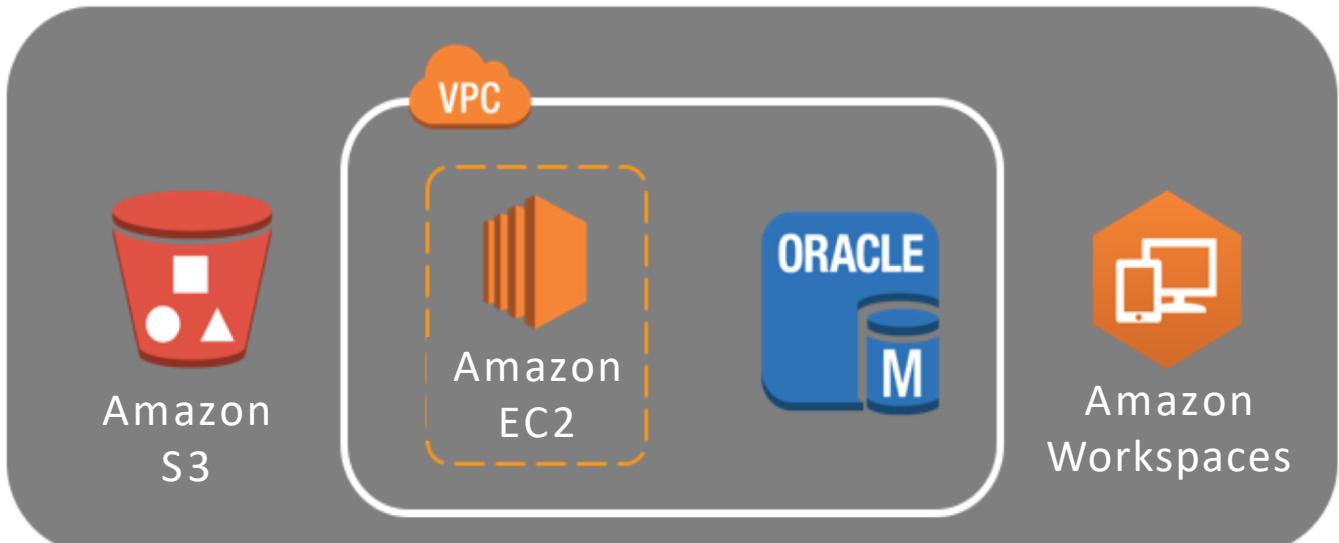


e

Customer

AWS

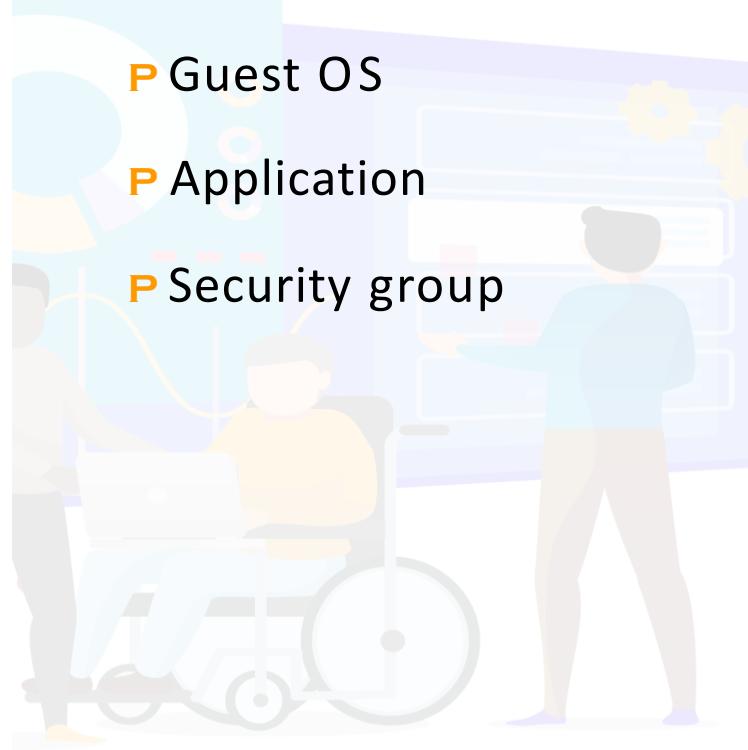
Accounts and Credentials



AWS Global Infrastructure

Customer Responsibility:

- Guest OS
- Application
- Security group



y

■ AWS and the customer share security responsibilities

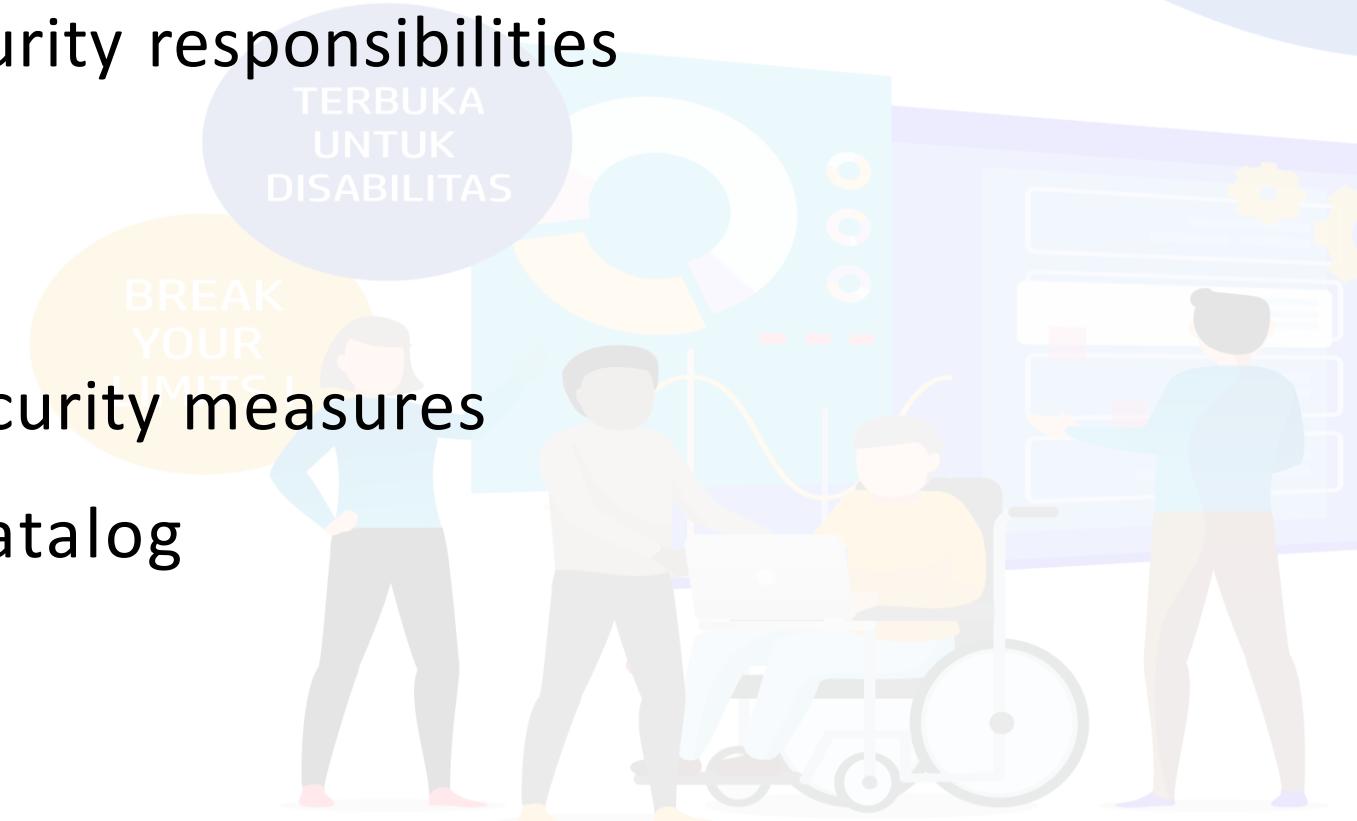
P AWS: Security of the cloud

P Customer: Security in the cloud

■ Customer has full control over security measures

■ Customer can use AWS Service Catalog

■ “Infrastructure” Service



AWS Access Control and Management



IAM

Control access to AWS resources

Authentication

Authorization

Controls access to services such as:

Compute

Storage

Database

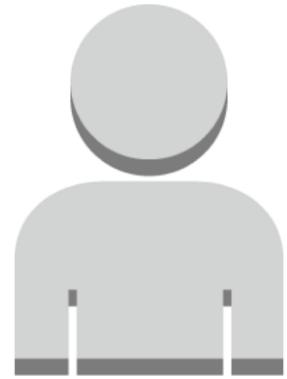
Application services



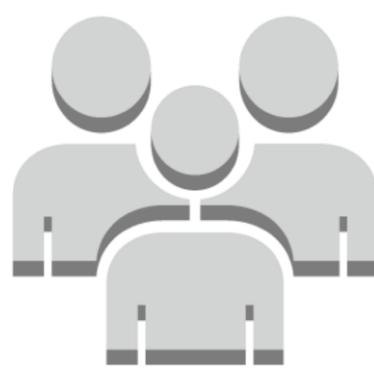
IAM

>Create users and groups

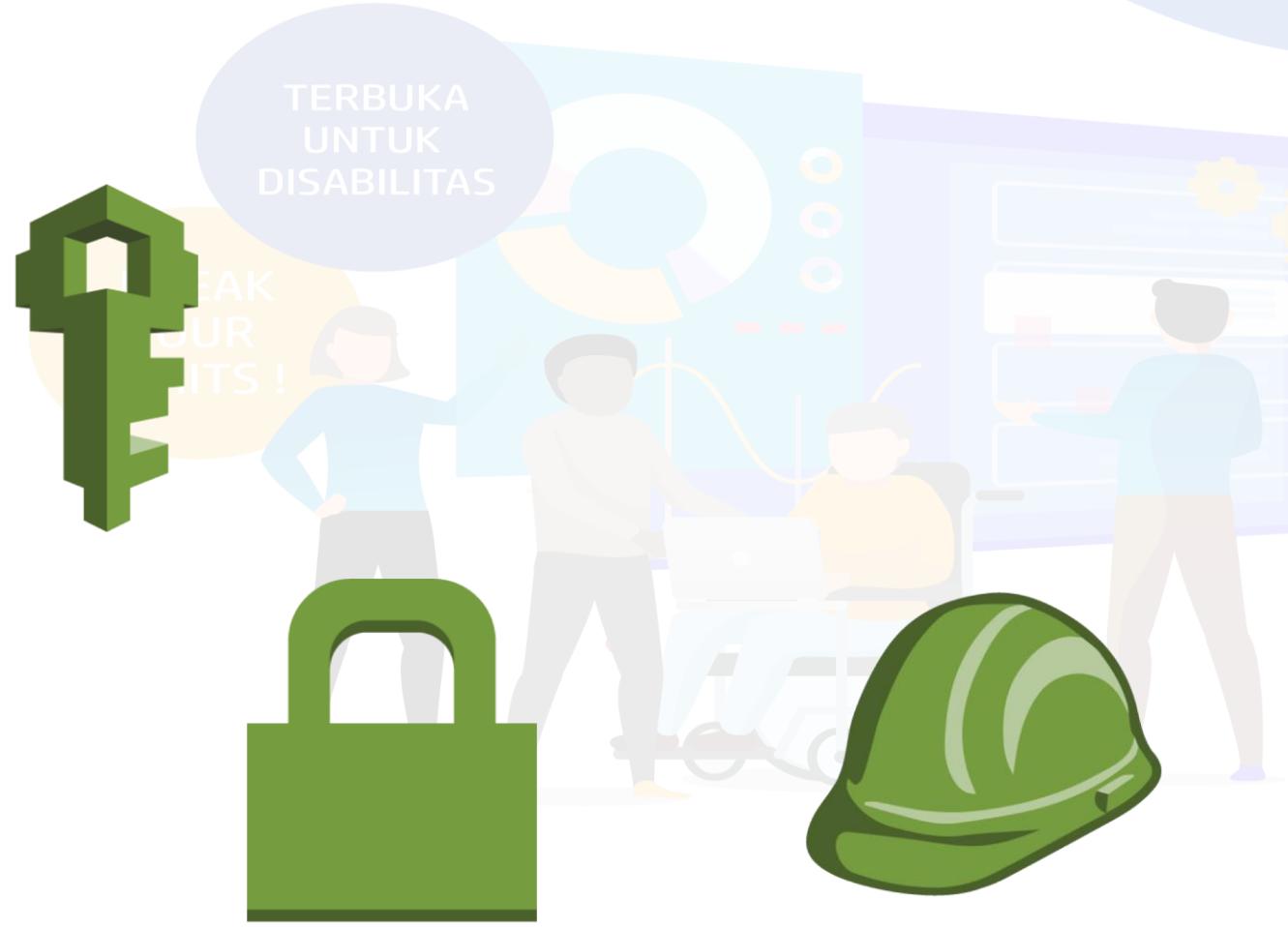
Grant permissions



User



Group



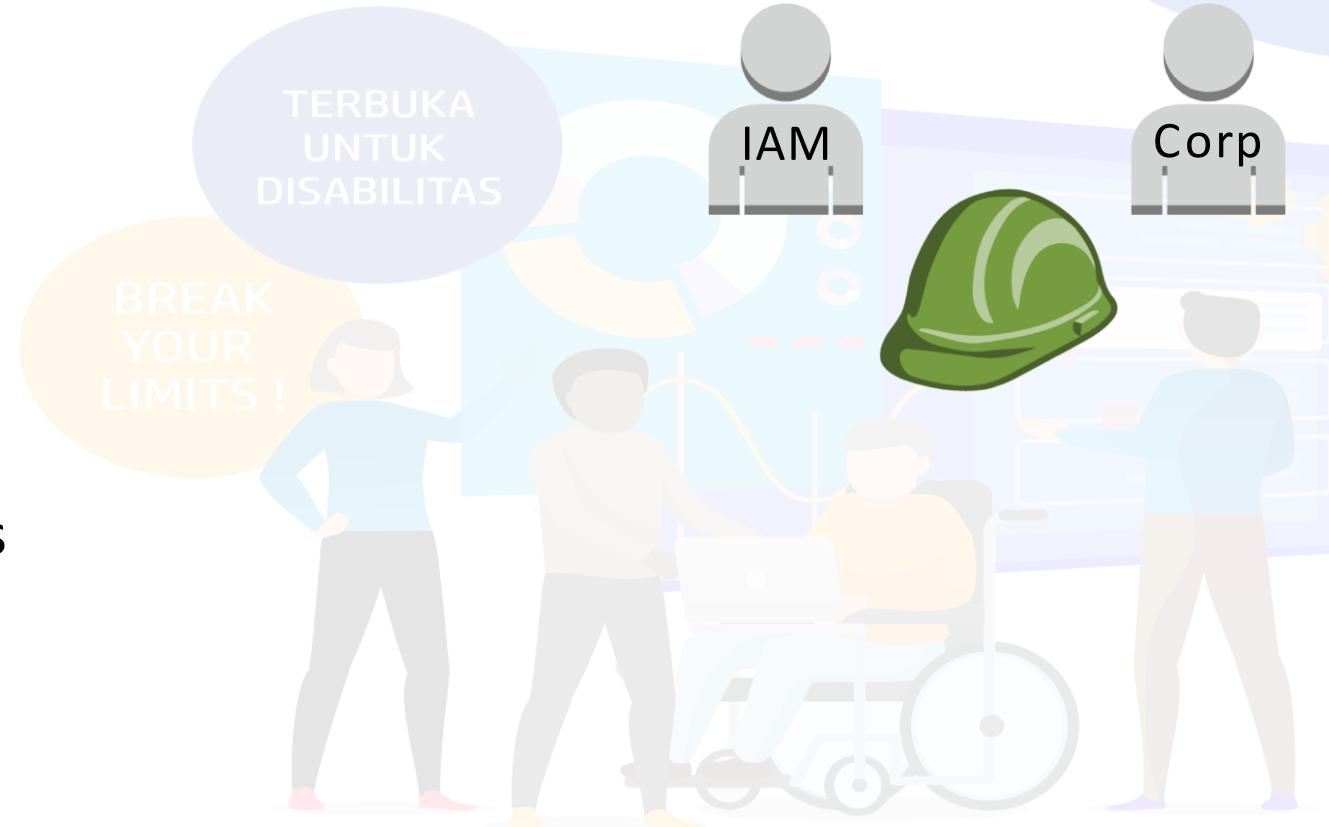
AWS IAM



Functionality

Manage

- ▶ Users and their access
- ▶ Roles and their permissions
- ▶ Federate users and their permissions



User

Account root user has complete access to all AWS Services.

Create an AWS account

Email address

Password

Confirm password

AWS account name i

Continue

[Sign in to an existing AWS account](#)

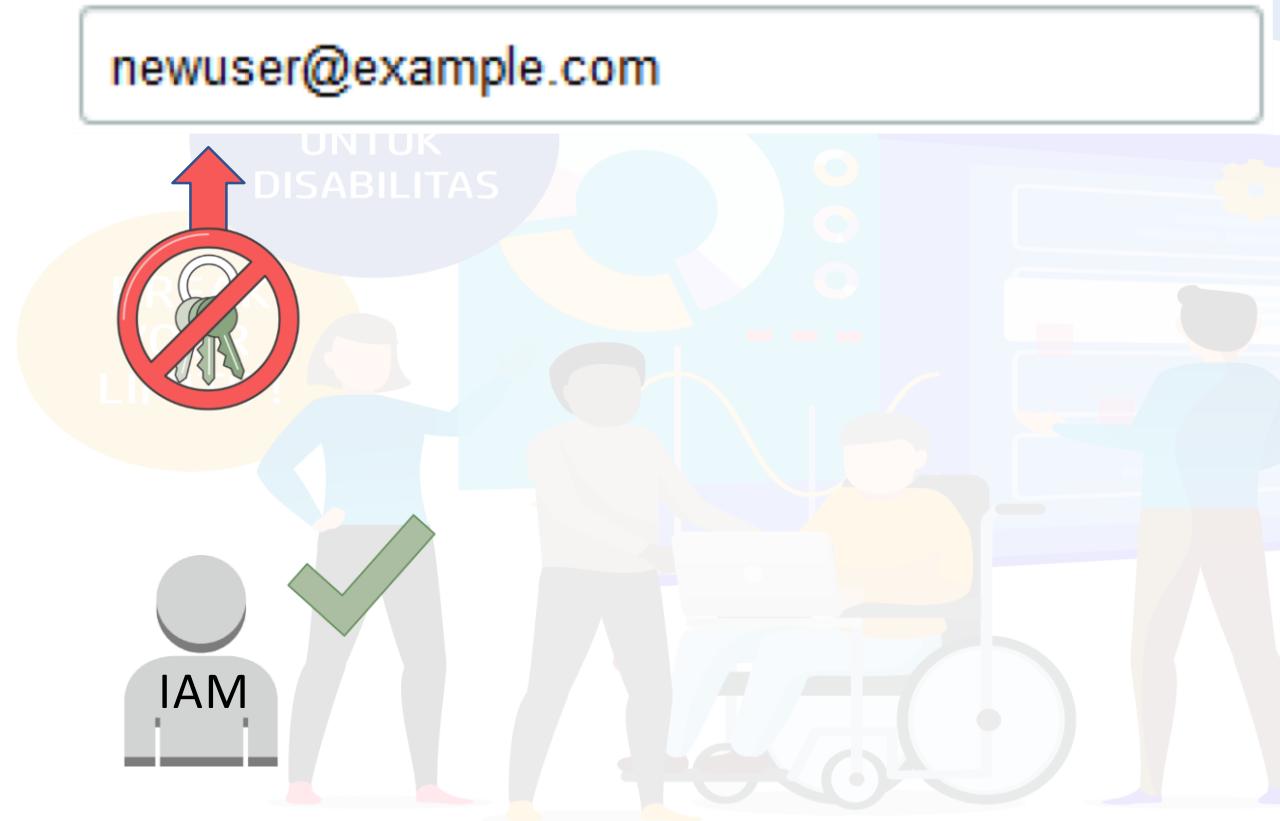
© 2018 Amazon Web Services, Inc. or its affiliates.
All rights reserved.

[Privacy Policy](#) | [Terms of Use](#)

User

Recommendations

1. Delete root user access keys.
2. Create an IAM user.
3. Grant administrator access.
4. Use IAM credentials to interact with AWS.



Authentication

Programmatic access

- P Enables access key ID and secret access key

Management console access

- P Uses AWS account name and password
- P MFA prompts for code

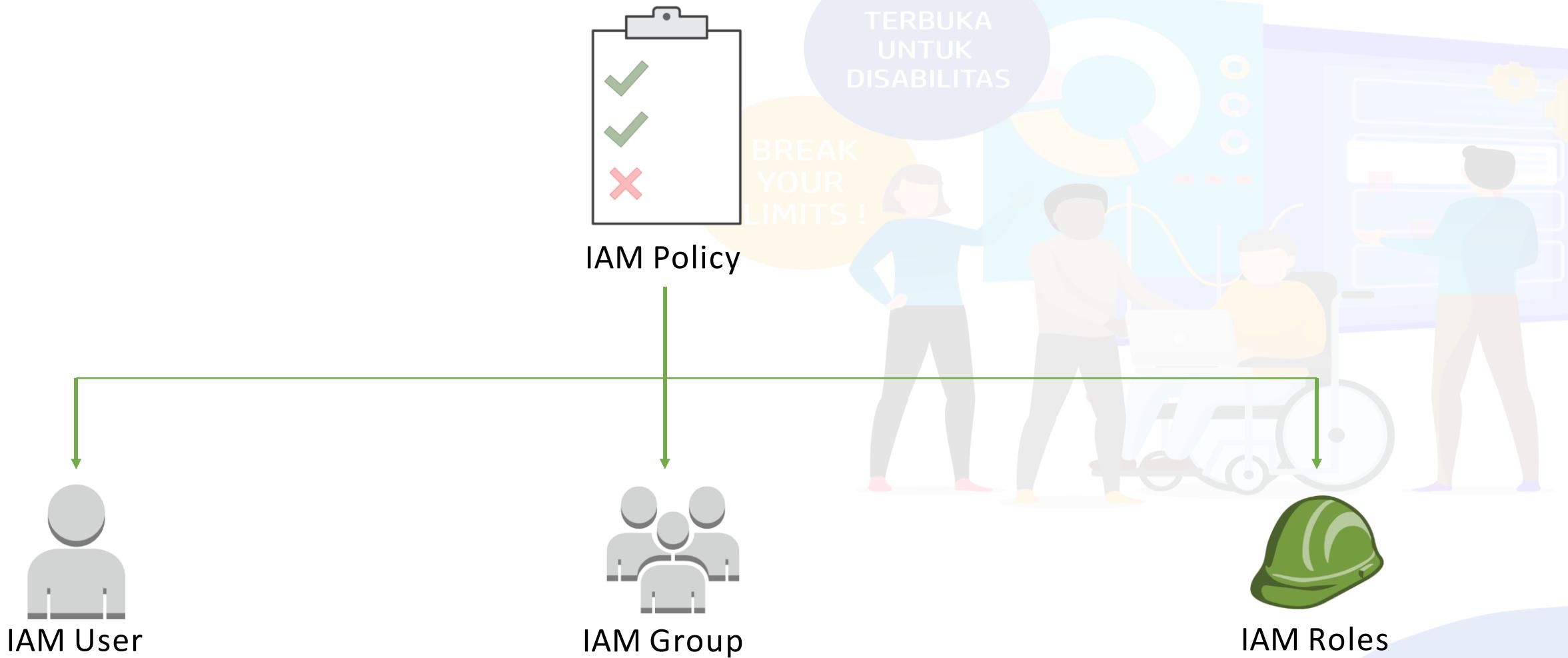


Authorization

- Access AWS services
- P Grant authorization
- Assign permissions
- P Create an AWS IAM policy



Assignment



Practices

- Delete AWS root account access keys
- Activate multi-factor authentication (MFA)
- Give IAM users only the permissions they must have
- Use IAM groups
- Apply an IAM password policy



Practices

(Roles)

- P Use roles for applications
- P Use roles instead of sharing credentials

(Credentials)

- P Rotate credentials regularly
- P Remove unnecessary users and credentials

(Use policy conditions for extra security)

(Monitor activity in your AWS account)



AWS Security Compliance Programs



Overview



- AWS compliance approach
- AWS risk and compliance programs
- AWS customer compliance responsibilities



Approach

- AWS and customers share control

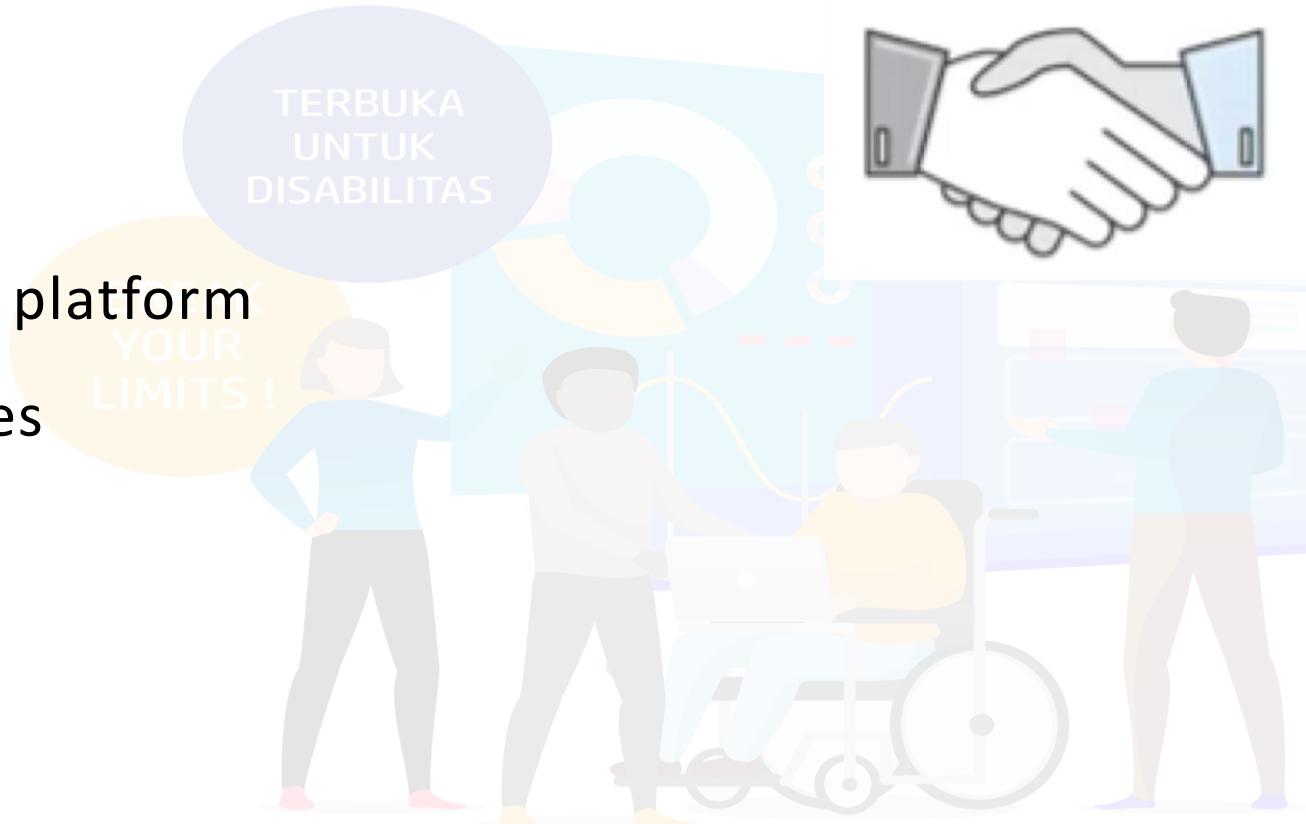
- AWS responsibility

- ▶ Provide highly secure and controlled platform

- ▶ Provide wide array of security features

- Customers responsibility

- ▶ Configure IT



AWS Security Information



AWS shares security information by

- Obtaining industry certifications
- Publishing security and control practices
- Compliance report directly under NDA

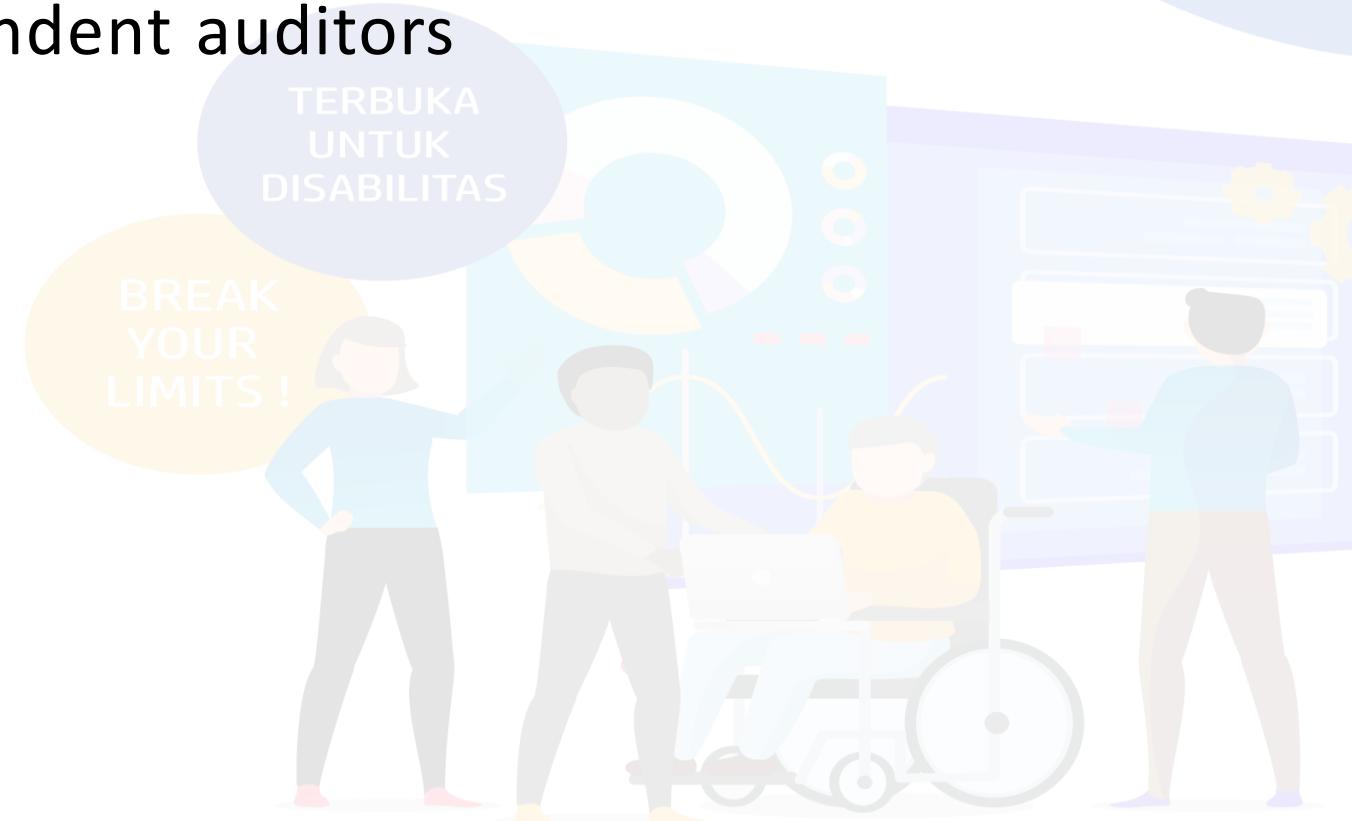


Programs

AWS, certifying bodies, and independent auditors

Provide:

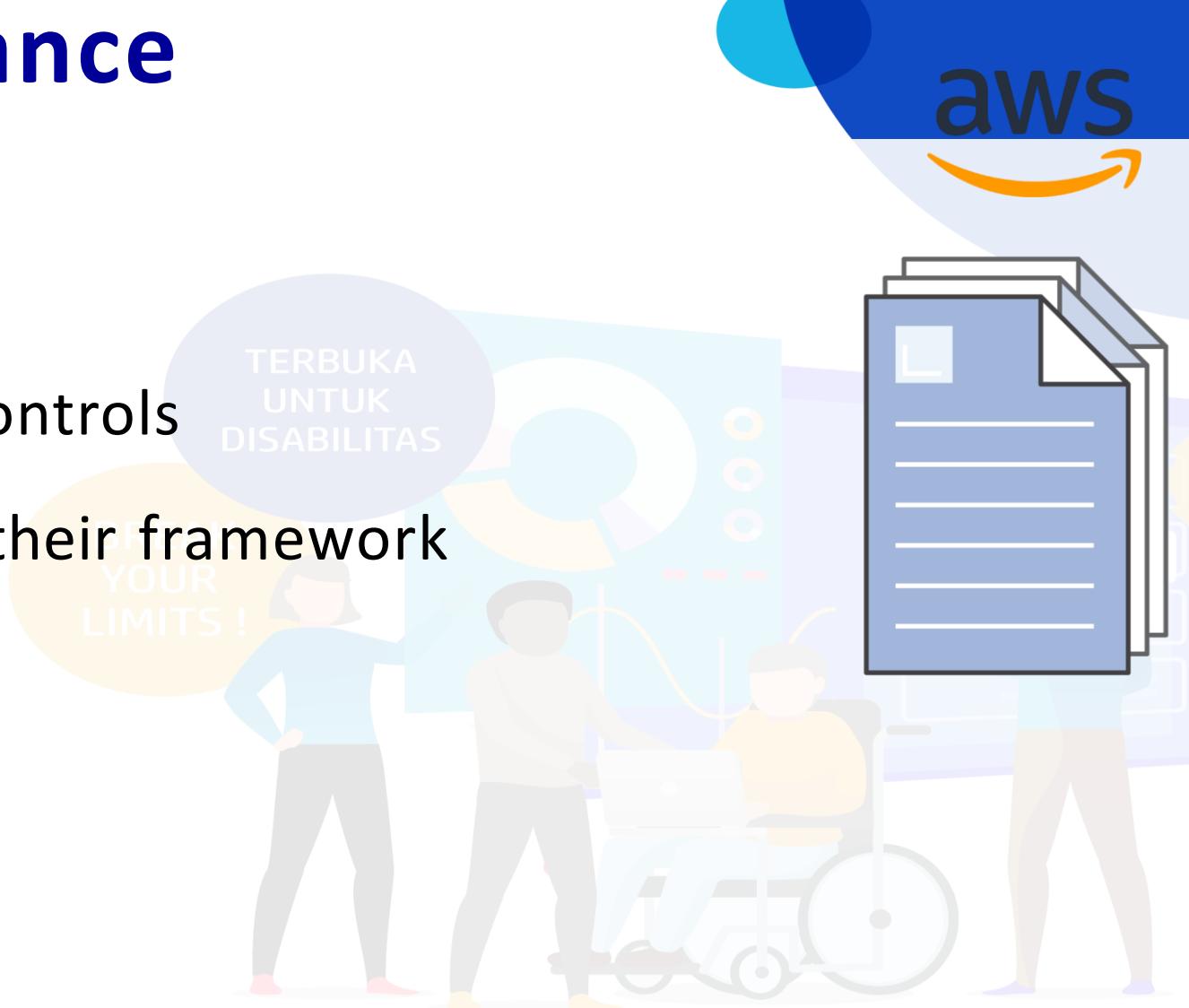
- Certifications and attestations
- Laws, regulations, and privacy
- Alignments and frameworks



Programs

AWS risk and compliance programs

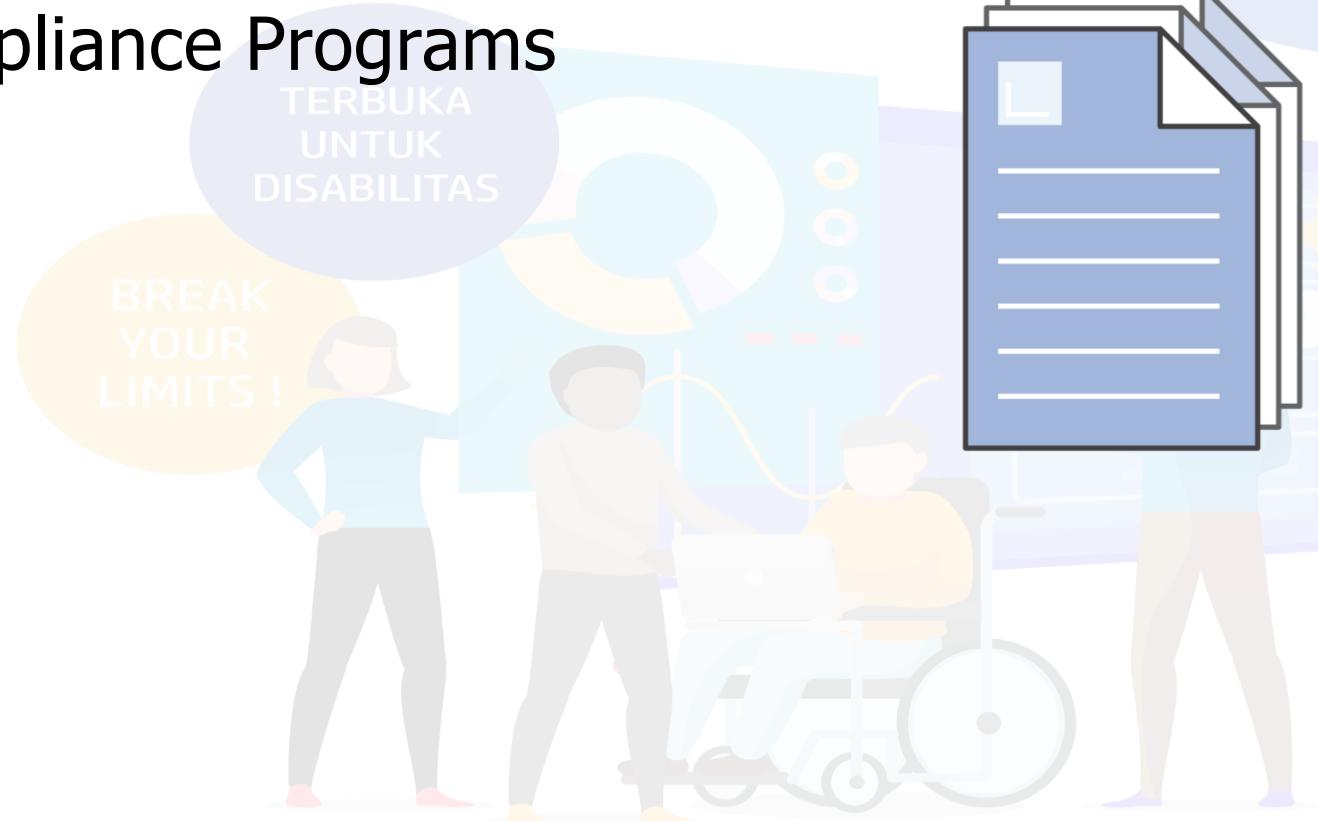
- Provide information about AWS controls
- Assist customers in documenting their framework



Programs

Components of AWS Risk and Compliance Programs

- Risk management
- Control environment
- Information security



Management

AWS management

Business plan

- P Includes risk management
- P Re-evaluated at least biannually

Responsibilities

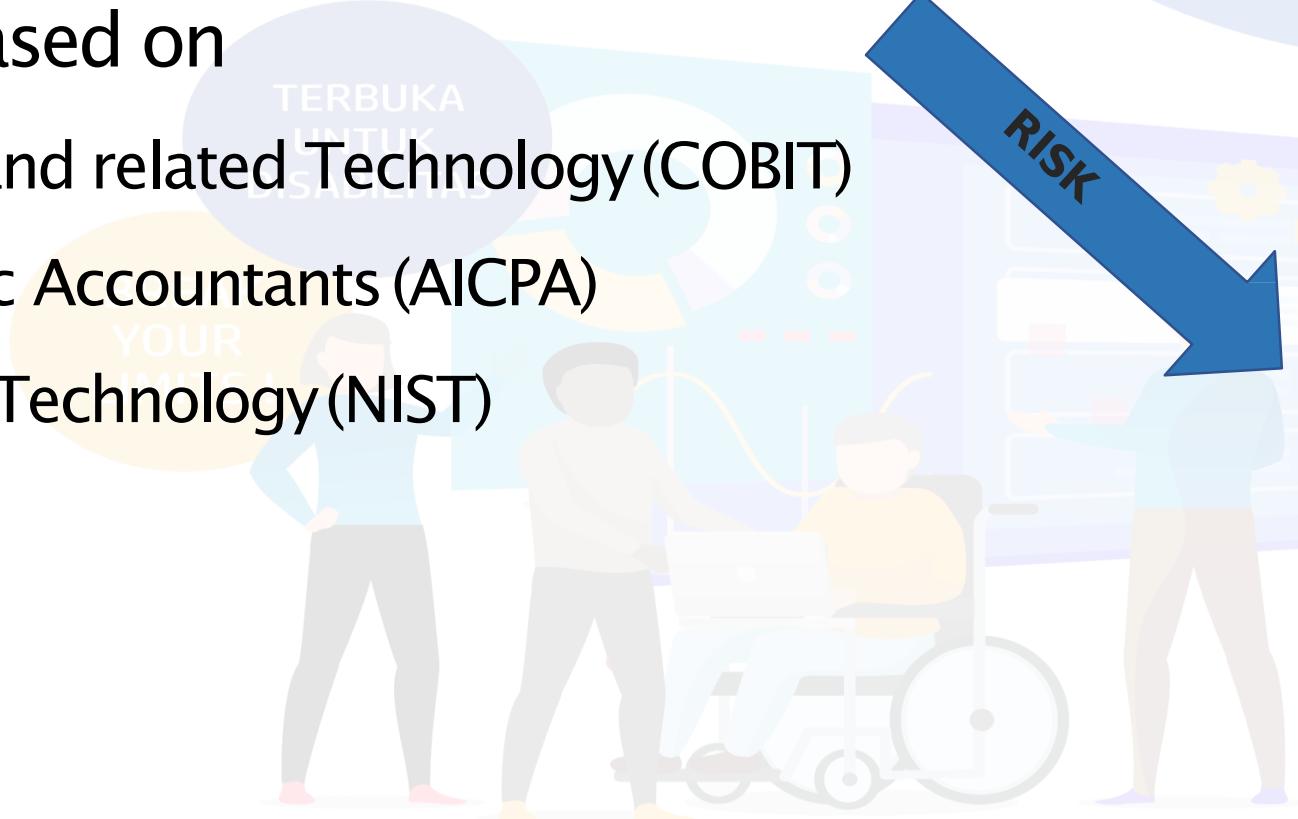
- P Identifies risks
- P Implements appropriate measures
- P Assesses various internal/external risks



Risk Management

Information security network is based on

- ▶ Control Objectives for Information and related Technology (COBIT)
- ▶ American Institute of Certified Public Accountants (AICPA)
- ▶ National Institute of Standards and Technology (NIST)



Management

AWS

- Maintains the security policy
- Provides security training to employees
- Performs application security reviews
 - P Confidentiality
 - P Integrity
 - P Availability of data
 - P Conformance to IS policy



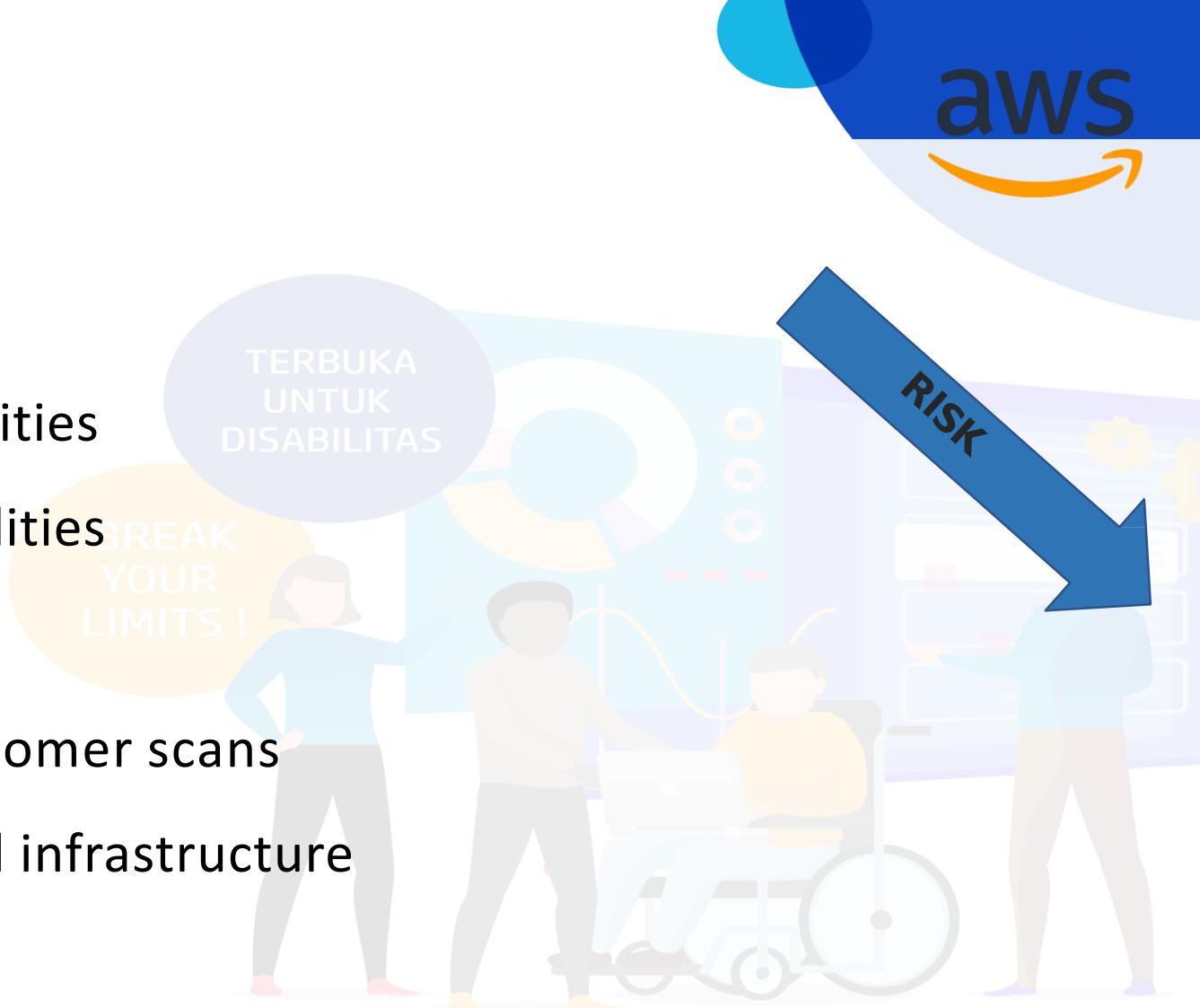
Management

AWS security

- ▶ Scan service endpoints for vulnerabilities
- ▶ Notifies for remediation of vulnerabilities

Independent security firms

- ▶ Scans are not a replacement for customer scans
- ▶ Customers can request to scan cloud infrastructure



Environment

- Includes policies, processes, control activities
- Secure delivery of AWS' service offerings
- Supports the operating effectiveness of AWS' control framework
- Integrates controls
- Monitors for leading practices



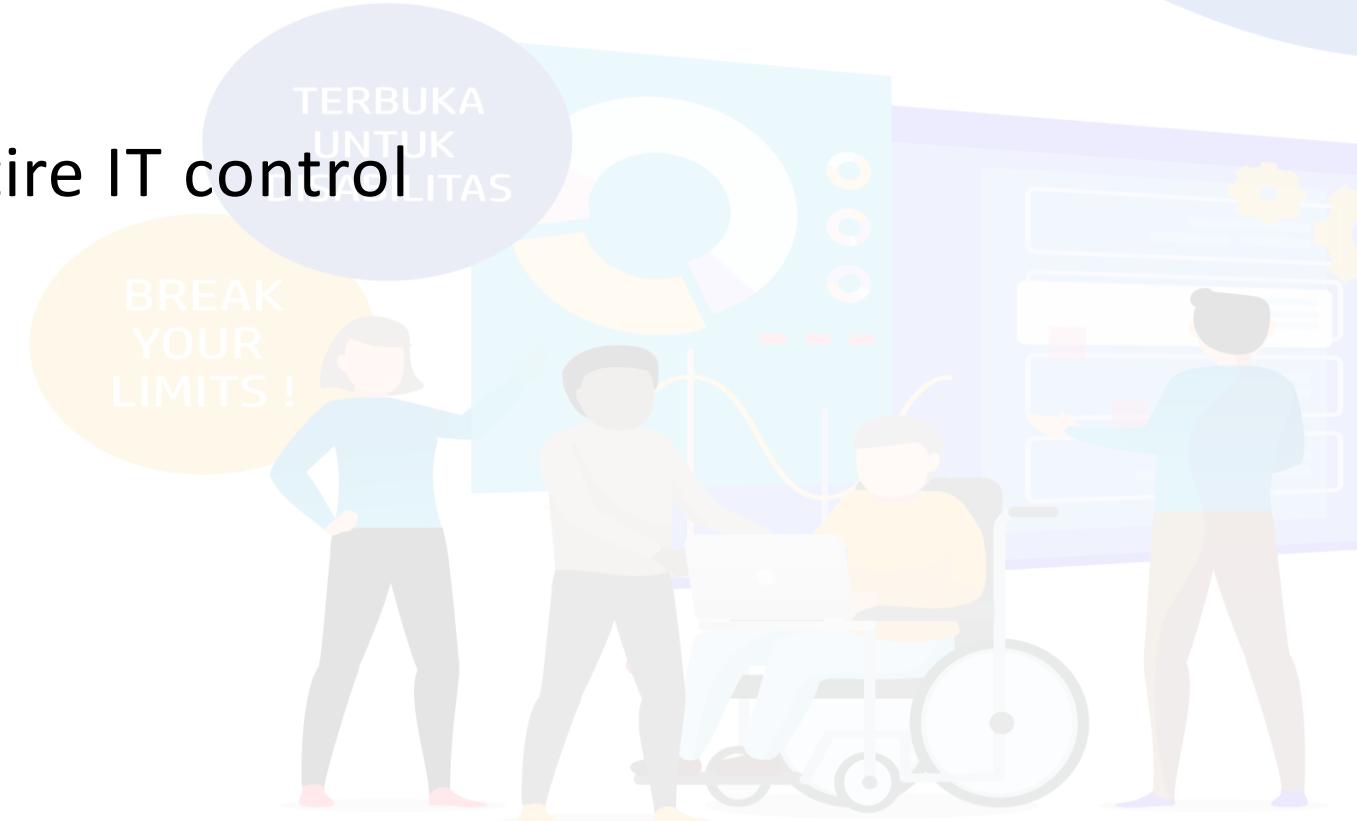
- Designed to protect
 - P Confidentiality
 - P Integrity
 - P Availability
- Publishes security whitepaper



Customer Compliance

Customer requirements

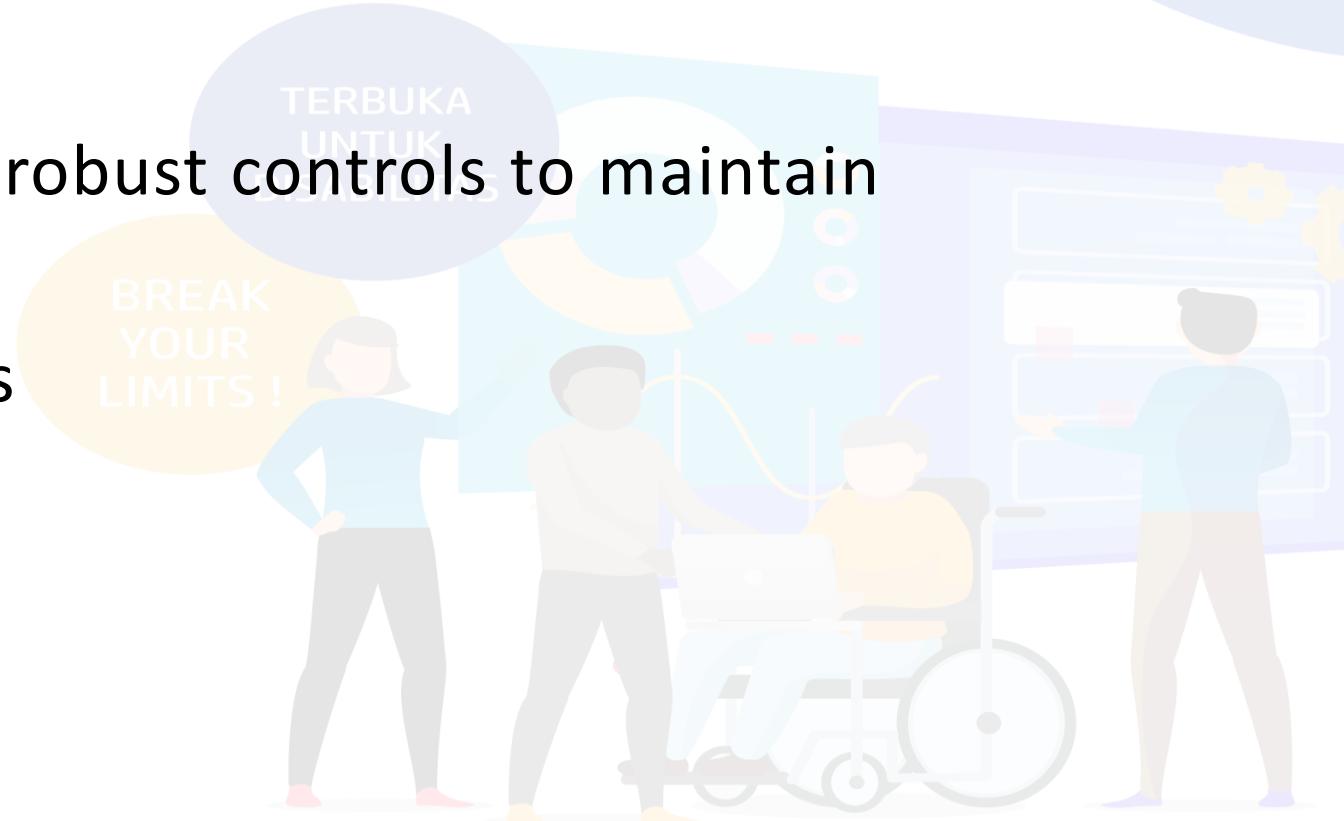
- Maintain governance over the entire IT control environment
- Understand
 - ▶ Required compliance objectives
 - ▶ Validation based risk tolerance
- Establish control environment
- Verify effectiveness of control environment



y

AWS security compliance programs

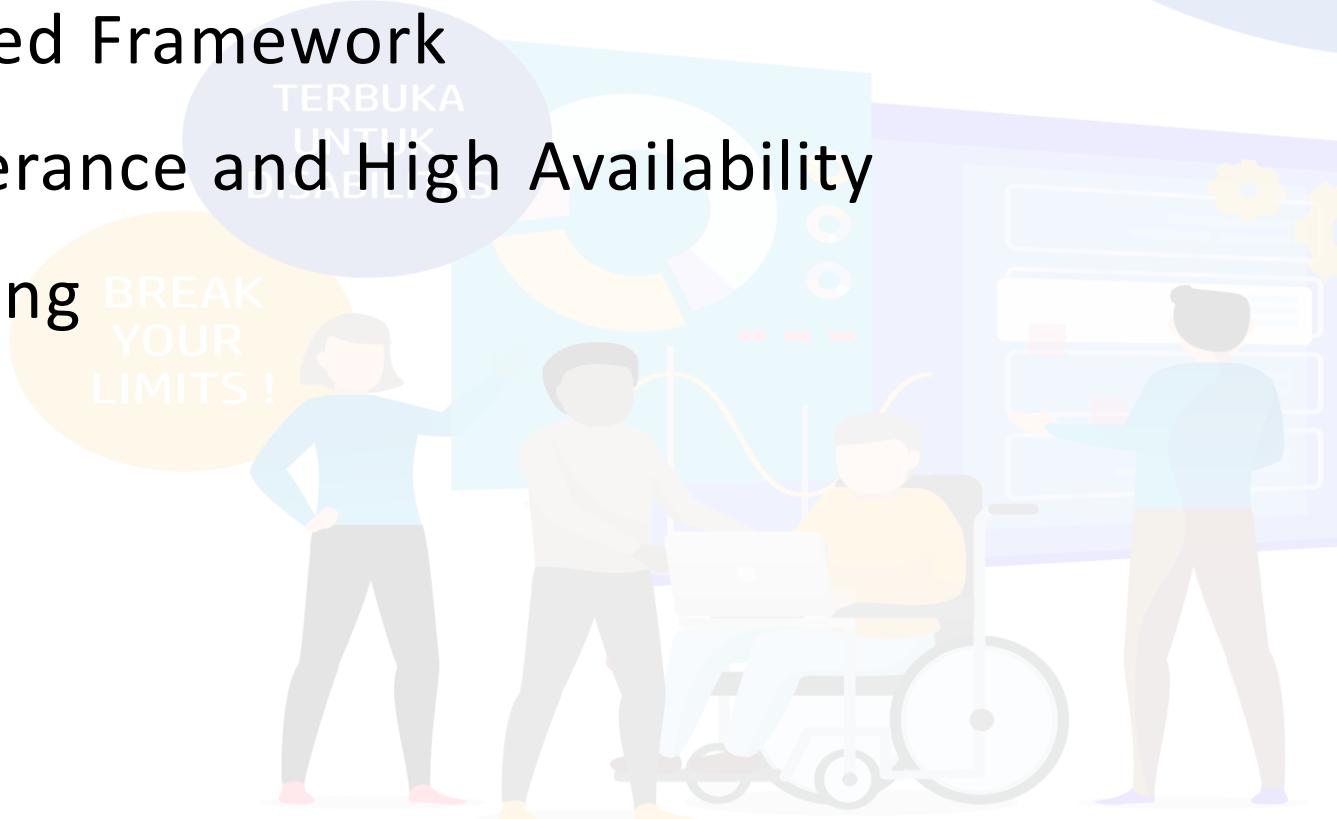
- Enables customers to understand robust controls to maintain security and data protection
- Shared compliance responsibilities



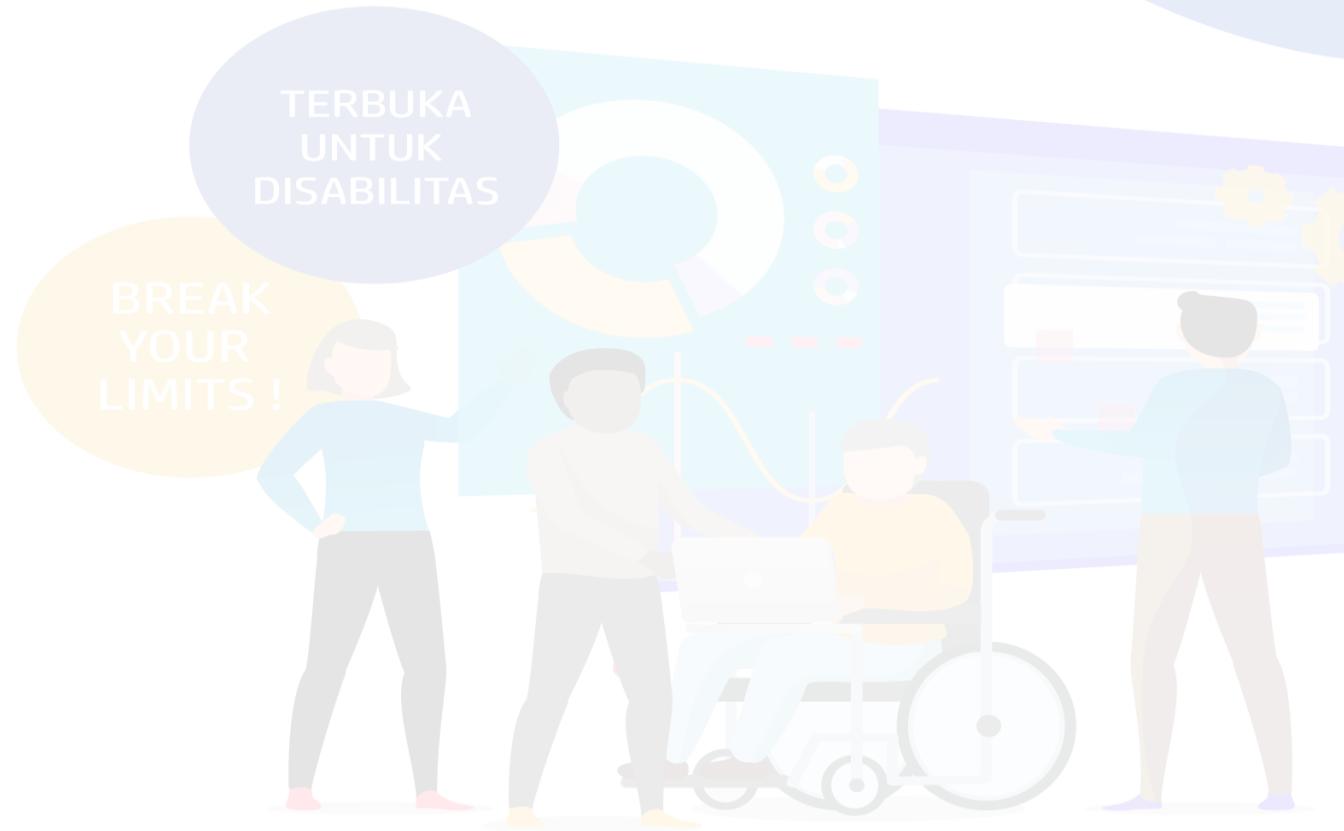


Module 4: AWS Architecting Essentials

- Introduction to the Well-Architected Framework
- Reference Architecture – Fault Tolerance and High Availability
- Reference Architecture: Web Hosting



Introduction to the Well- Architected Framework

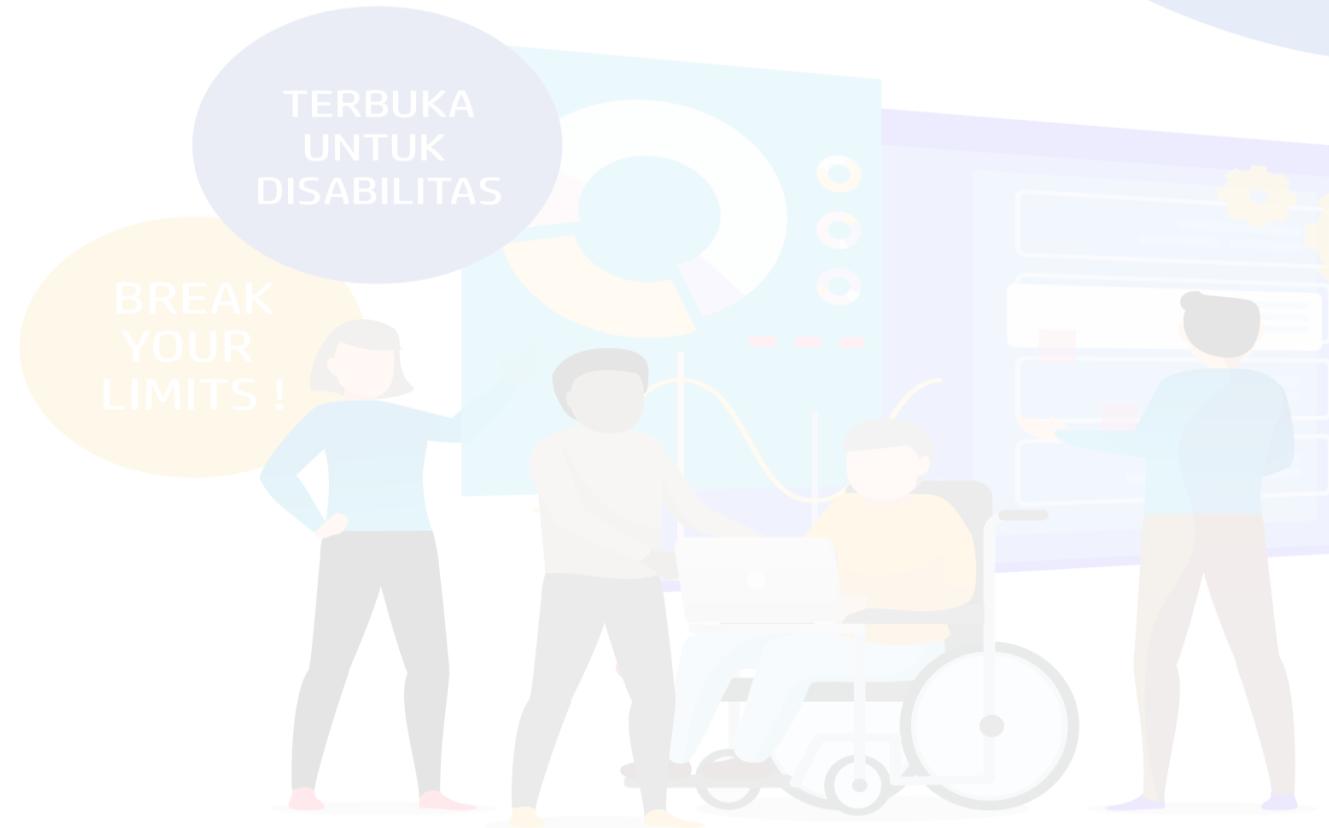


- Assess and improve architectures
- Understand how design decisions impact business
- Learn the five pillars and design principles



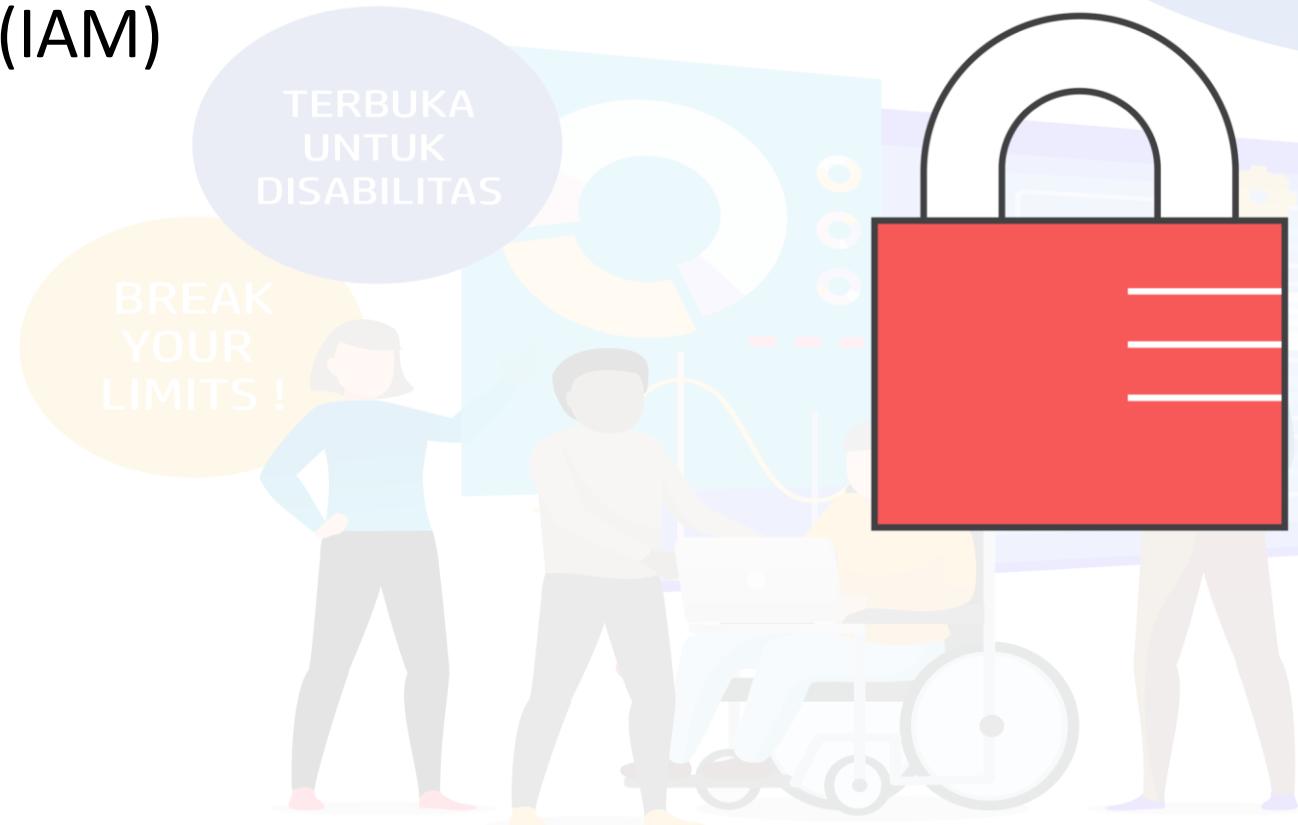
Pillars

- Security
- Reliability
- Performance efficiency
- Cost optimization
- Operational excellence



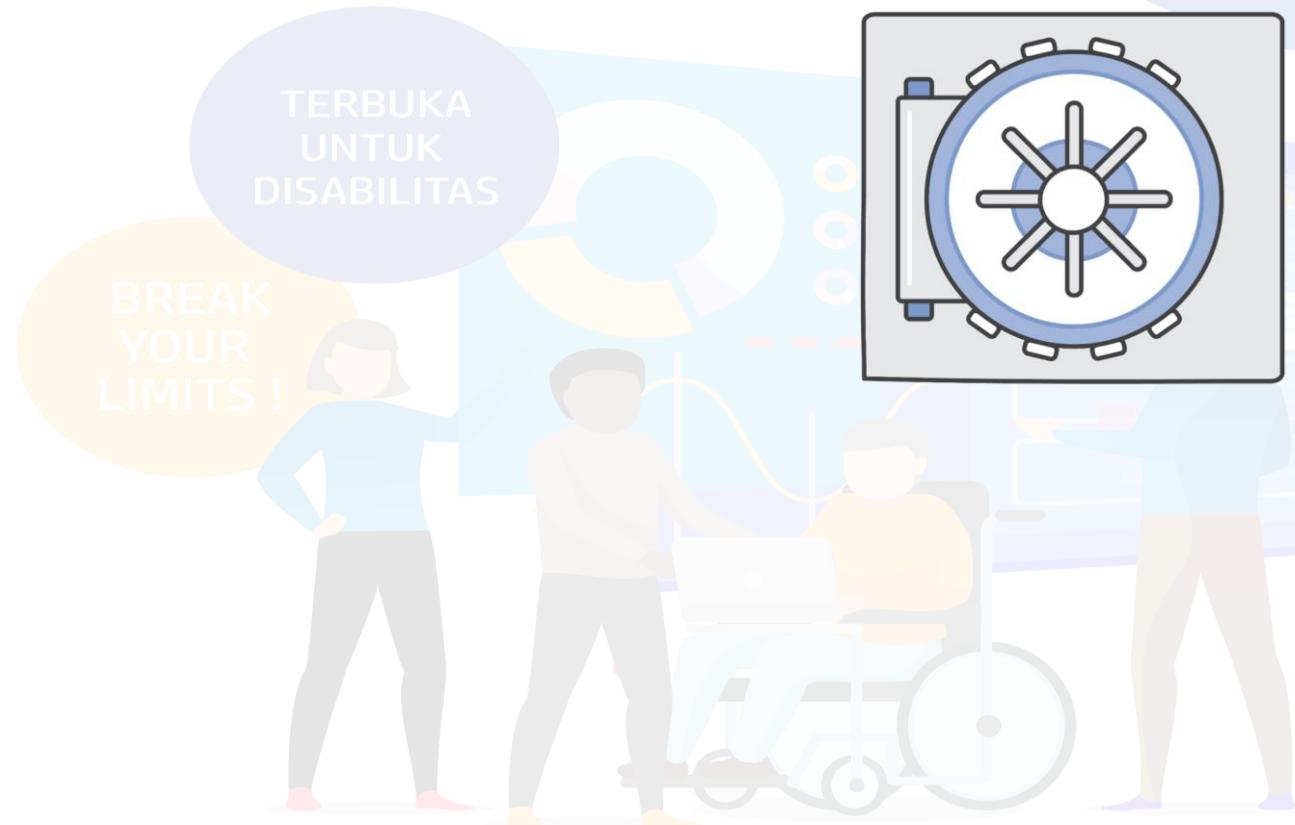
Pillar

- Identity and access management (IAM)
- Detective controls
- Infrastructure protection
- Data protection
- Incident response



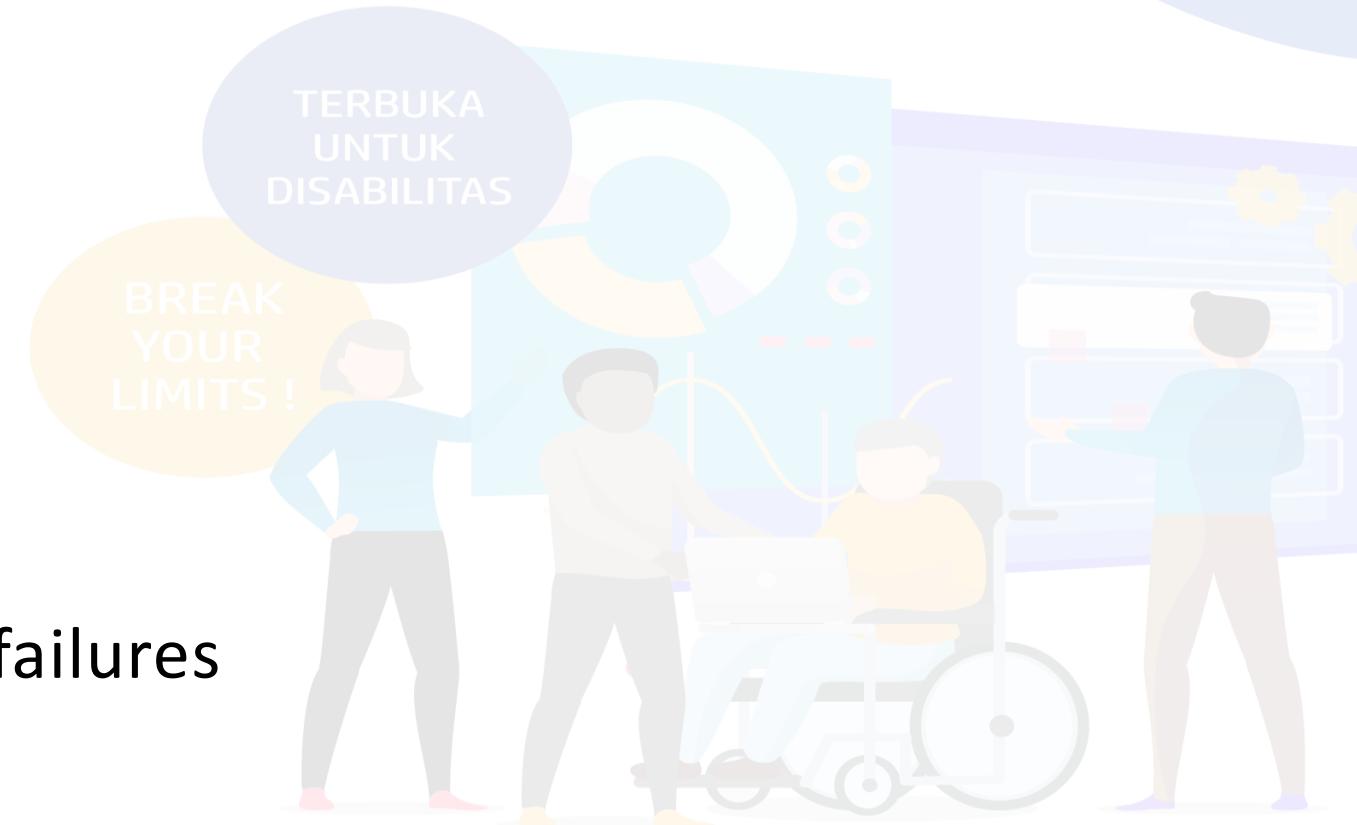
Principles

- Implement security at all layers
- Enable traceability
- Apply principle of least privilege
- Focus on securing your system
- Automate



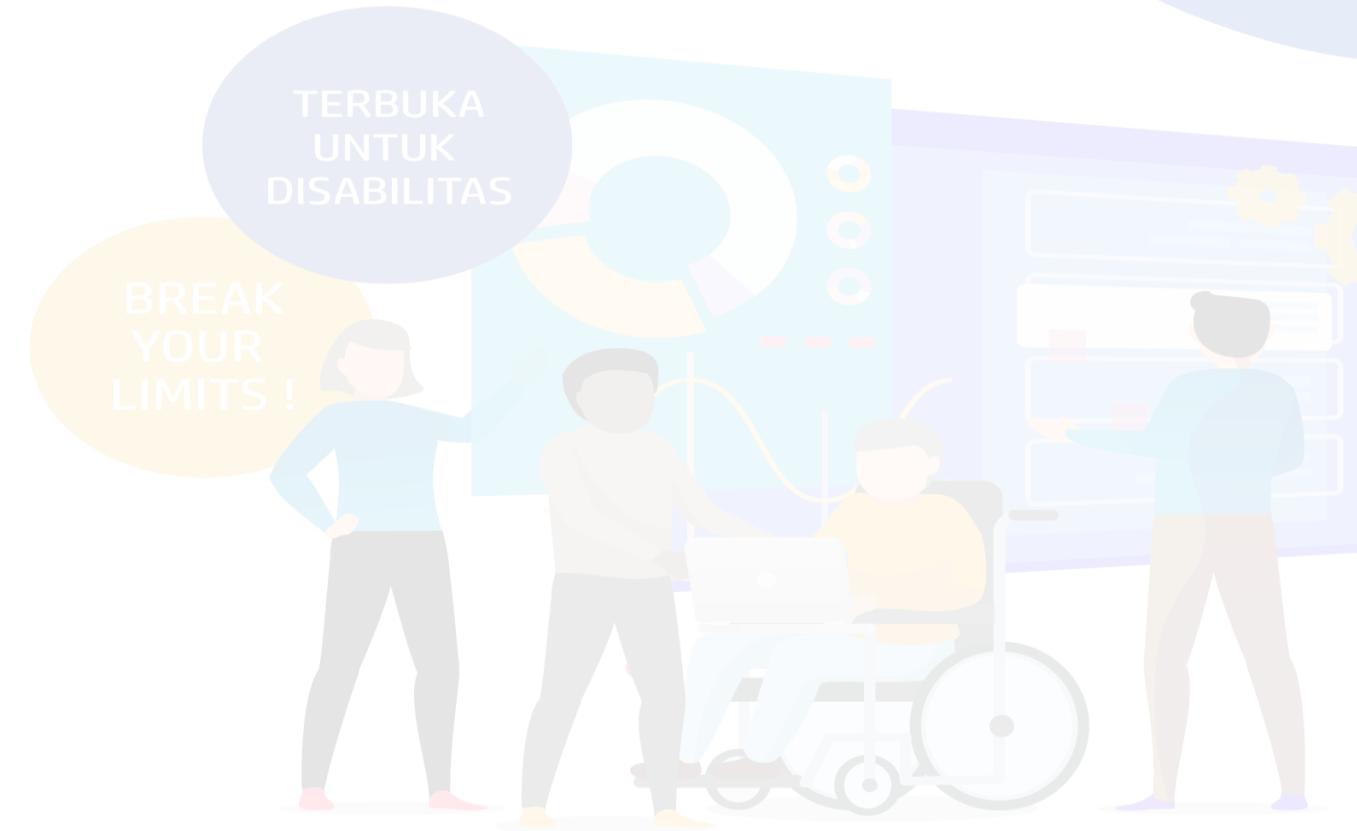
Pillar

- Recover from issues/failures
- Apply best practices in:
 - ▶ Foundations
 - ▶ Change management
 - ▶ Failure management
- Anticipate, respond, and prevent failures



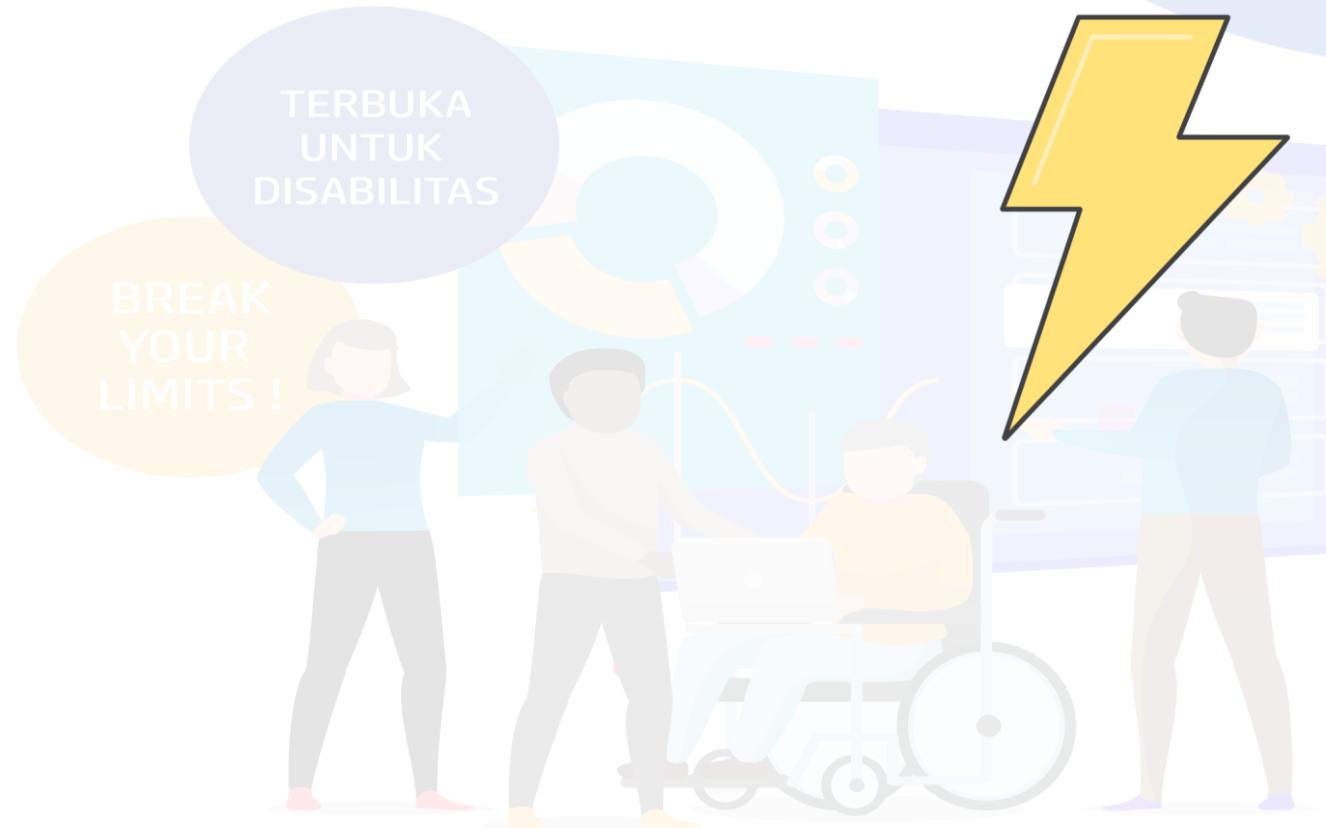
Principles

- Test recovery procedures
- Automatically recover
- Scale horizontally
- Stop guessing capacity
- Manage change in automation



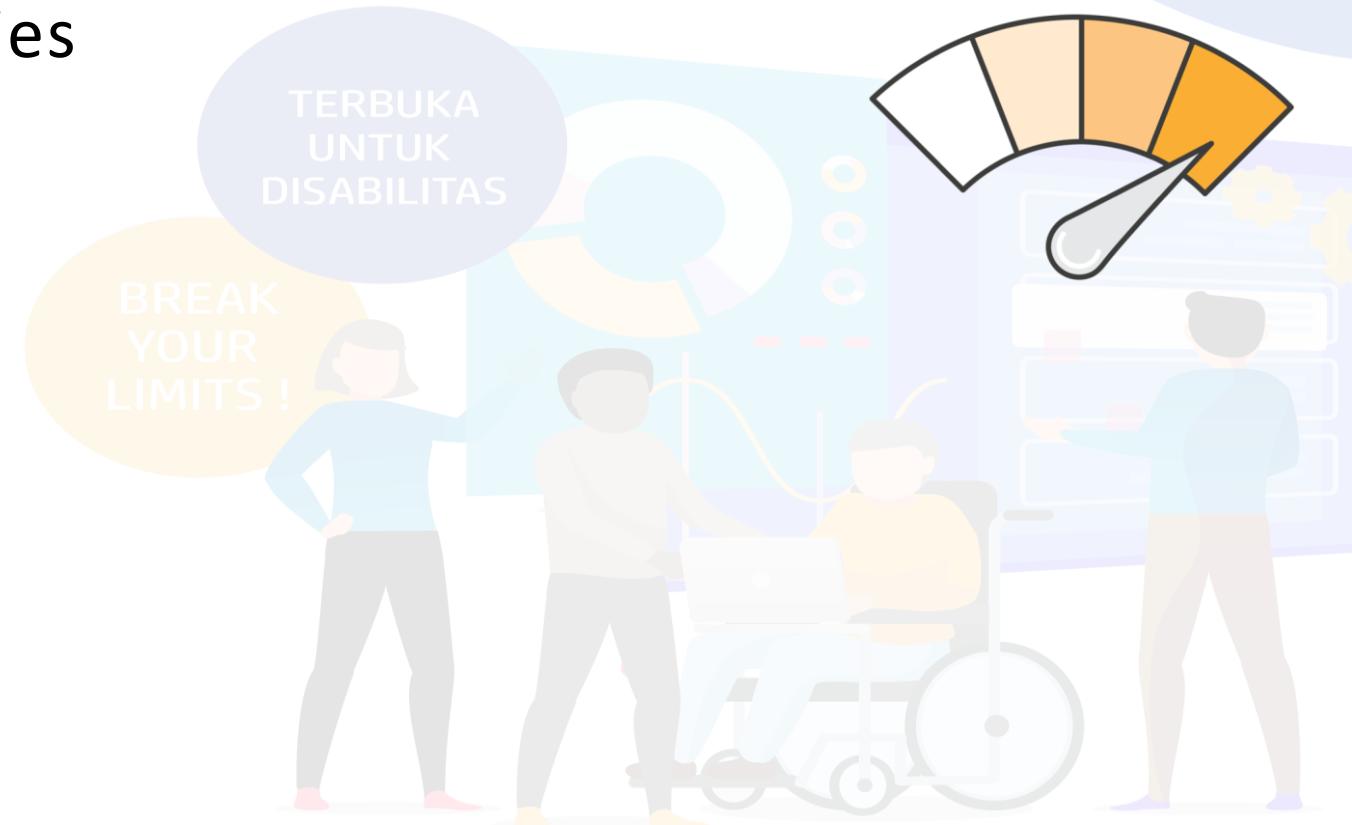
Pillar

- Select customizable solutions
- Review to continually innovate
- Monitor AWS services
- Consider the trade-offs



Performance Efficiency Pillar: Design Principles

- Democratize advanced technologies
- Go global in minutes
- Use a serverless architectures
- Experiment more often
- Have mechanical sympathy



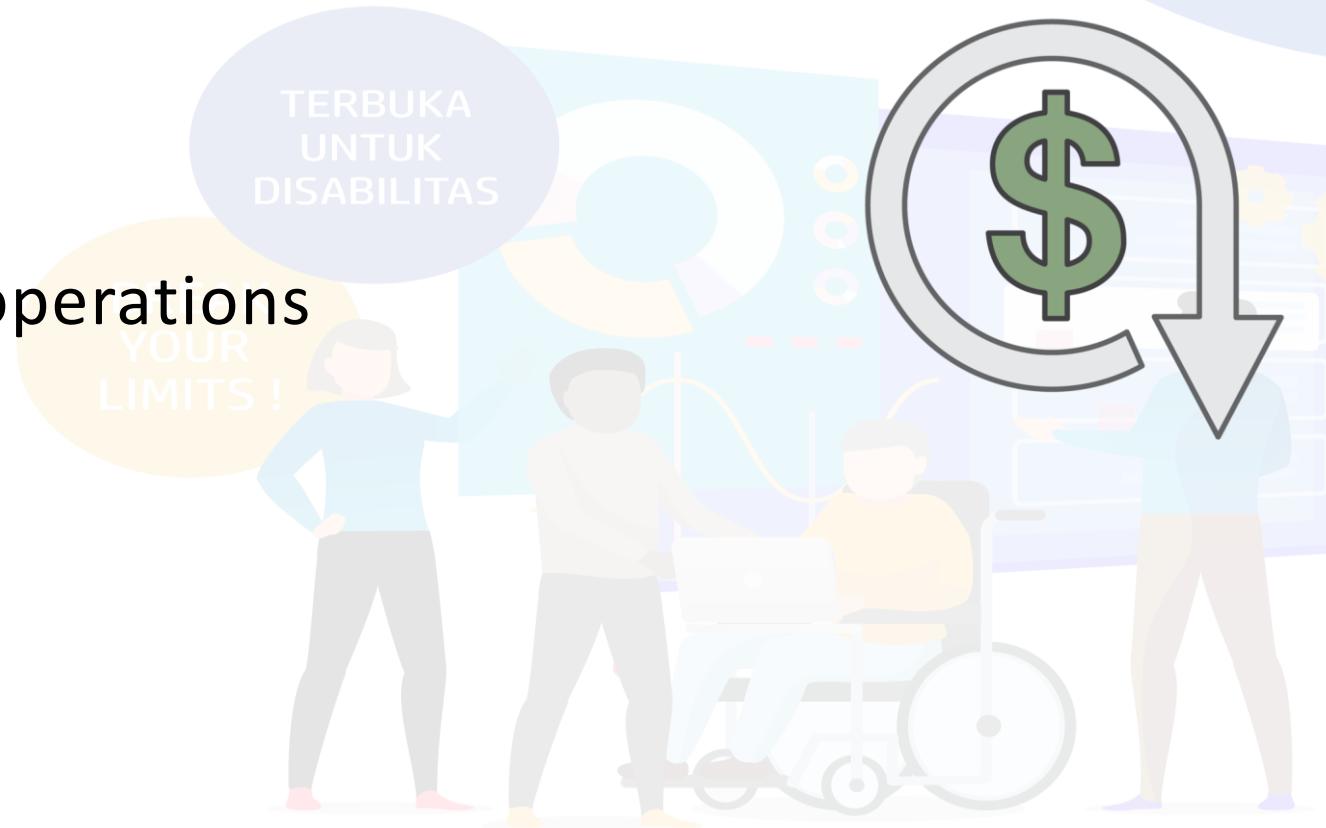
Pillar

- Use cost-effective resources
- Matching supply with demand
- Increase expenditure awareness
- Optimize over time



Principles

- Adopt a consumption model
- Measure overall efficiency
- Reduce spending on data center operations
- Analyze and attribute expenditure
- Use managed services



Pillar

- Manage and automate changes
- Respond to events
- Define the standards



y

Five pillars and their associated design principles

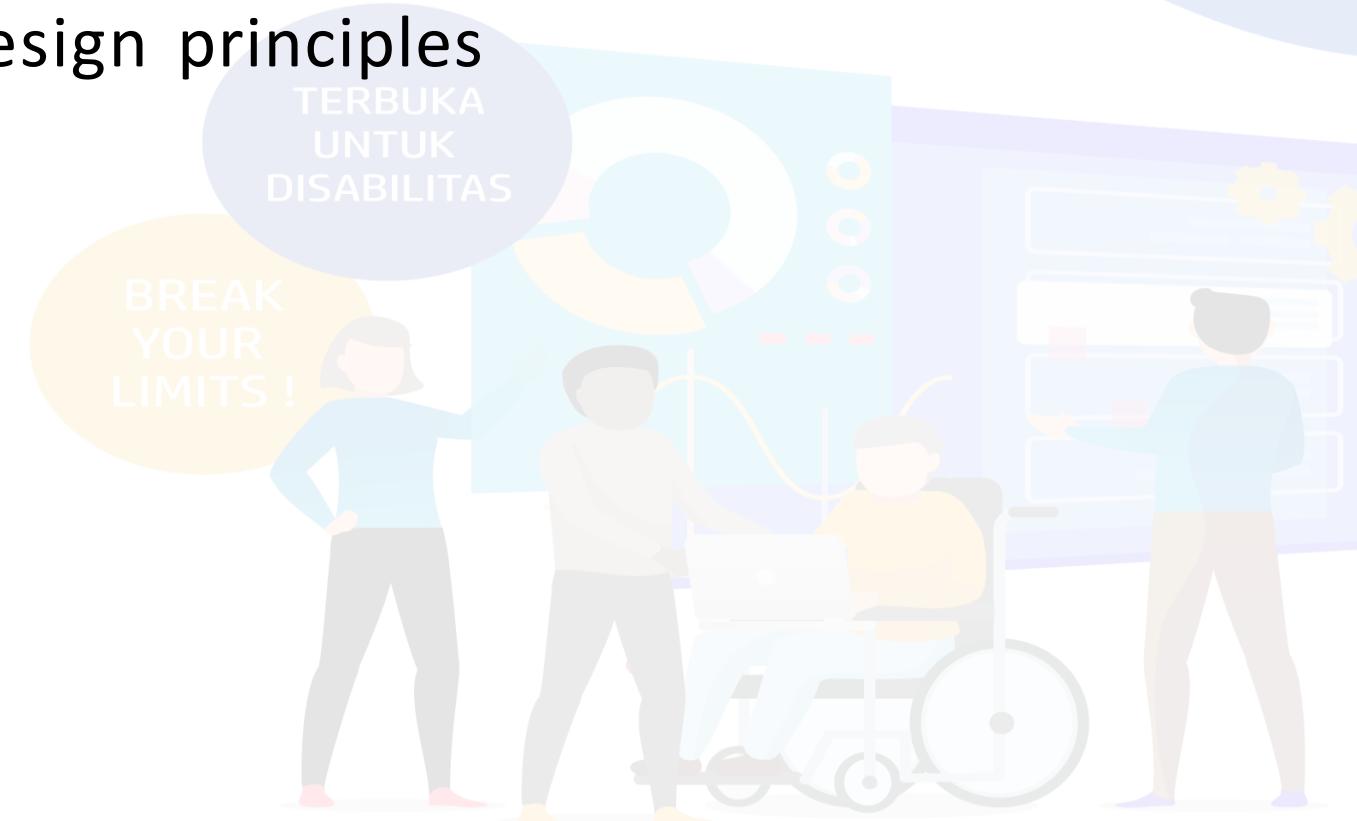
P Security

P Reliability

P Performance Efficiency

P Cost Optimization

P Operational Excellence

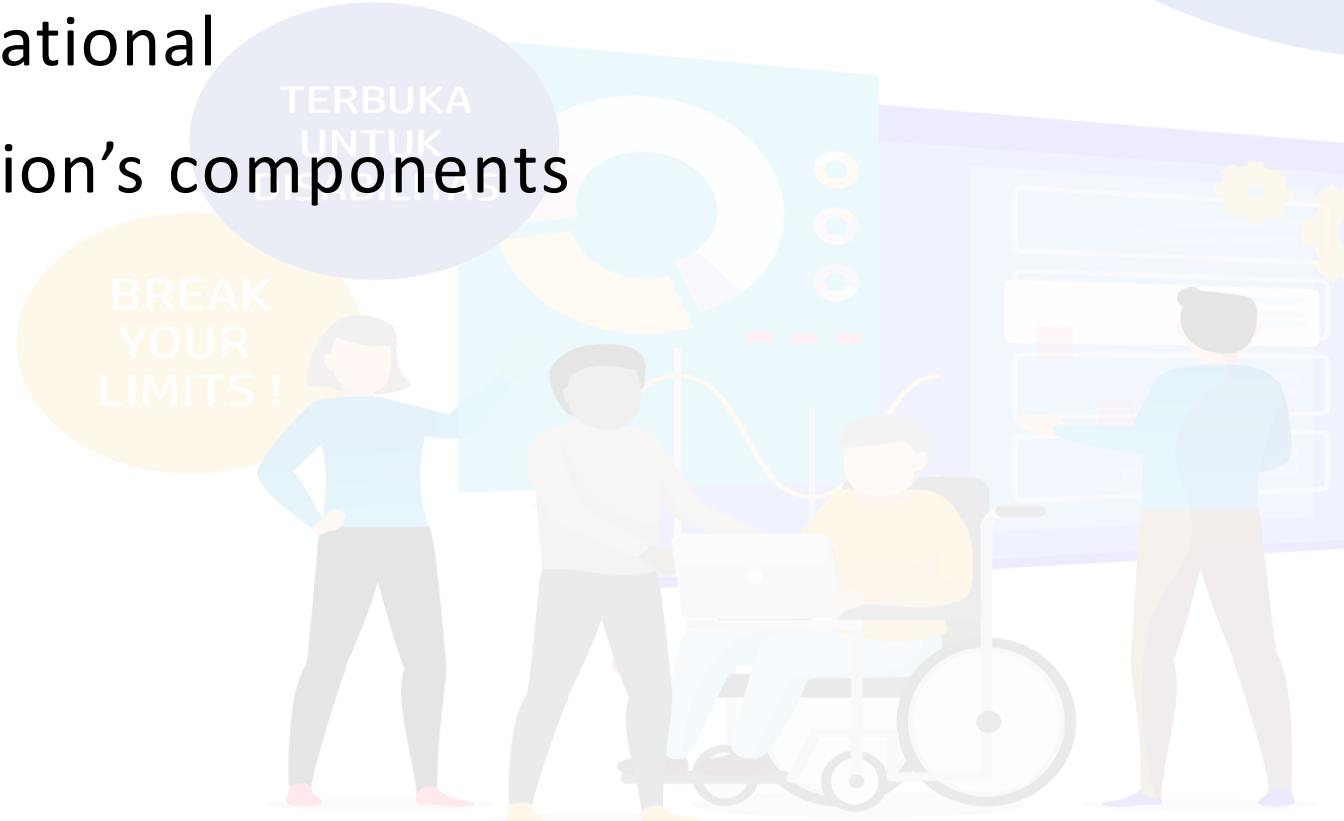


Reference Architecture – Fault Tolerance and High Availability



Fault Tolerance

- Ability of a system to remain operational
- Built-in redundancy of an application's components



Availability

High availability is designed to keep

- Systems generally functioning and accessible
- Downtime minimized
- Minimal human intervention required
- Minimal up-front financial investment





High Availability: On Premises vs AWS

► Traditional (on premises)

P Expensive

P Only mission-critical applications

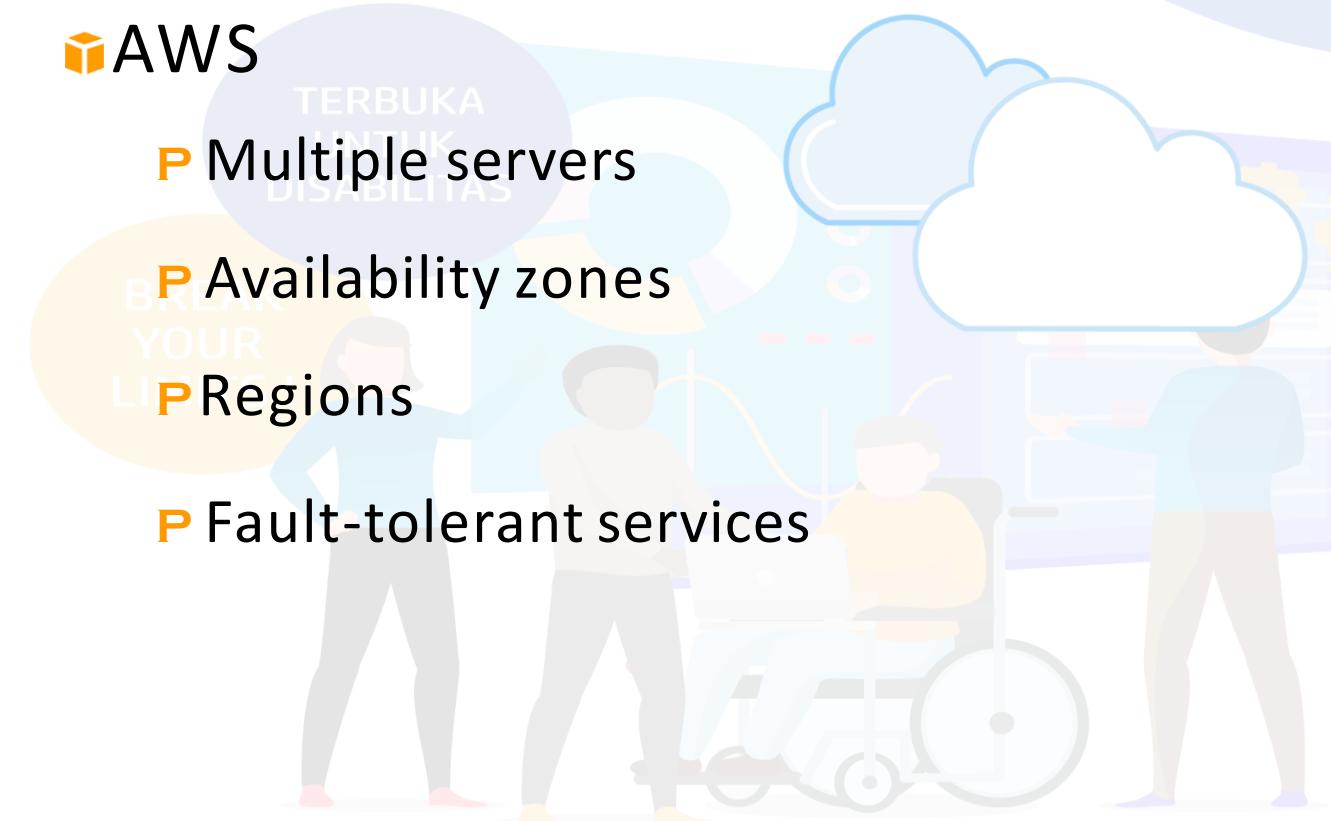
► AWS

P Multiple servers

P Availability zones

P Regions

P Fault-tolerant services



Services

AWS Services and High Availability

- üAmazon S3 and Amazon Glacier
- üDynamoDB
- ü Amazon CloudFront
- ü Amazon SWF
- üAmazon SQS
- ü Amazon SNS
- üAmazon SES
- ü Amazon Route53
- ü Elastic Load Balancing
- ü IAM
- ü Amazon CloudWatch
- ü Amazon CloudSearch
- ü AWS Data Pipeline
- ü Amazon Kinesis

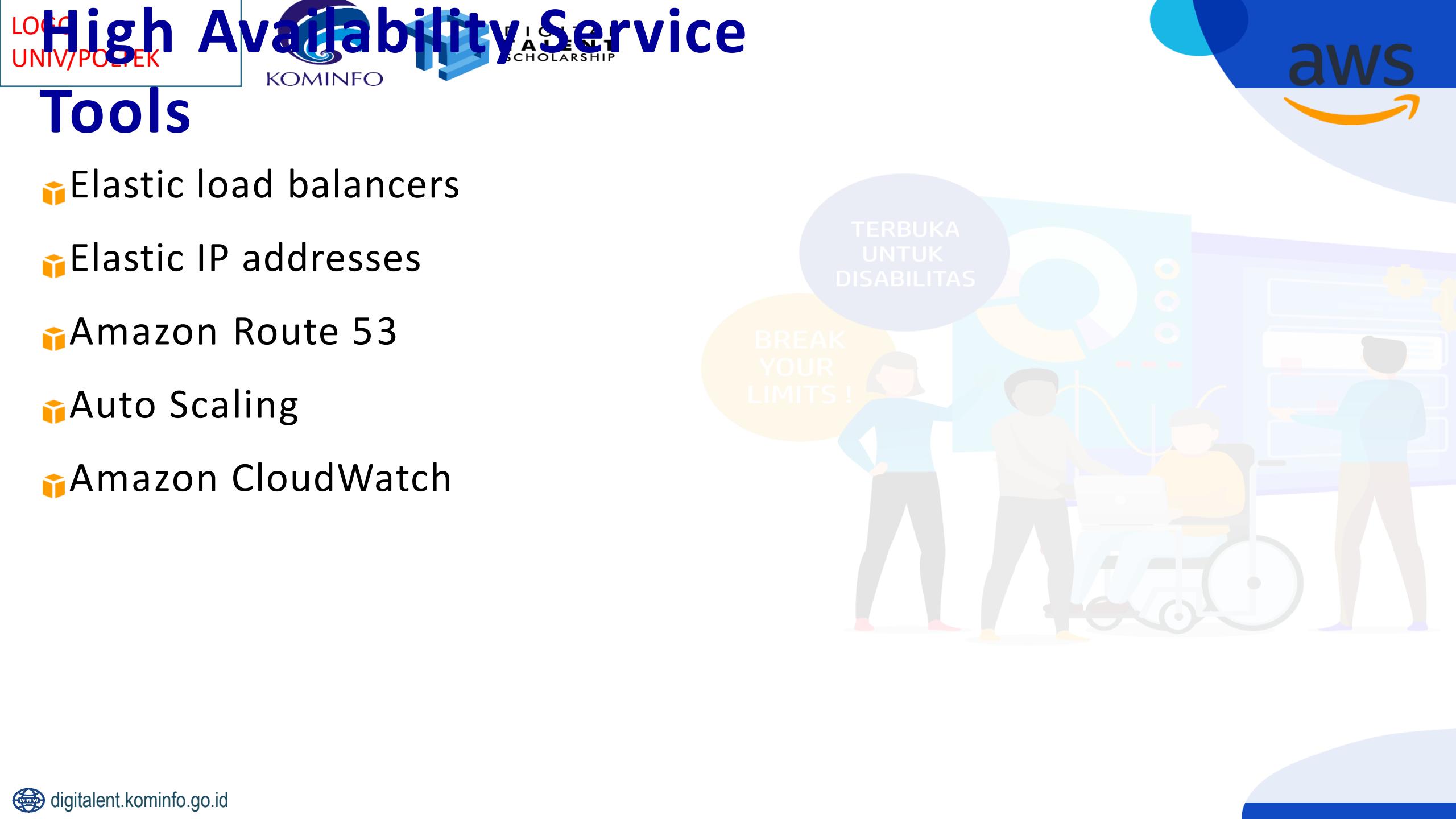
- üAuto Scaling
- ü Amazon Elastic File System
- ü AWS CloudFormation
- ü Amazon WorkMail
- ü AWS Directory Service
- üAWS Lambda
- ü Amazon EBS
- üAmazon RDS

Inherently HA services

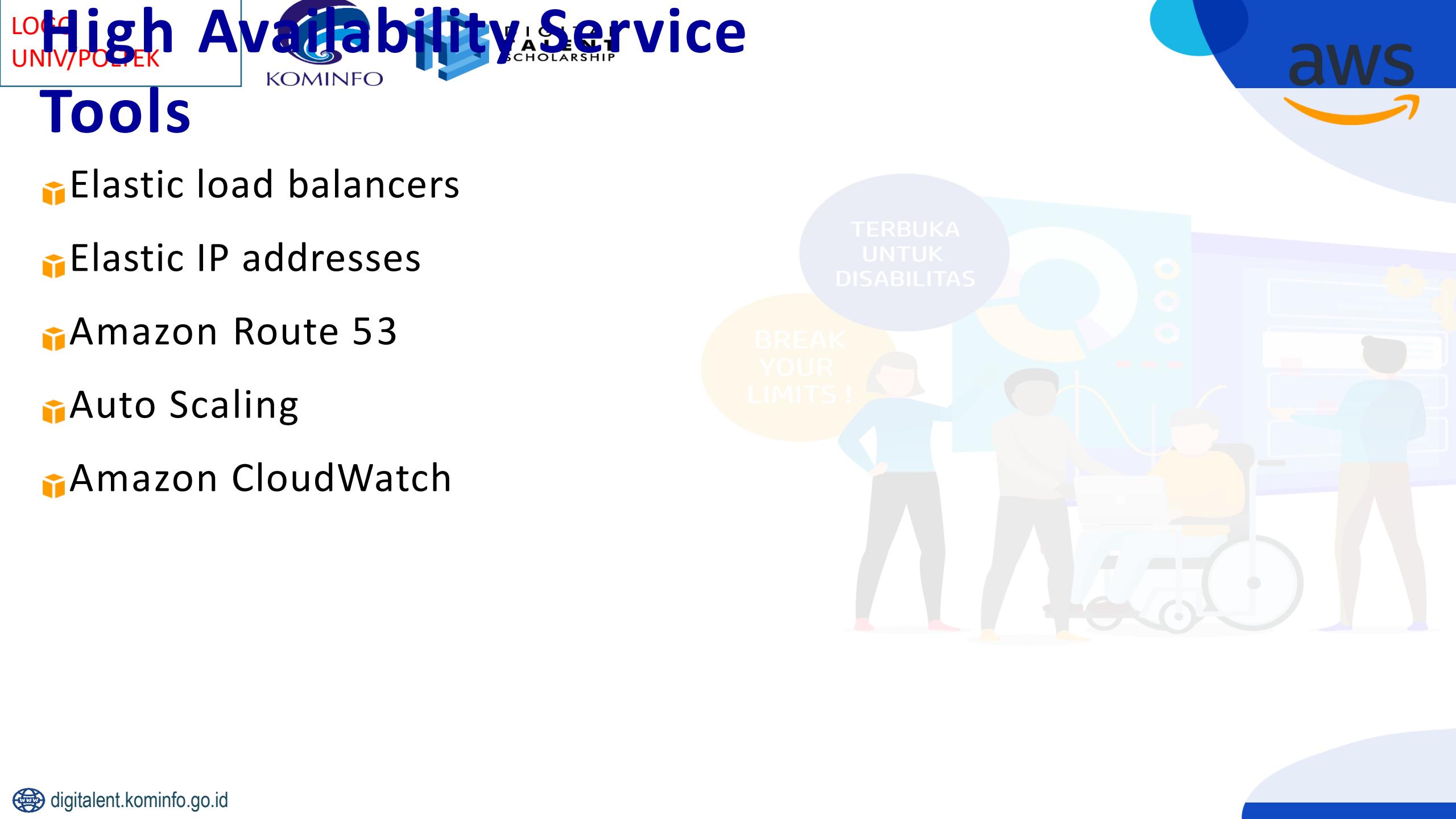
- ü Amazon EC2
- ü Amazon VPC
- ü Amazon Redshift
- ü Amazon ElastiCache
- ü AWS Direct Connect

*Not all services are listed here.

HA with the right architecture



High Availability Service



Tools

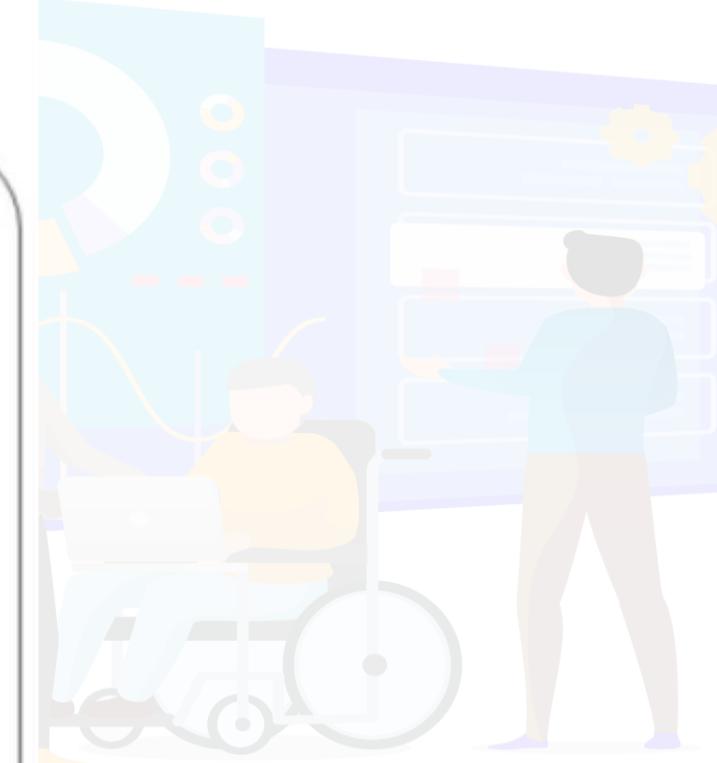
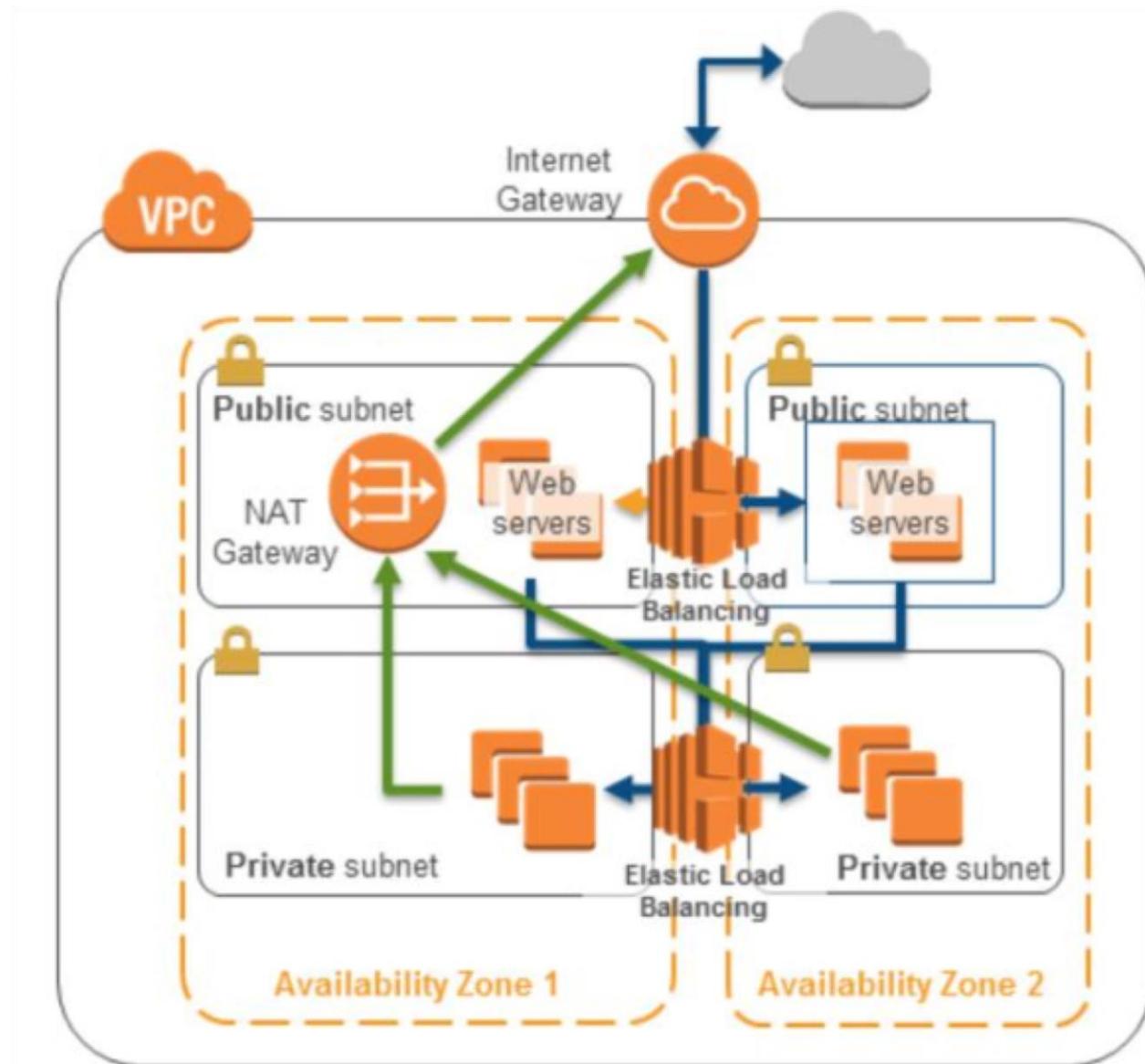
- Elastic load balancers
- Elastic IP addresses
- Amazon Route 53
- Auto Scaling
- Amazon CloudWatch

Elastic Load Balancers

- Distributes incoming traffic (loads)
- Sends metrics to Amazon CloudWatch
- Triggers and notifies
 - ▶ High latency
 - ▶ Over used

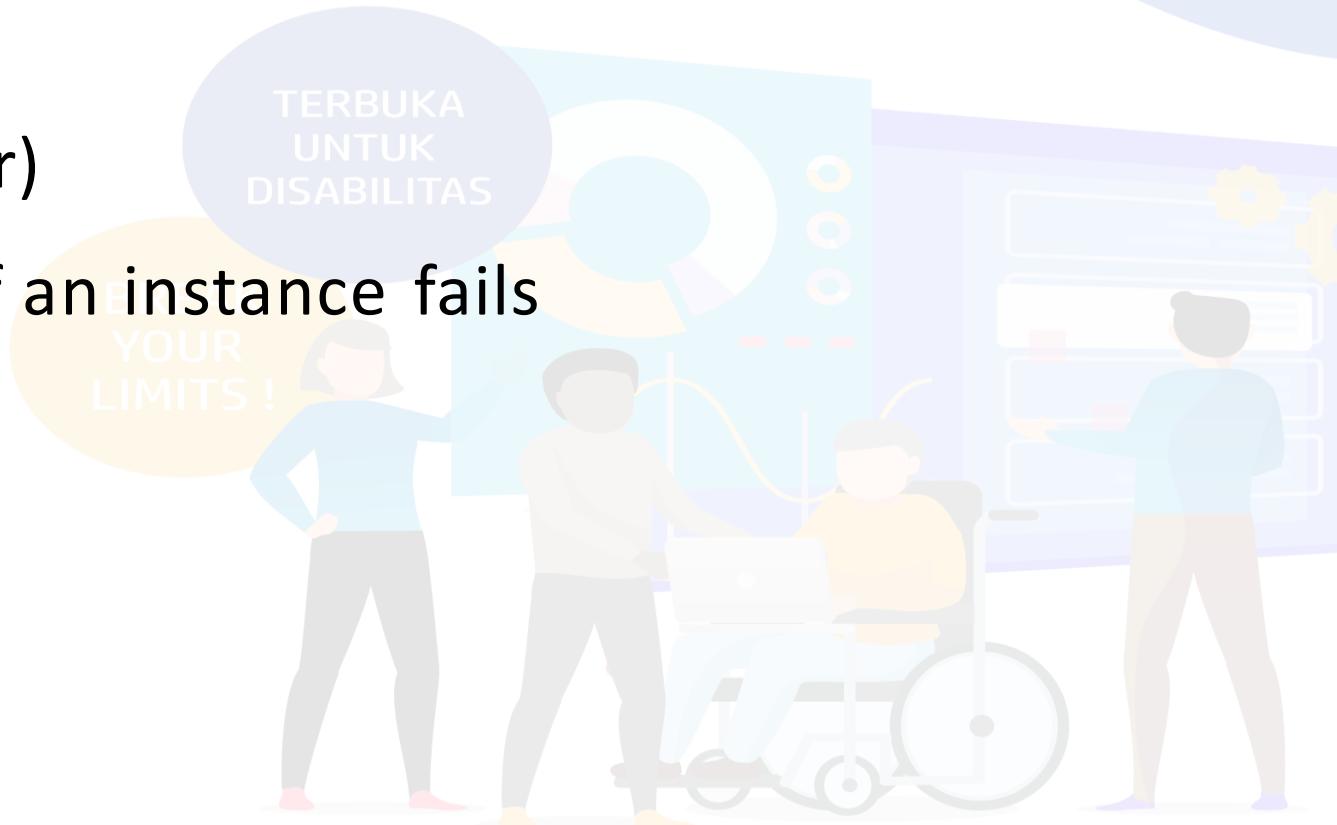


Balancers



Addresses

- Are static IP addresses
- Mask failures (if they were to occur)
- Continues to access applications if an instance fails



53

■ Authoritative DNS service

- ▶ Translates domain names to IP addresses

■ Supports:

- ▶ Simple routing
- ▶ Latency-based routing
- ▶ Health checks
- ▶ DNS failovers
- ▶ Geo-location routing



Scaling

- Terminates and launches instances
- Assists with adjusting or modifying capacity
- Creates new resources on demand



CloudWatch

■ Alarm examples:

- If CPU utilization is $>60\%$ for 5 minutes...
- If number of simultaneous connections is >10 for one minute...
- If number of healthy hosts is <5 for 10 minutes...





Fault Tolerant Tools

- Amazon Simple Queue Service

- Amazon Simple Storage Service

- Amazon SimpleDB

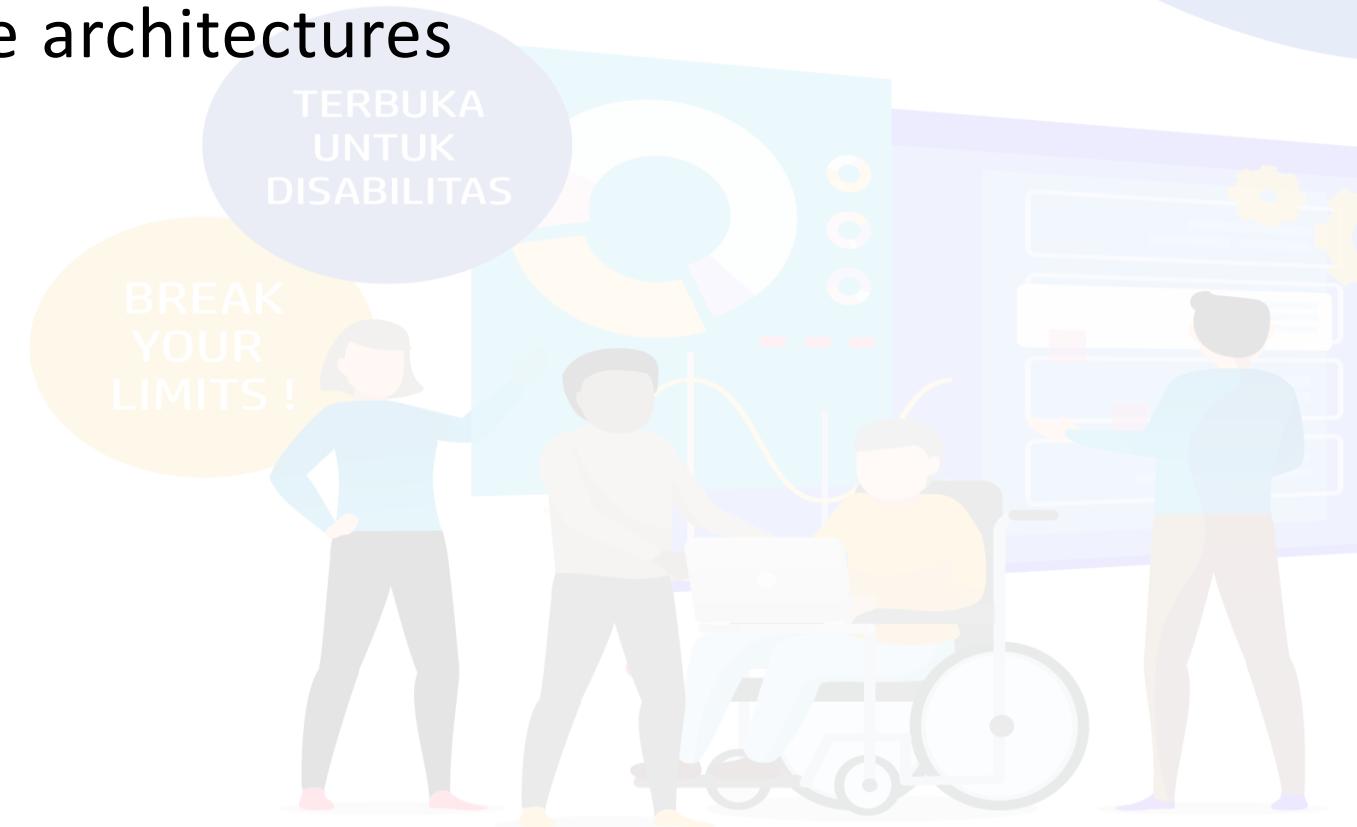
- Amazon Relational Database Service



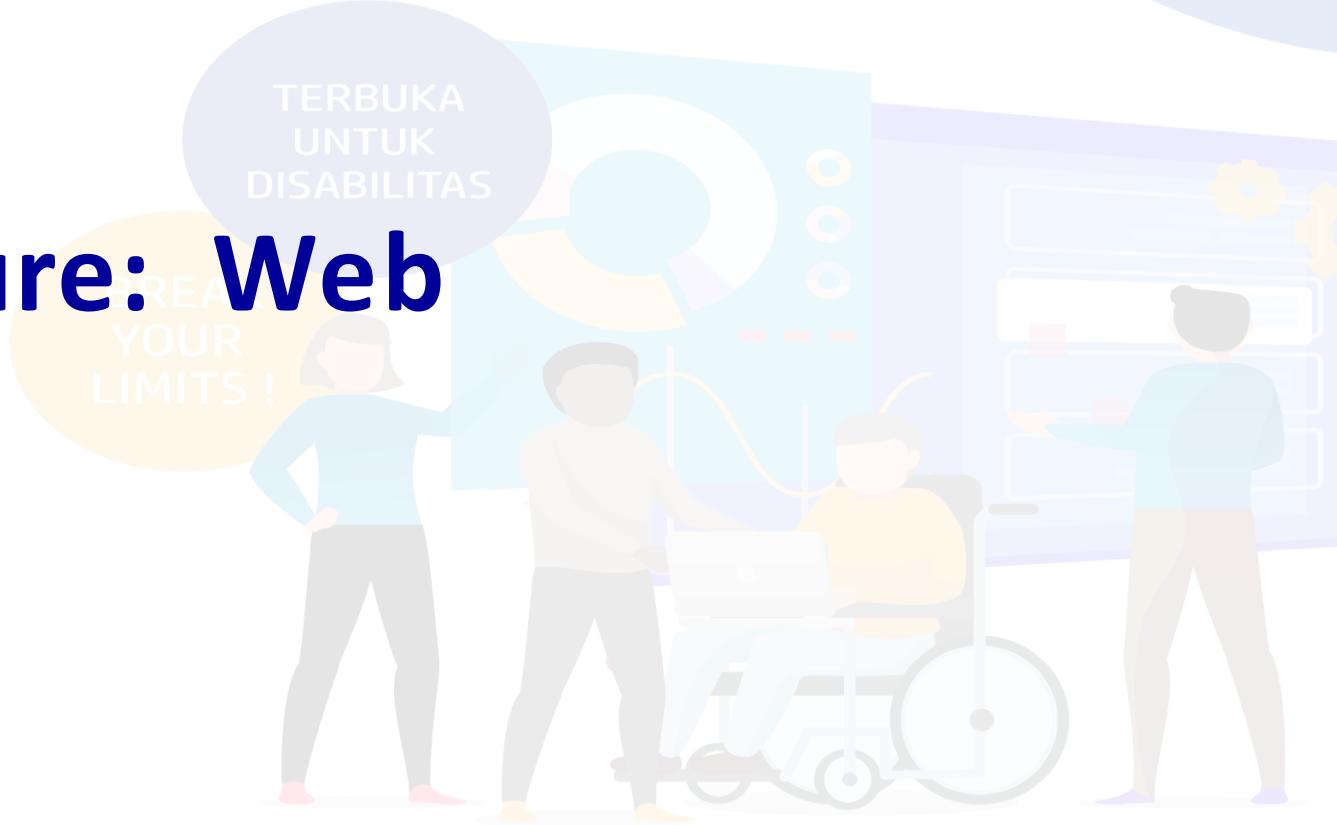


y

- Fault Tolerant and highly available architectures
- Services to assist architectures



Reference Architecture: Web Hosting



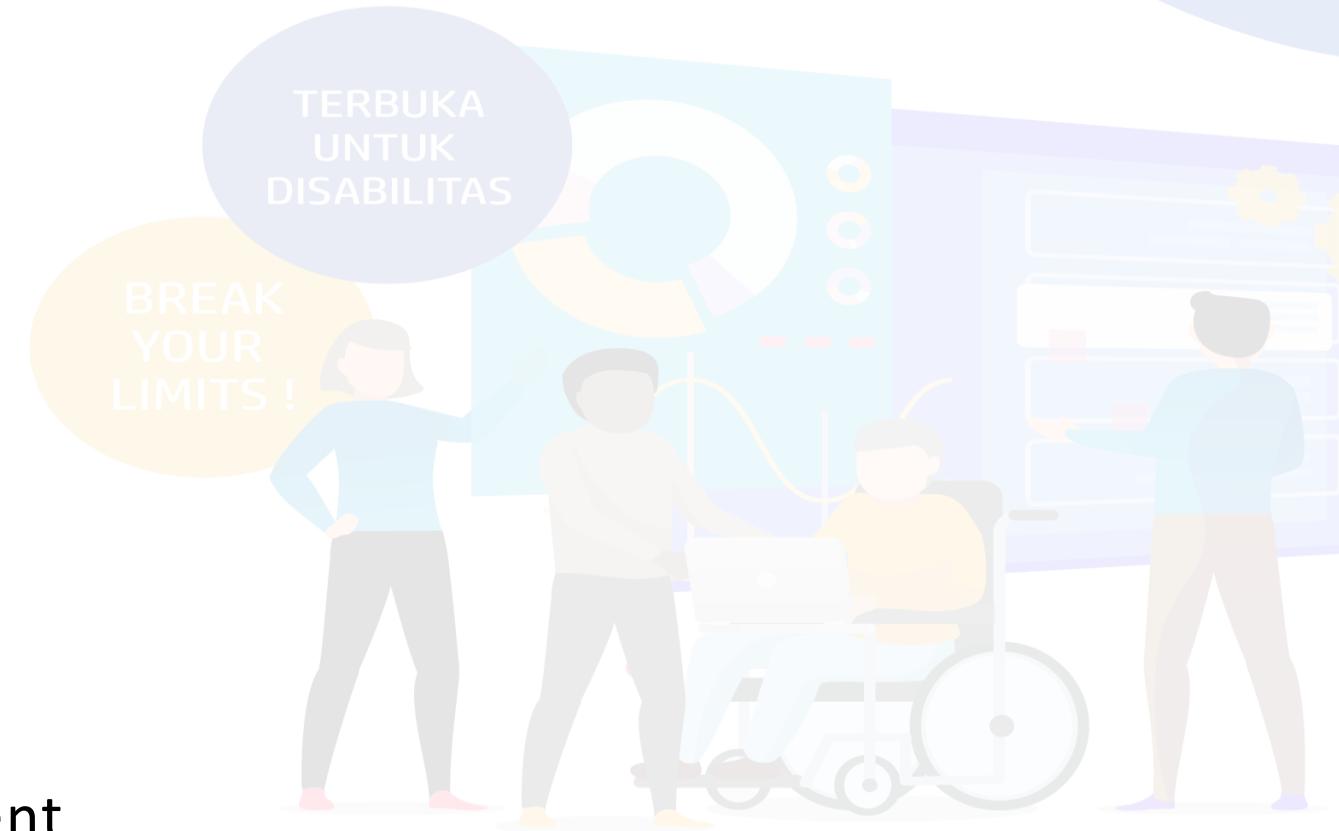
Hosting

Web hosting on AWS:

- ▶ Fast
- ▶ Straightforward
- ▶ Low cost

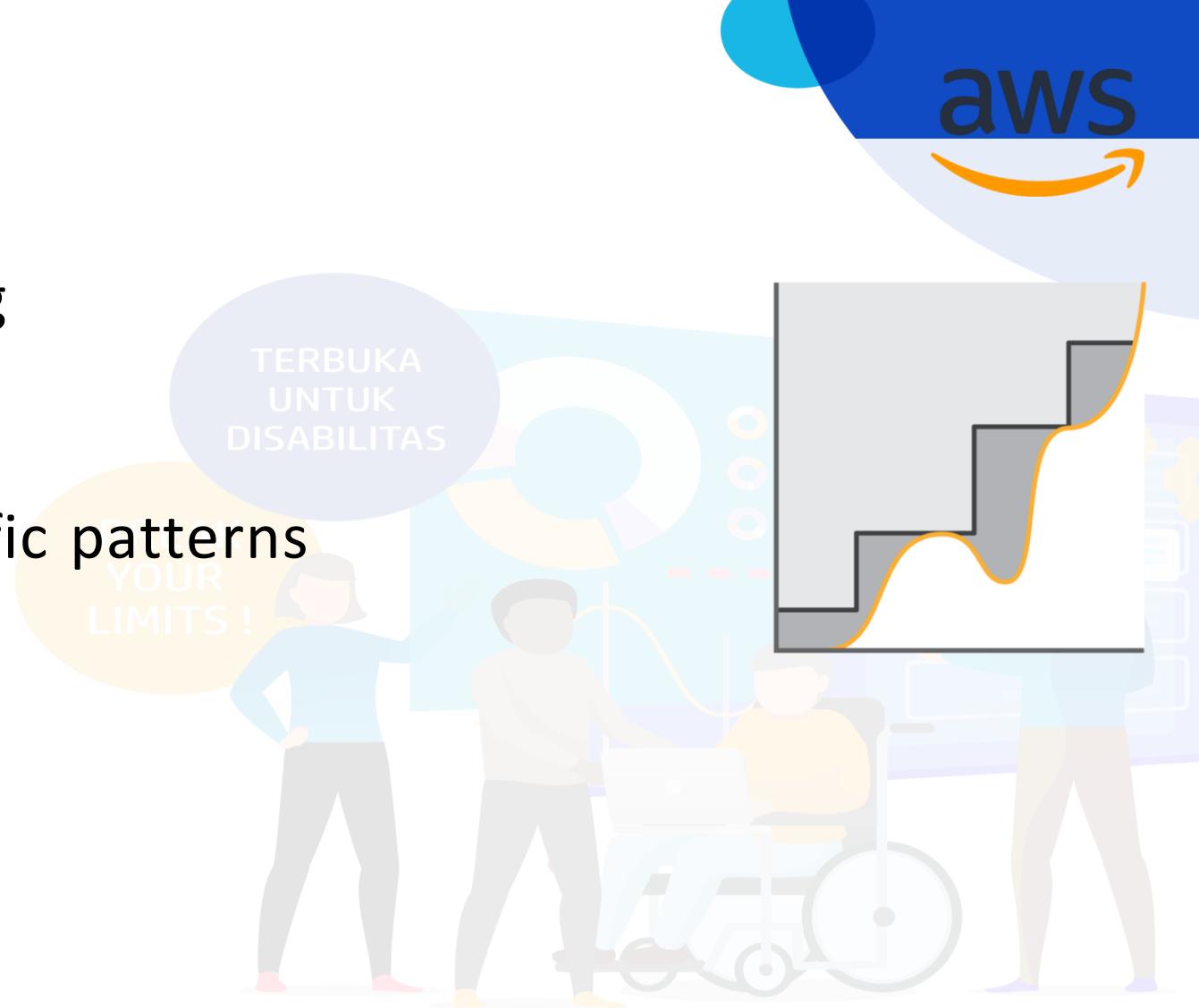
Common web applications:

- ▶ Company website
- ▶ Content management system
- ▶ Social media application development
- ▶ Internal SharePoint site



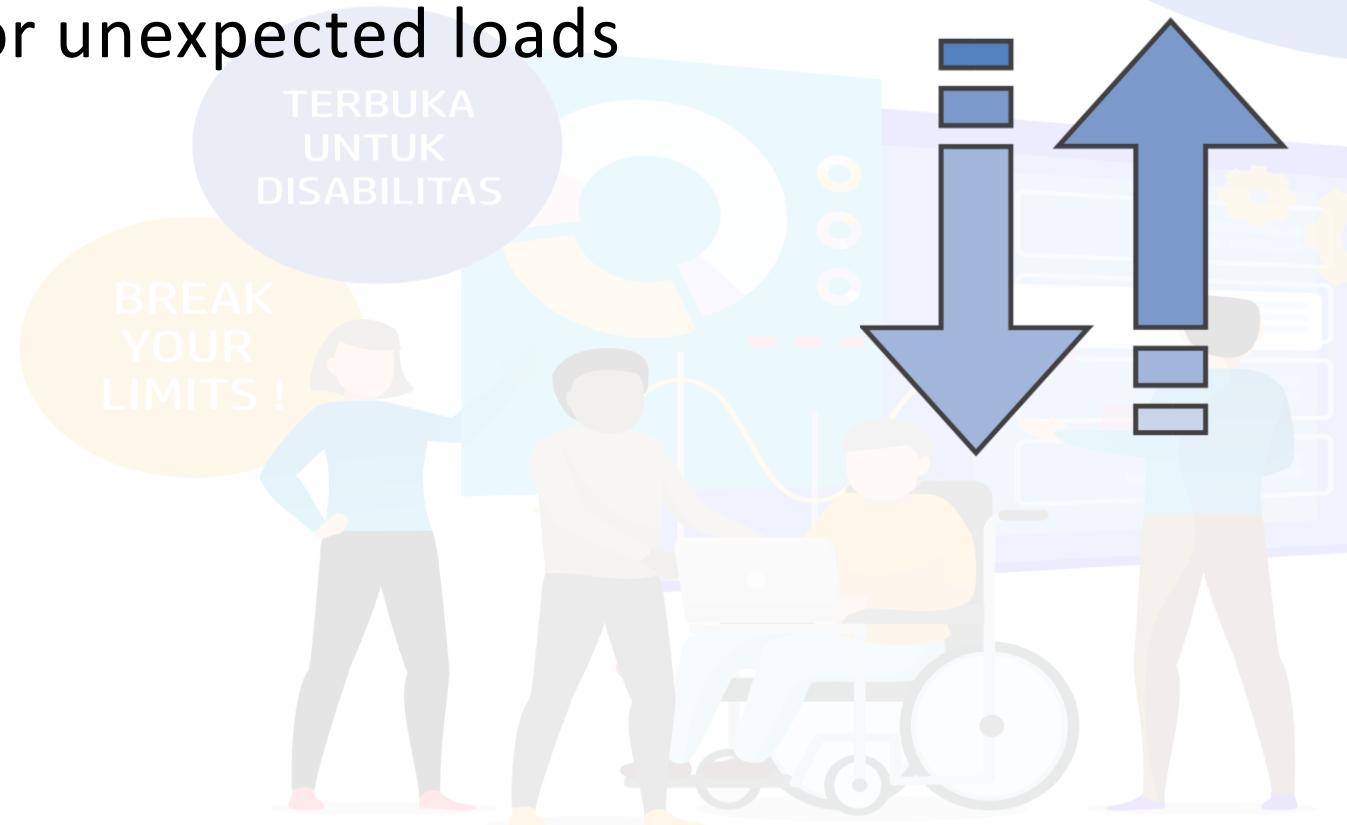
Alternative

- Leverage on-demand provisioning
- Eliminate wasted capacity
- Continuously adjust to actual traffic patterns



e

- Handle unexpected traffic peaks or unexpected loads
- Launch new hosts in minutes
- Scale hosts up or down





On-Demand Solution for Various Environments



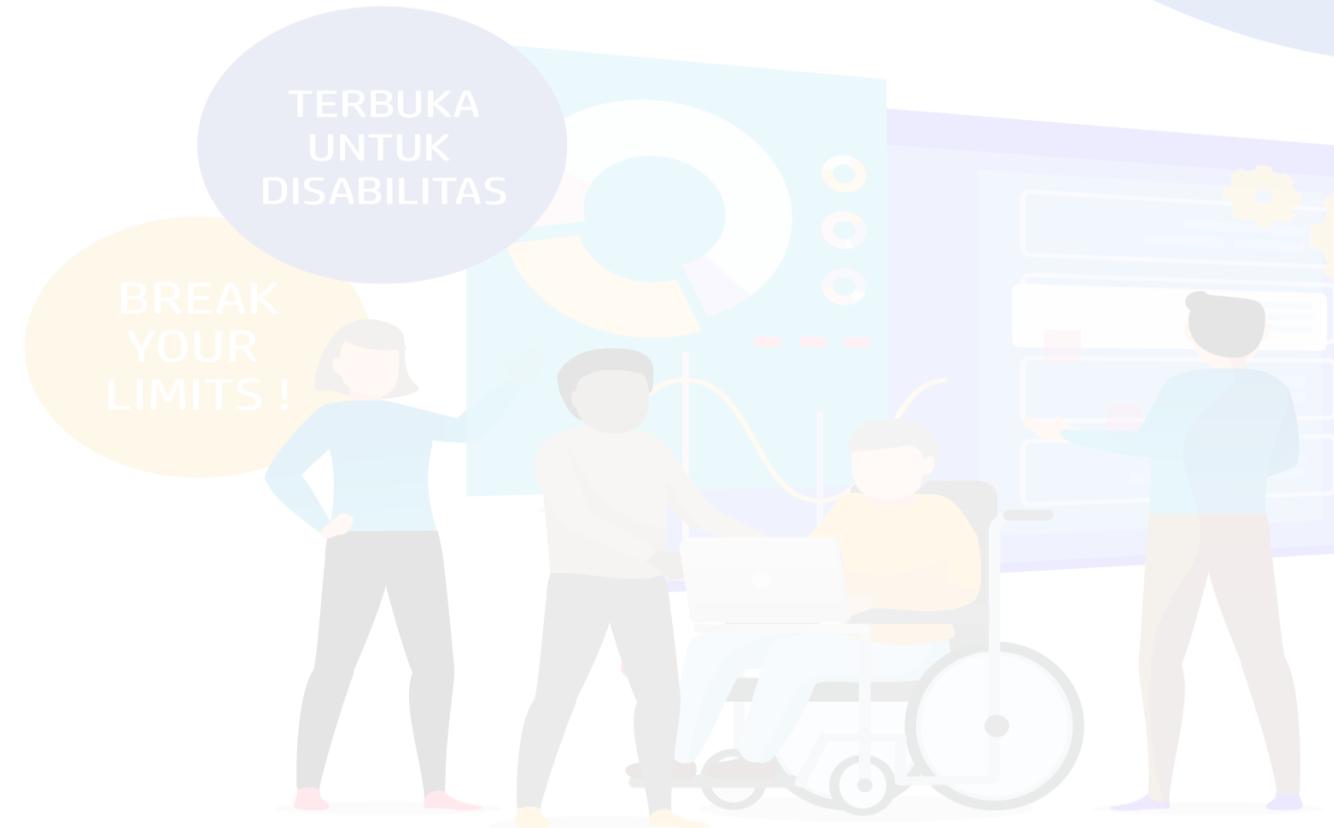
- Provision testing fleets
- Develop staging in minutes
- Simulate user traffic



Migrating to AWS Web Hosting Services

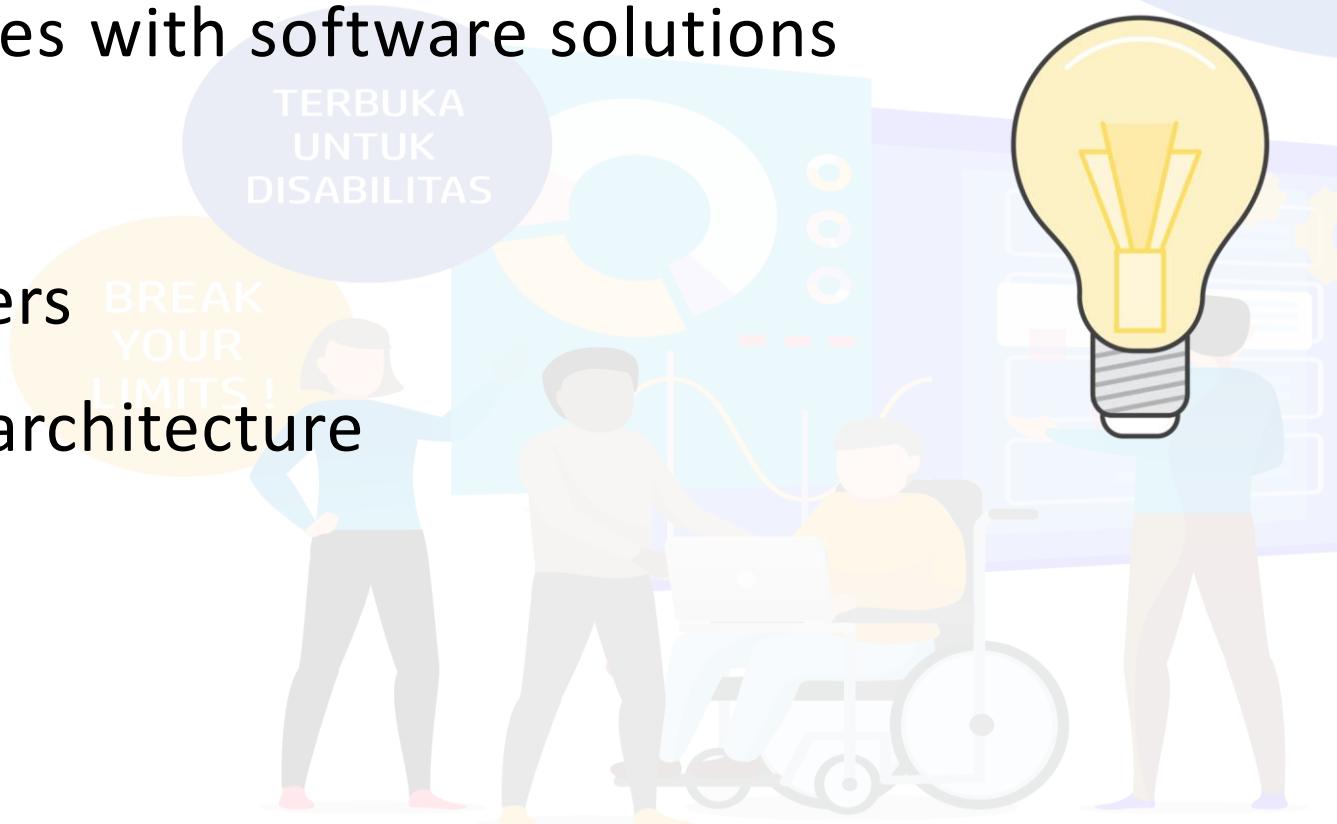
Products to assist transition:

- P Amazon Virtual Private Cloud
- P Amazon Route 53
- P Amazon CloudFront
- P Elastic load balancing
- P Firewalls/AWS Shield
- P Auto Scaling
- P App servers/EC2 instances
- P Amazon ElastiCache
- P Amazon RDS/Amazon DynamoDB



Key Architectural Considerations

- Replace physical network appliances with software solutions
- Deploy firewalls everywhere
- Make available multiple data centers
- Build an ephemeral and dynamic architecture





y

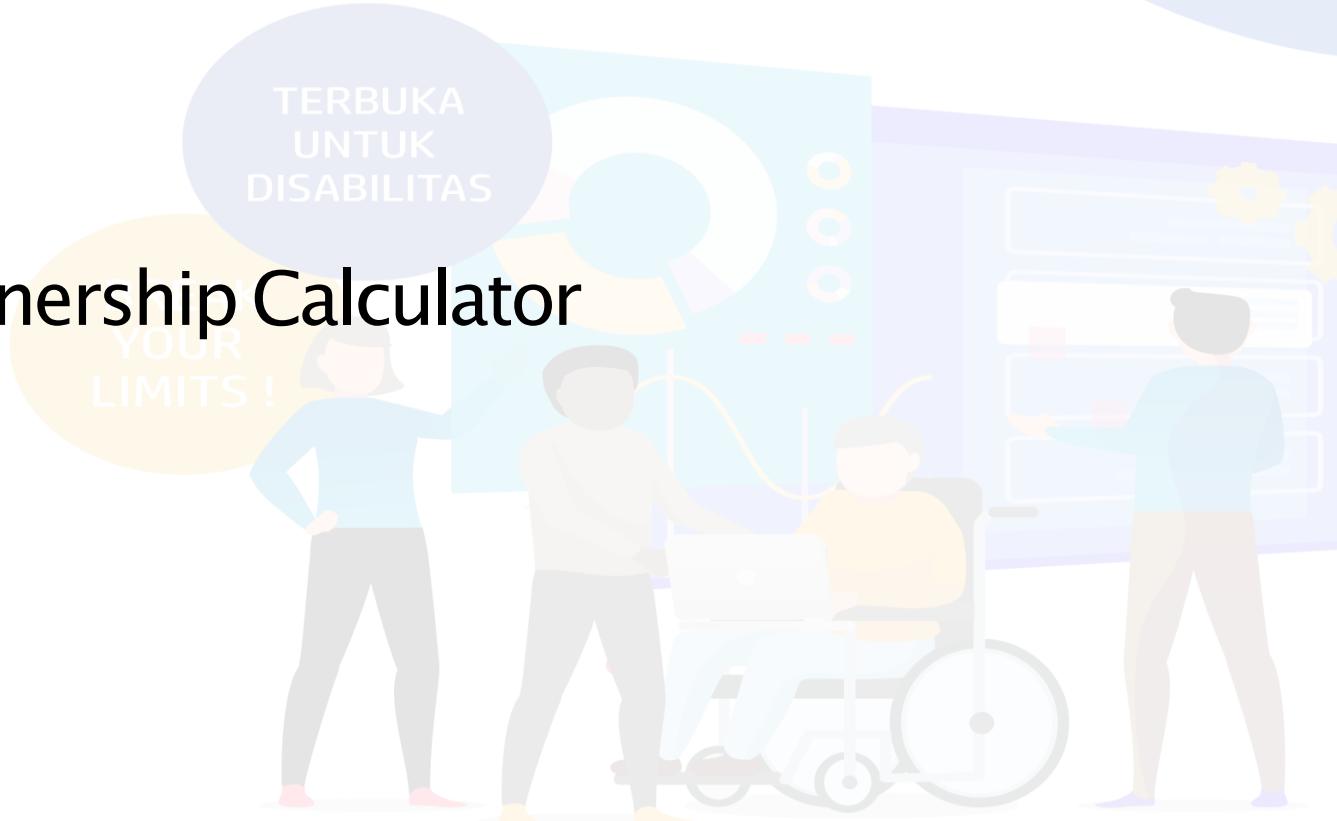
- AWS and web hosting
- AWS web hosted services
- Key considerations for web hosted architectures





Module 5: Pricing Overview

- Fundamentals of Pricing
- Pricing Details
- Overview of the Total Cost of Ownership Calculator



Fundamentals of Pricing

TERBUKA
UNTUK
DISABILITAS

BREAK
LIMES!



Model

- Pay-as-you-go
- Pay less when you reserve
- Pay even less per unit by using more
- Pay even less as AWS grows





Pay-As-You-Go



Pay only for the services you consume, with no large upfront expenses.

- Lower variable costs
- Pay only as long as you need the service
- Adapt to changing business needs
- Redirect focus on innovation and invention



Reserve

Invest in reserved instances

- Save up to 75%
- Options
 - ▶ All Upfront
 - ▶ Partial Upfront
 - ▶ No Upfront payments



More

Realize volume-based discounts

- Savings as usage increases
- Tiered pricing for services (for example, Amazon S3, Amazon EC2)
- No charge for inbound data transfer
- Storage services options



Grows

As AWS grows

- Focuses on lowering cost of doing business
- Passes savings from economies of scale down to you



Pricing

Meet varying needs through custom pricing

- Available for high-volume projects with unique requirements



Tier

■ AWS Free Tier helps customer get started in the cloud

■ Limitations:

▶ Up to one year

▶ Certain services and options

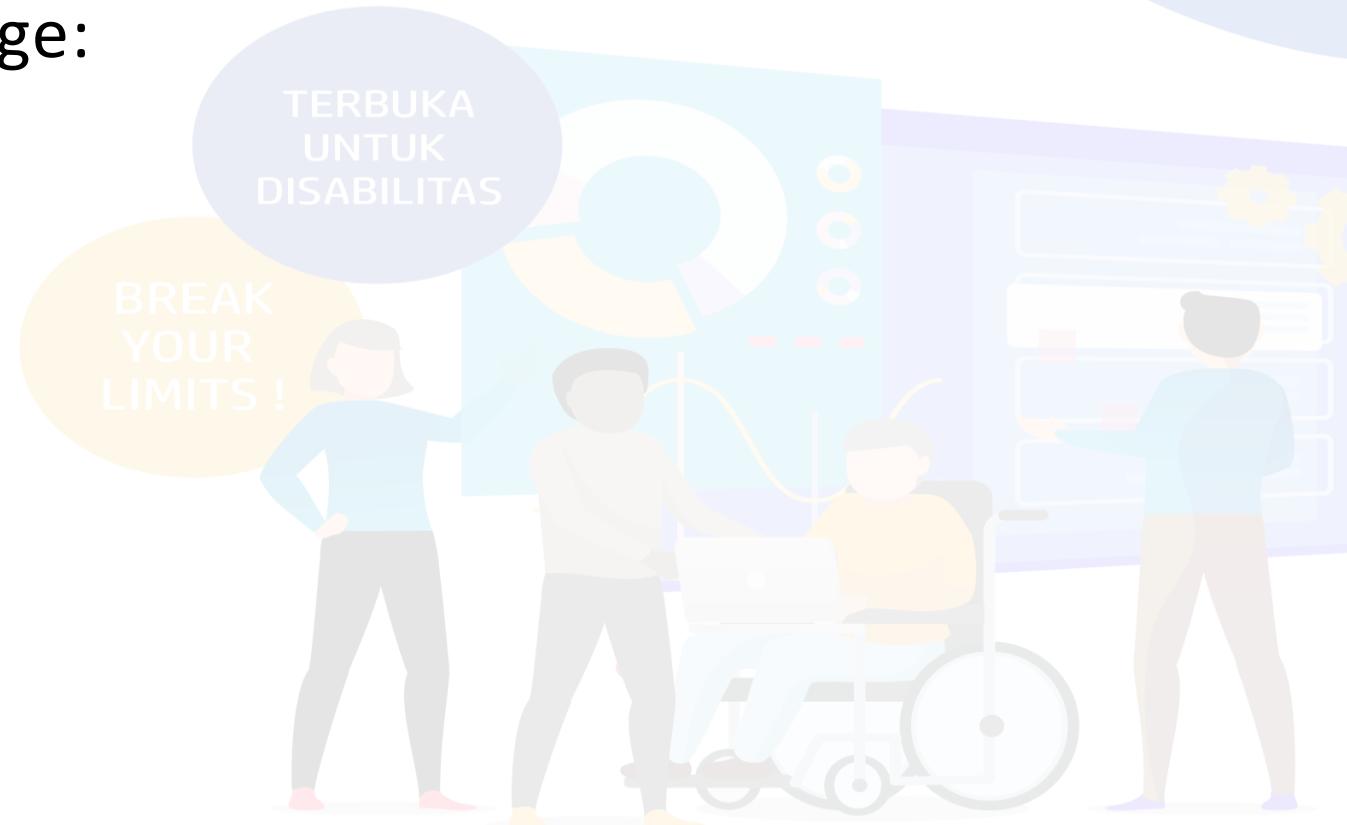
For more details, see: <https://www.aws.amazon.com/free>



Charge

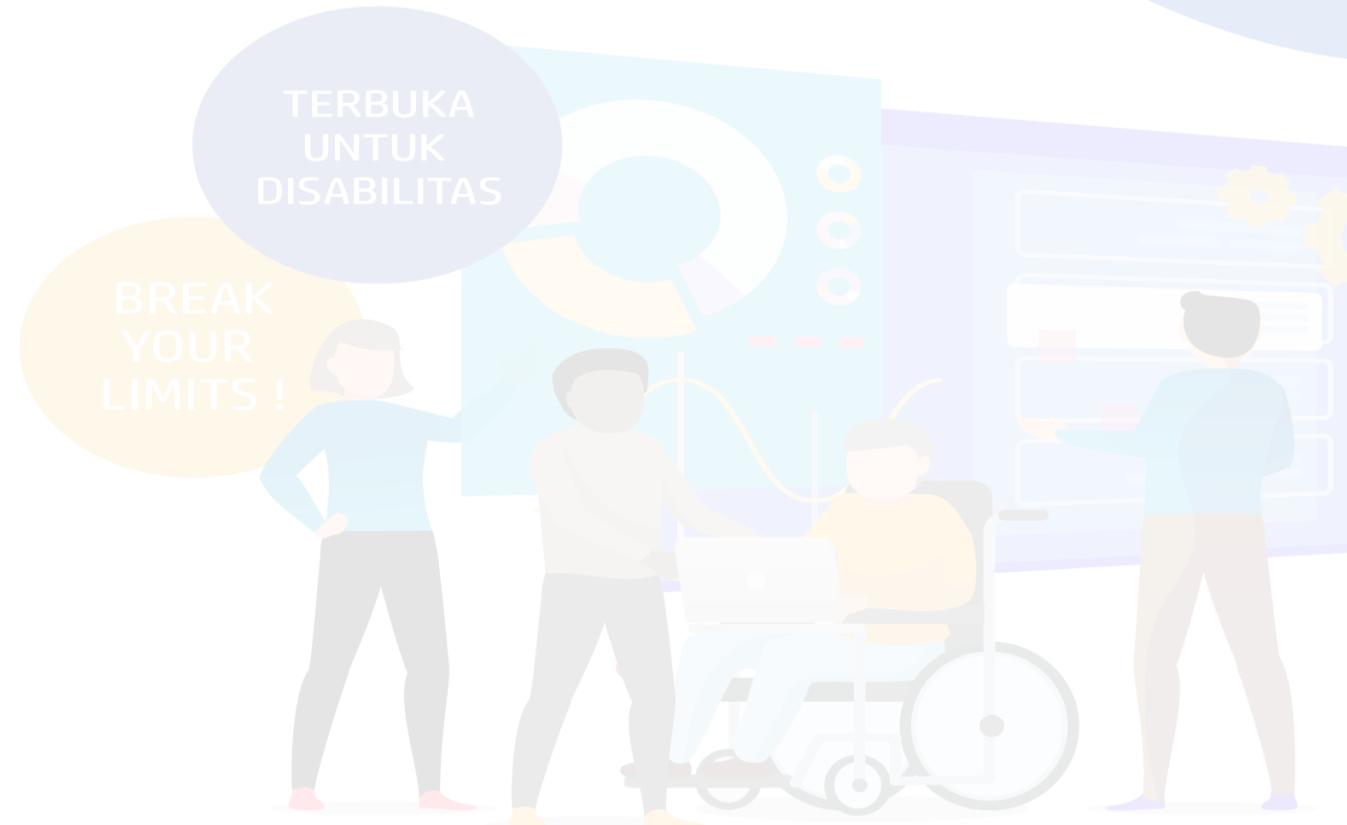
AWS services for no additional charge:

- Amazon VPC
- AWS Elastic Beanstalk
- AWS CloudFormation
- AWS IAM
- Auto Scaling



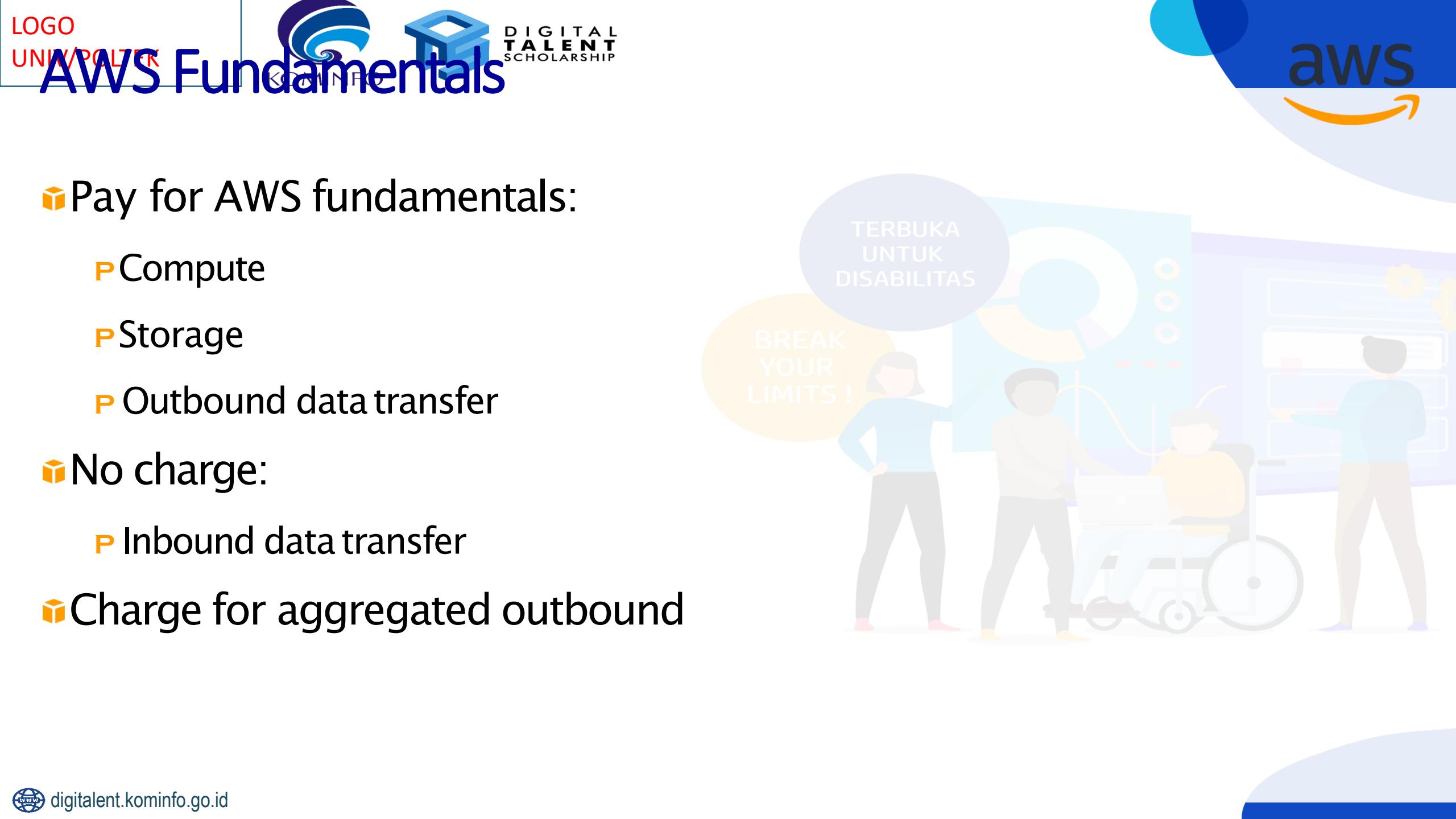
y

- Pay only for what you use
- Start and stop anytime
- No long-term contracts required



Pricing Details





AWS Fundamentals

💡 Pay for AWS fundamentals:

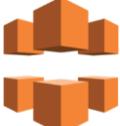
- ▶ Compute
- ▶ Storage
- ▶ Outbound data transfer

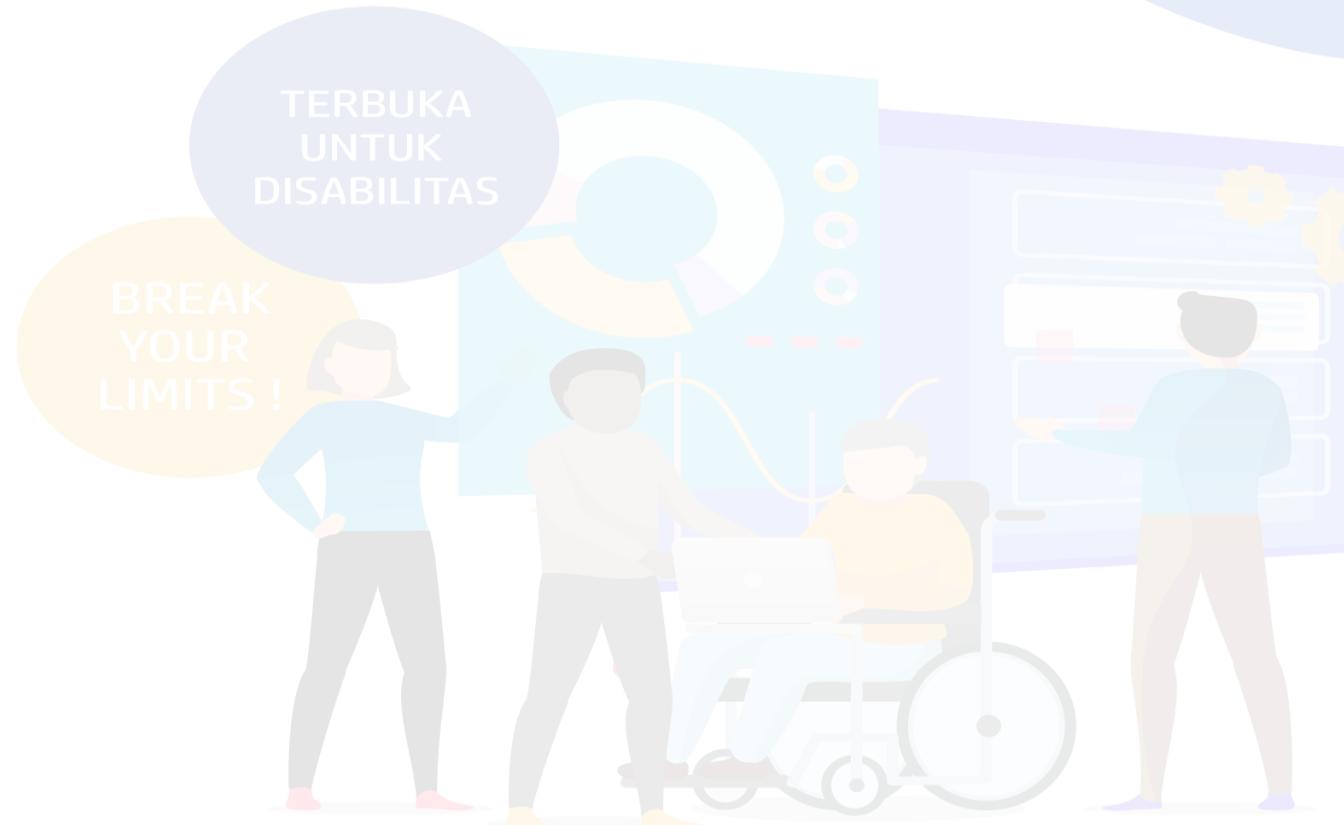
💡 No charge:

- ▶ Inbound data transfer

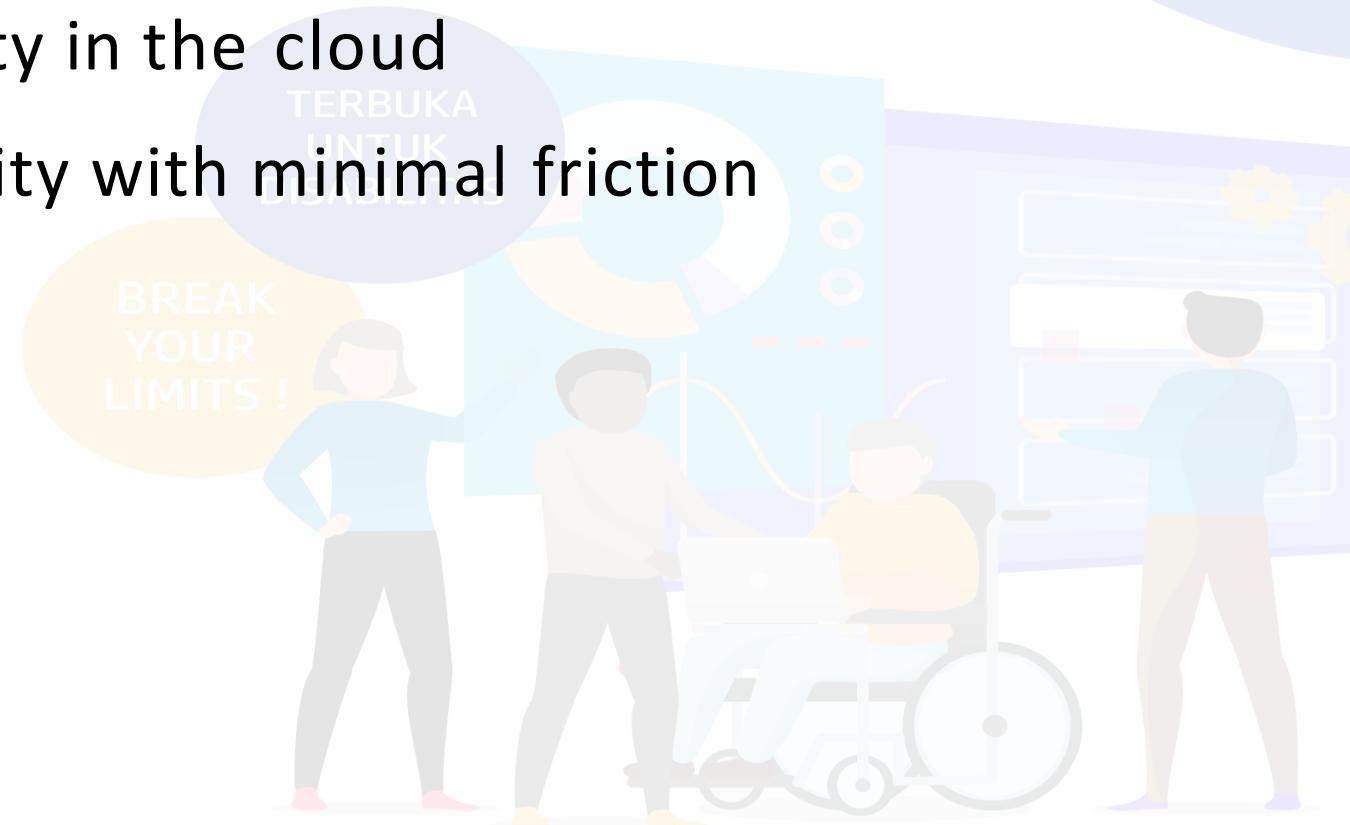
💡 Charge for aggregated outbound

Service Pricing for AWS Offerings

-  Amazon EC2
-  Amazon S3
-  Amazon EBS
-  Amazon RDS
-  Amazon CloudFront



- Provide resizable compute capacity in the cloud
- Allows the configuration of capacity with minimal friction
- Provides complete control
- Charges only for capacity used





Amazon EC2: Billing and Instance Configuration



Clock-Second/Hourly Billing

- (Resources incur charges only when running)

Instance Configuration

- Physical capacity of the instance

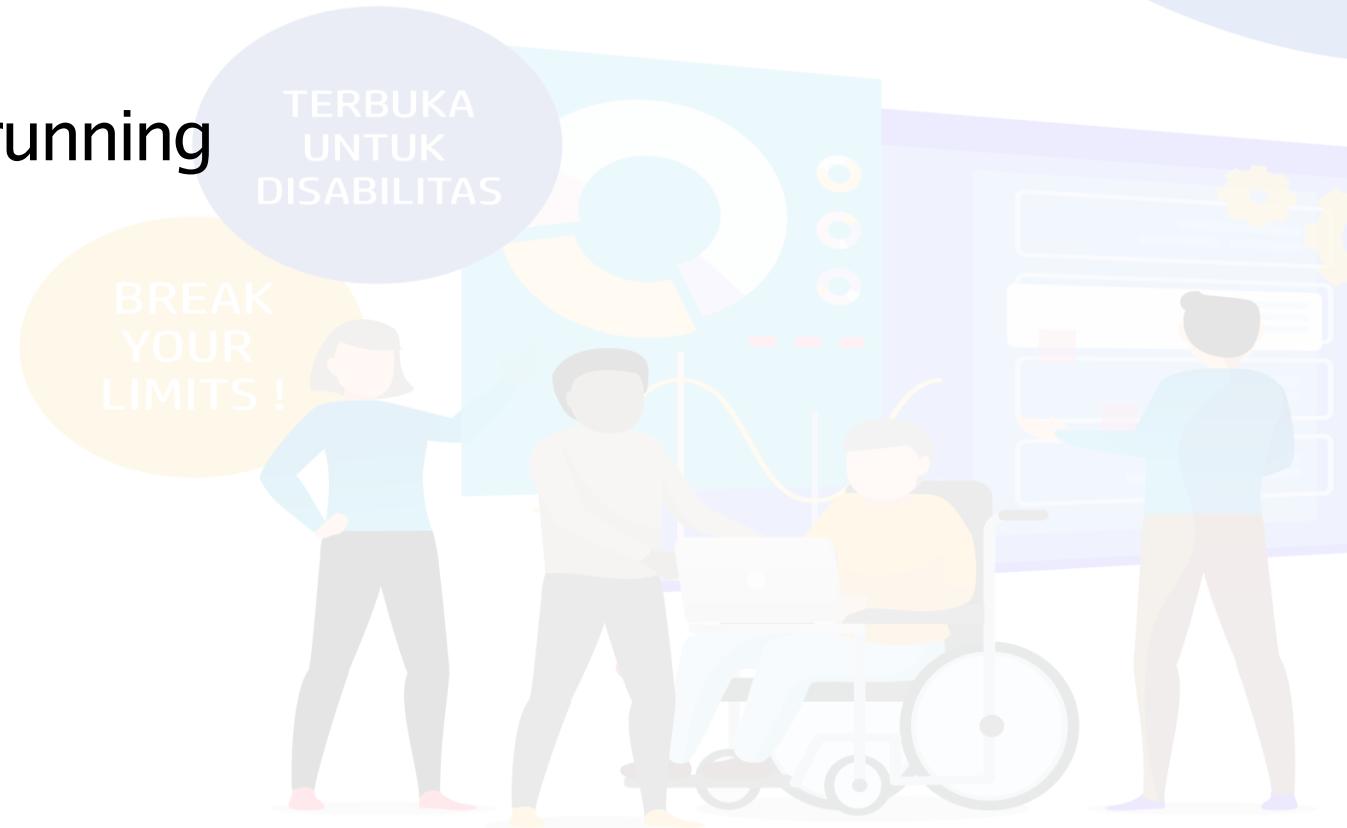
- Pricing varies with:

 - P AWS region

 - P OS

 - P Instance Type

 - P Instance Size



Ways to pay for Amazon EC2 instances

■ On-demand instances

- ▶ Compute capacity by the hour and second
- ▶ Minimum of 60 seconds

■ Reserved Instances

- ▶ Low or no up-front payment instances reserved
- ▶ Discount on hourly charge for that instance

■ Spot Instances

- ▶ Bid for unused Amazon EC2 capacity



Number of Instances

- Provision multiple instances to handle peak loads

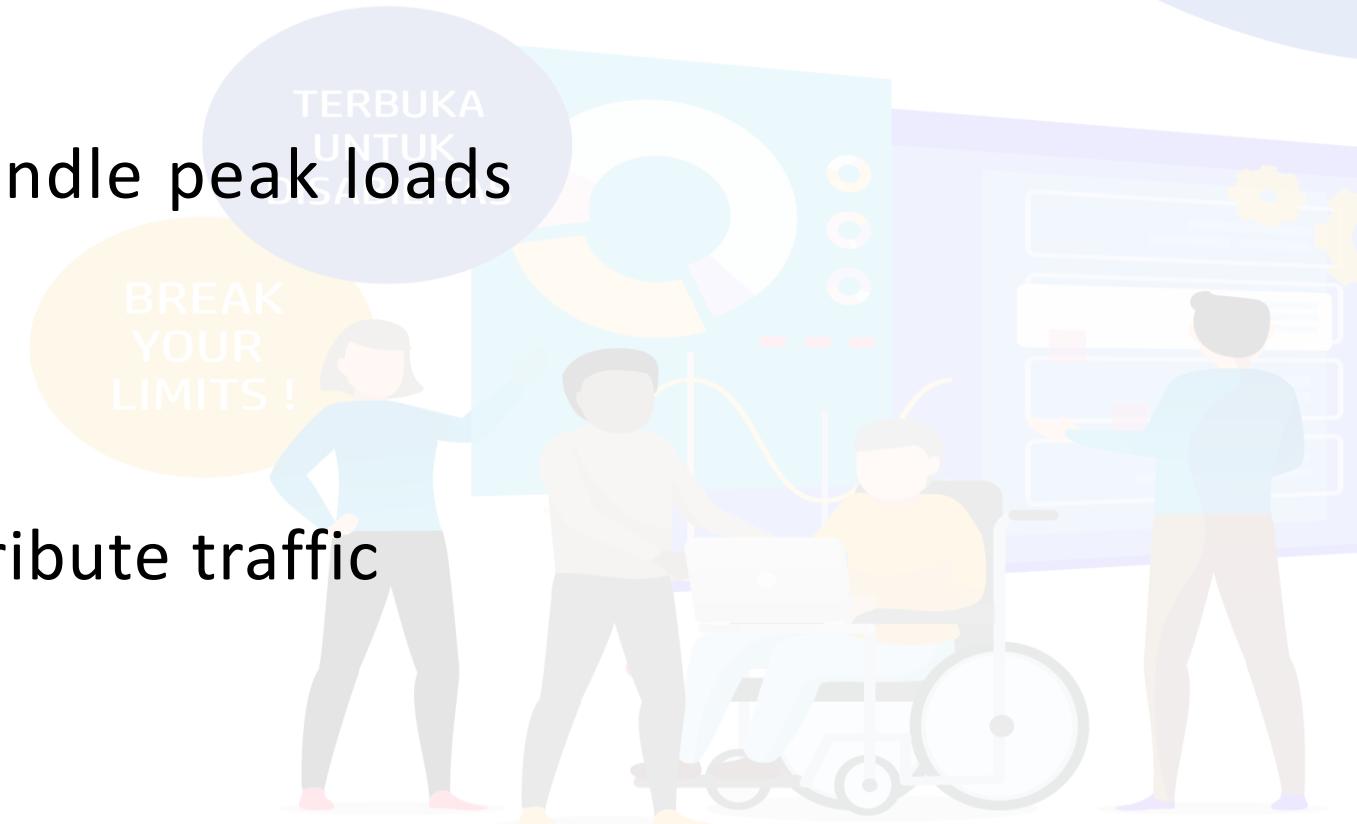
Load Balancing

Uses Elastic Load Balancing to distribute traffic

- Calculates monthly cost based on

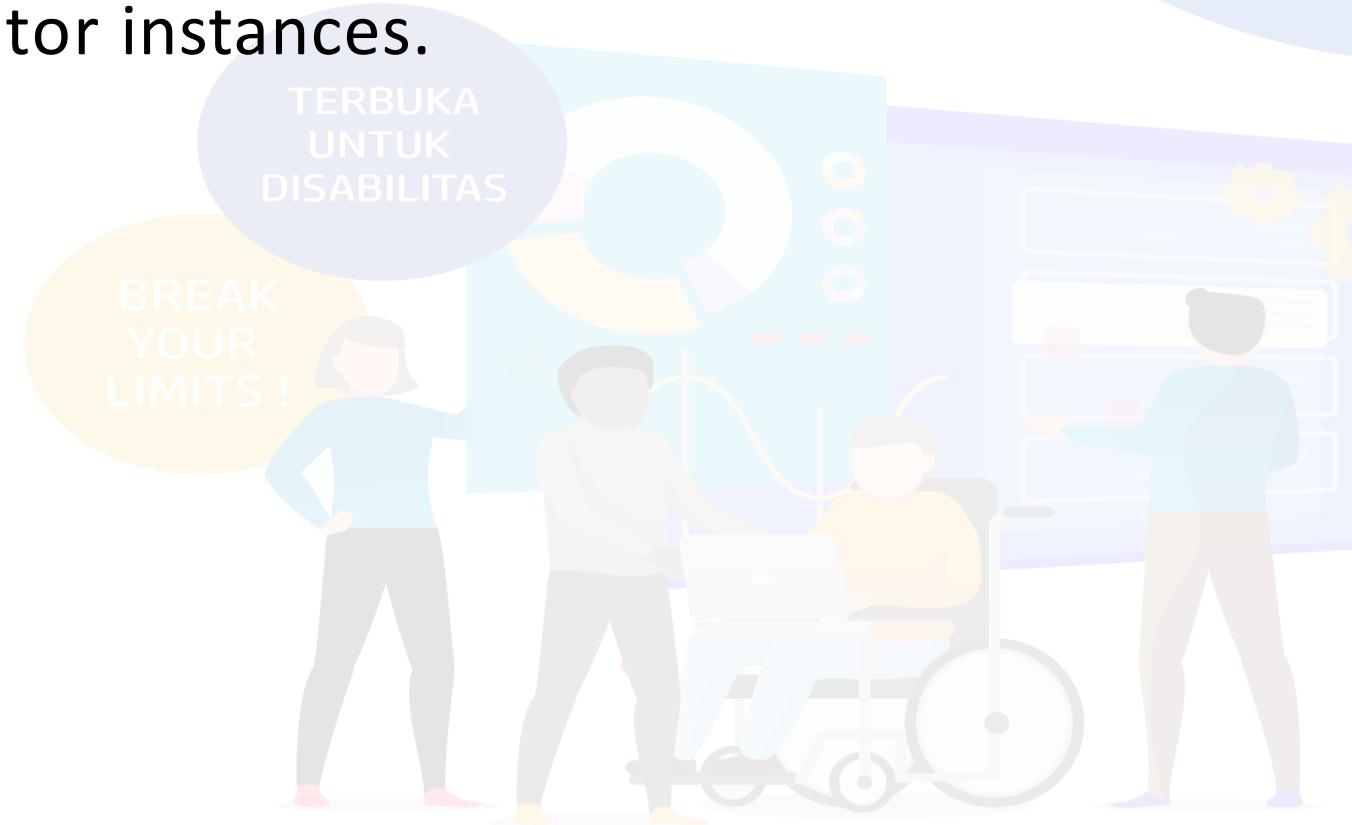
 ■ Hours load balancer runs

 ■ Data load balancer processes



Monitoring

- Use Amazon CloudWatch to monitor instances.
- Basic monitoring (default)
- Detailed monitoring
 - Fixed monthly rate
 - Prorated partial months



Auto Scaling

- Automatically adjusts number of instances
- Incurs no additional charge

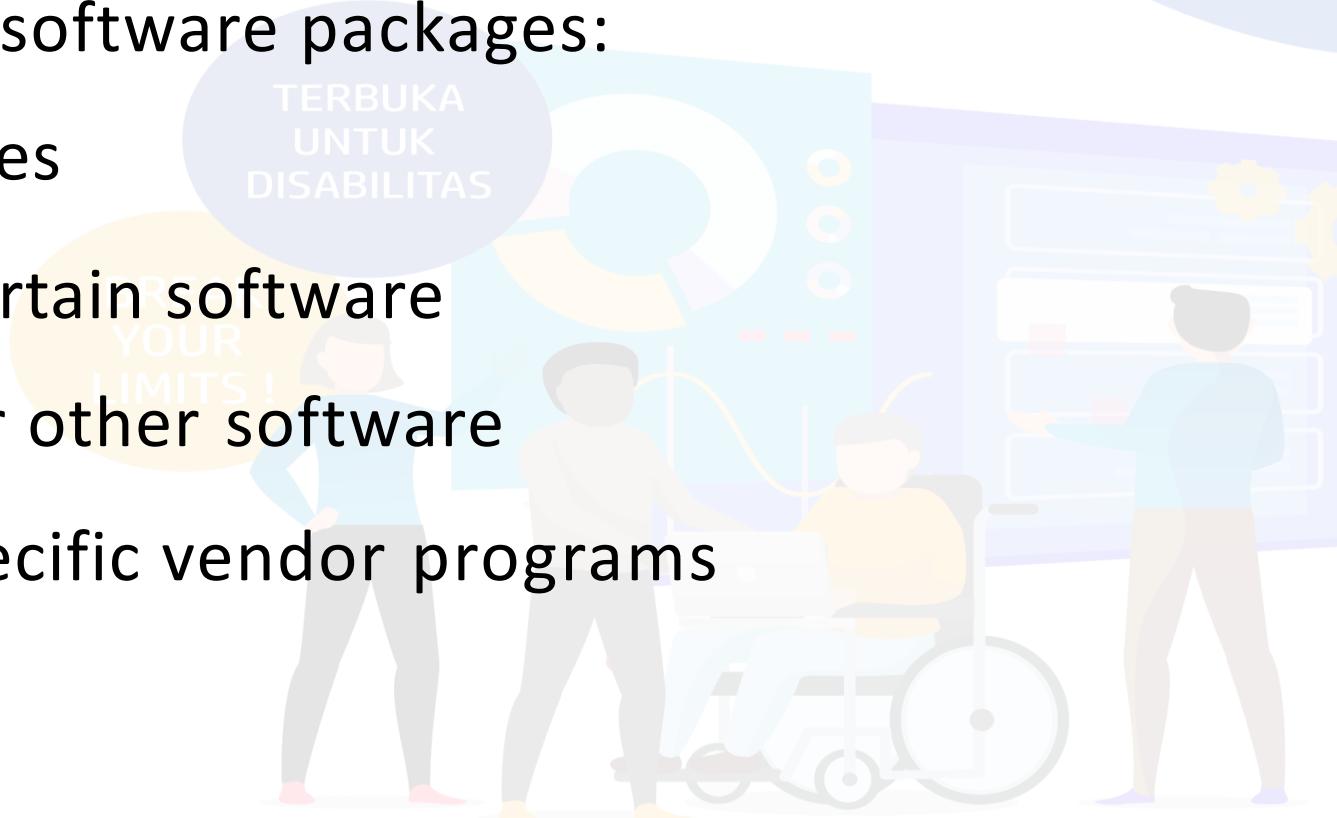
Elastic IP Addresses

- No charge for one Elastic IP address associated with a running instance.



Software

- Pricing for operating systems and software packages:
- Includes OS prices in instance prices
- Partners with other vendors for certain software
- Requires licenses from vendors for other software
- Brings existing license through specific vendor programs



Classes

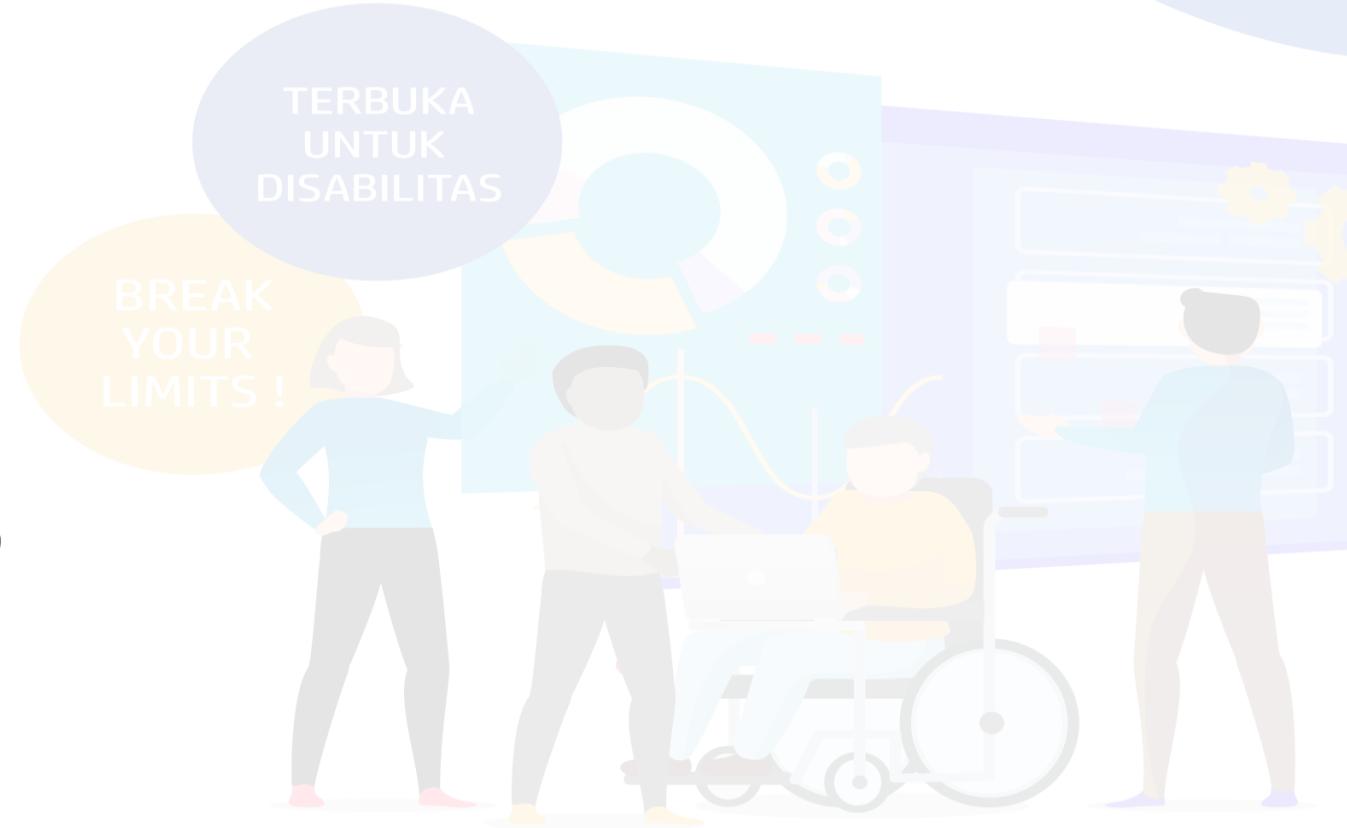
Types of storage classes

Standard Storage

- P 99.99999999% durability
- P 99.99% availability

Standard-Infrequent Access (S-IA)

- P 99.99999999% durability
- P 99.9% availability



Storage

Considerations for estimating storage cost

- P The number and size of objects
- P Type of storage



S3

Requests:

Pricing based on

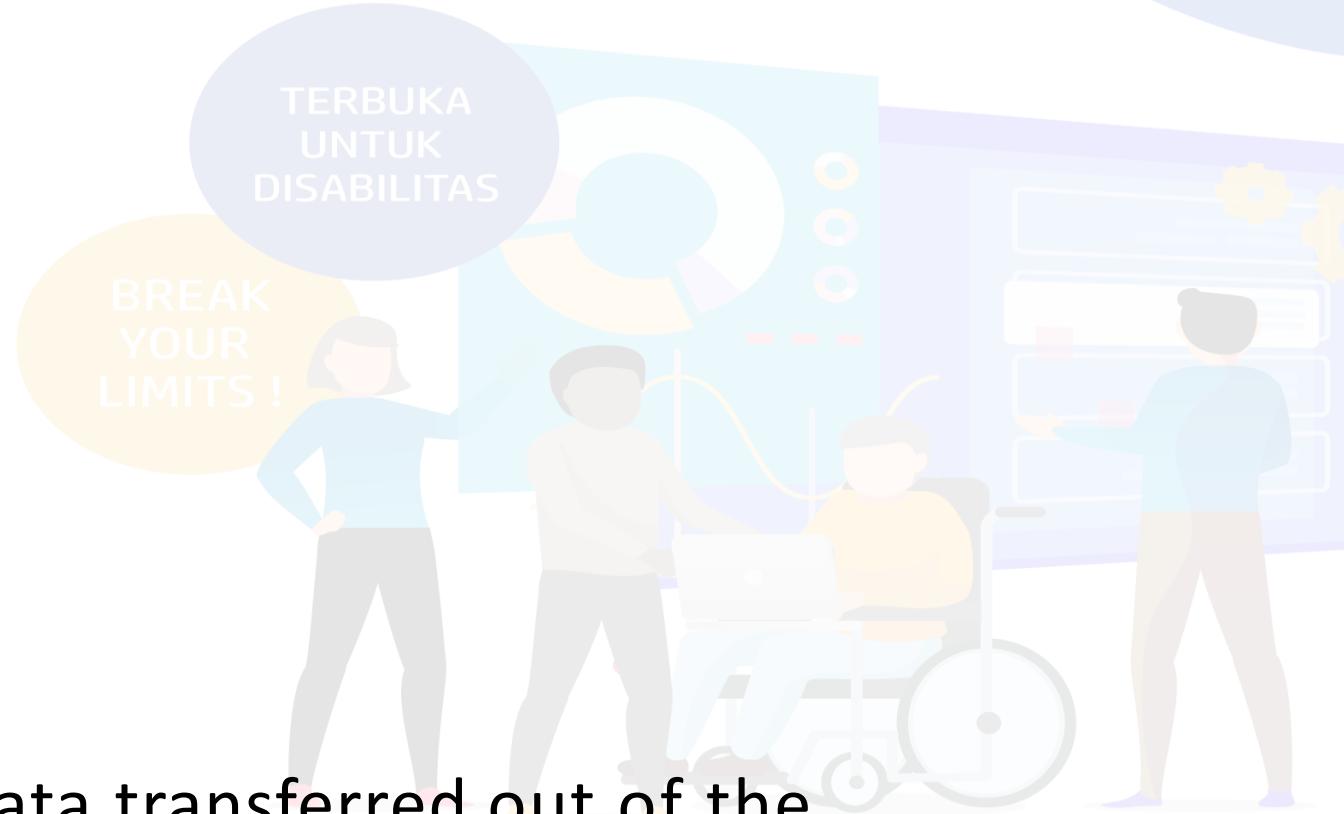
- Number of requests

- Type of requests

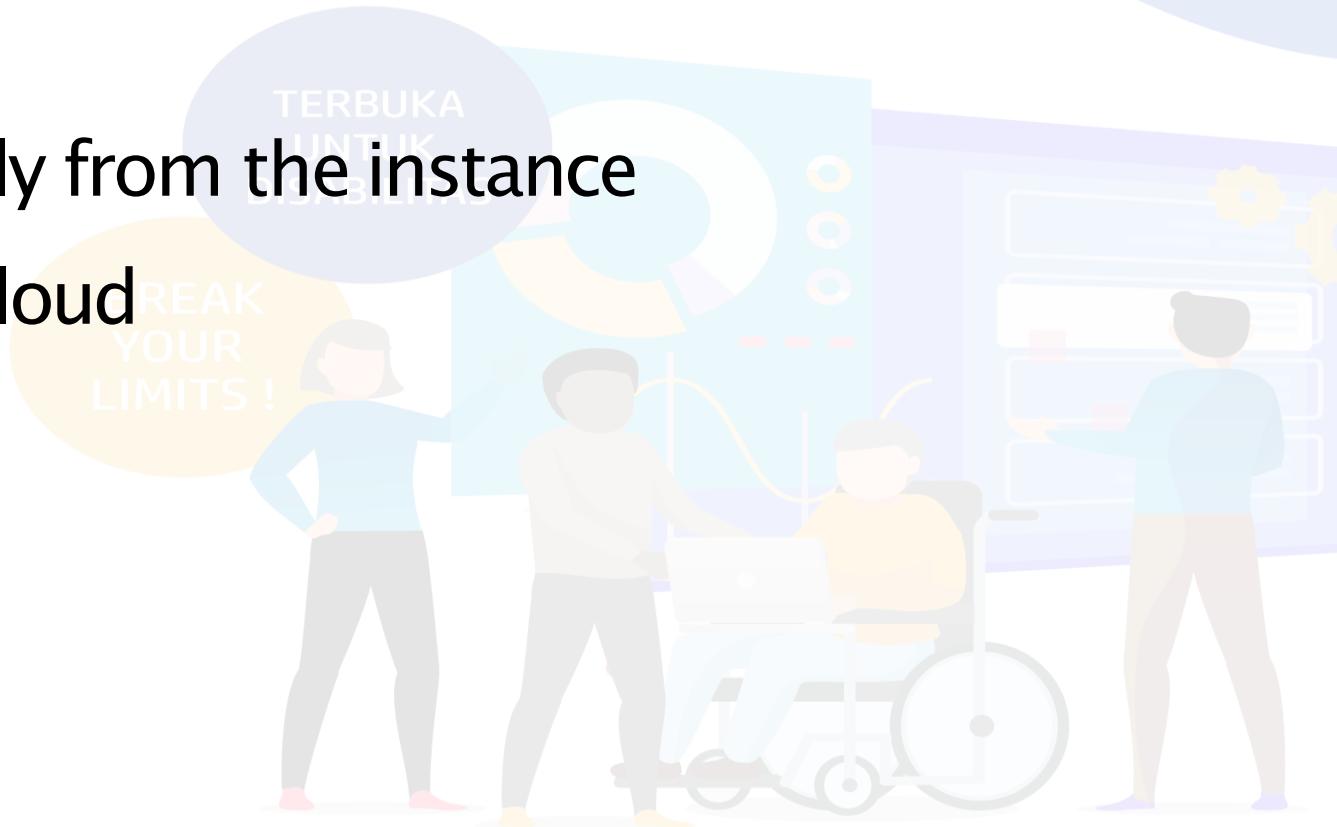
- P Different rates for GET requests

Data Transfer

- Pricing based on the amount of data transferred out of the Amazon S3 region



- Block-level storage for instances
- EBS volumes persist independently from the instance
- Analogous to virtual disks in the cloud
- Three volume types:
 - ▶ General Purpose (SSD)
 - ▶ Provisioned IOPS (SSD)
 - ▶ Magnetic



Volumes

- All volume types are charged by the amount provisioned per month

IOPS

- General Purpose (SSD)

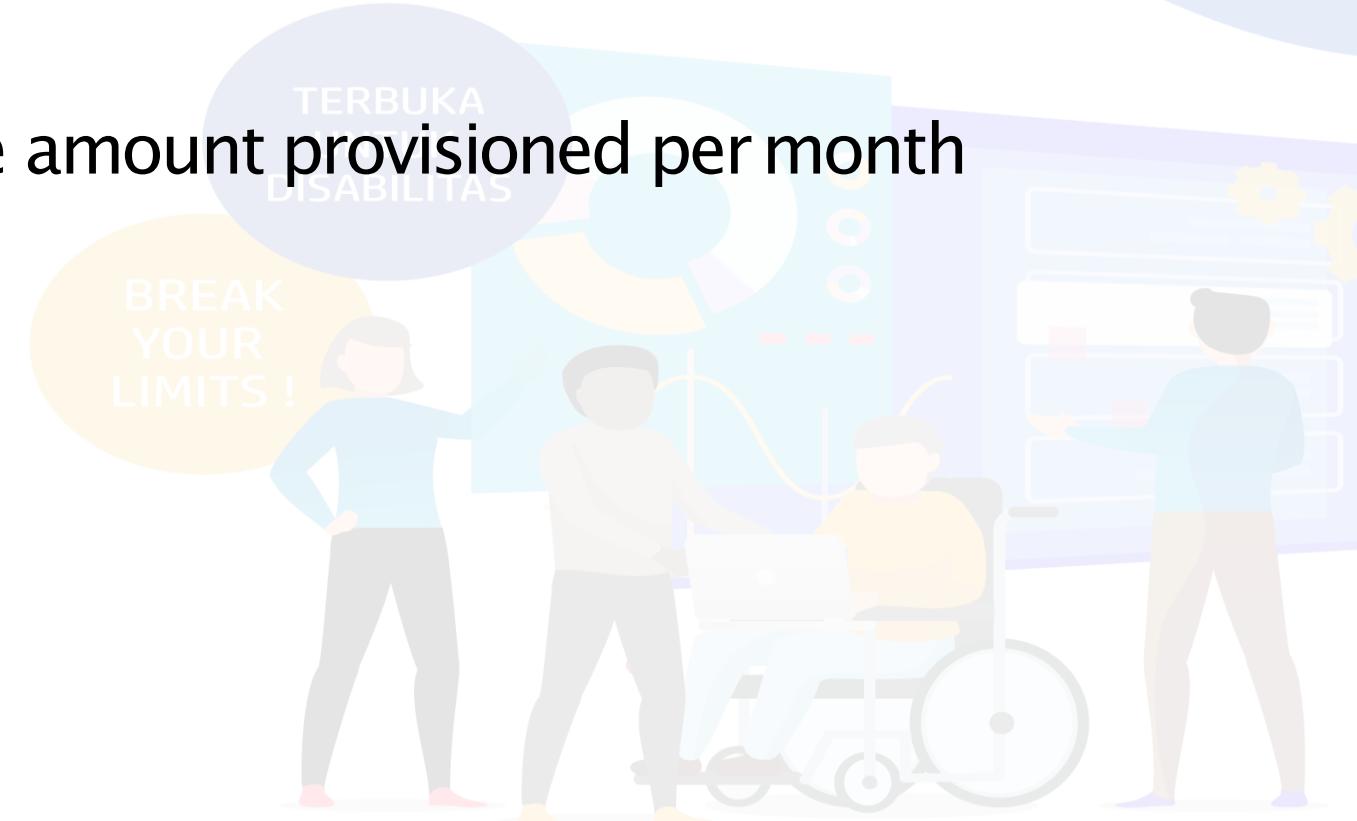
- ▶ Included in price

- Magnetic

- ▶ Charged by the number of requests

- Provisioned IOPS (SSD)

- ▶ Charged by the amount you provision in IOPS





Amazon EBS: Snapshots and Data Transfer

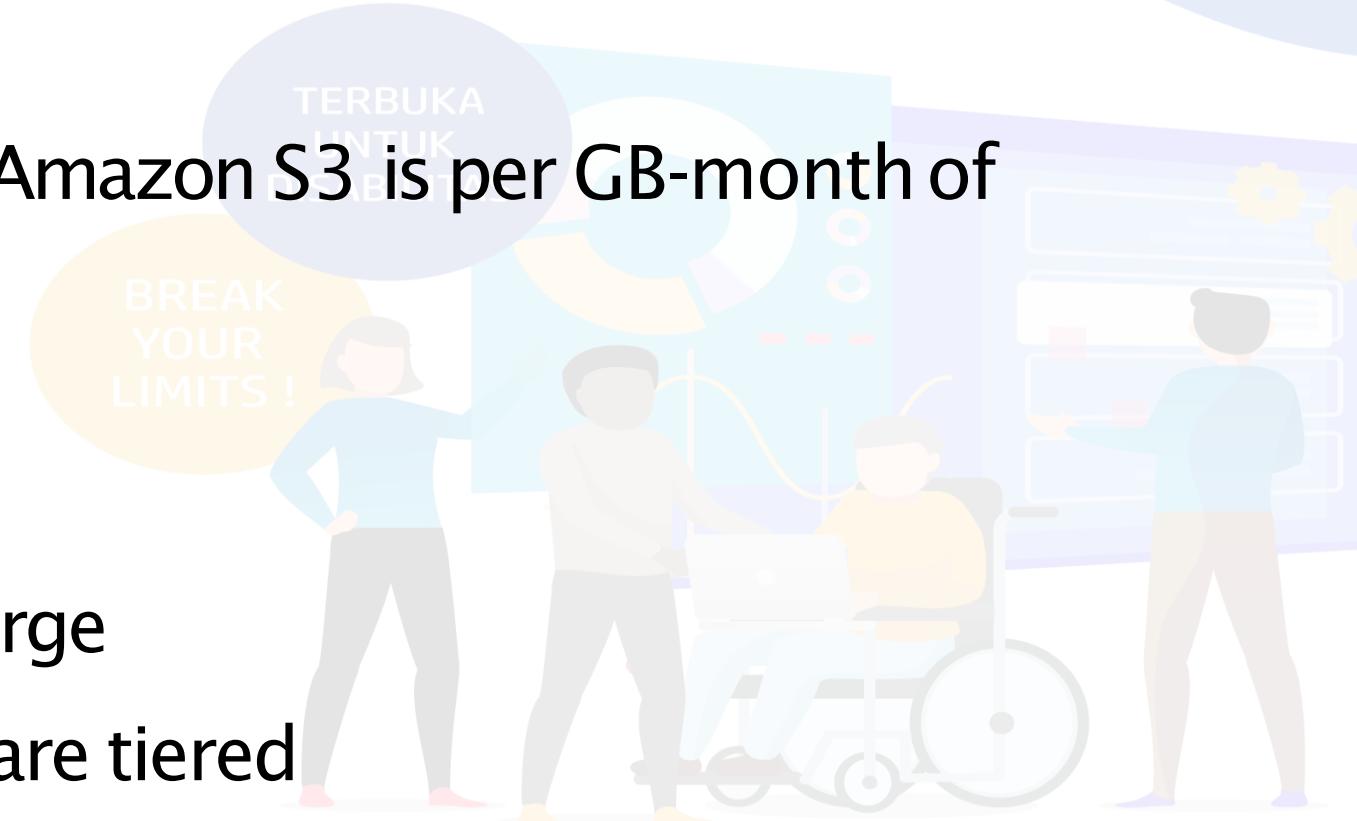


Snapshots

- Added cost of EBS snapshots to Amazon S3 is per GB-month of data stored

Data Transfer

- Inbound data transfer has no charge
- Outbound data transfer charges are tiered



RDS

- Relational database in the cloud
- Cost-efficient and resizable capacity
- Management of time-consuming administrative tasks



Database Characteristics

Clock-Hour Billing

- Resources incur charges when running

Database Characteristics

- Physical capacity of database:

- P Engine

- P Instance Type

- P Instance Size



DB Purchase Type

- On-demand database instances

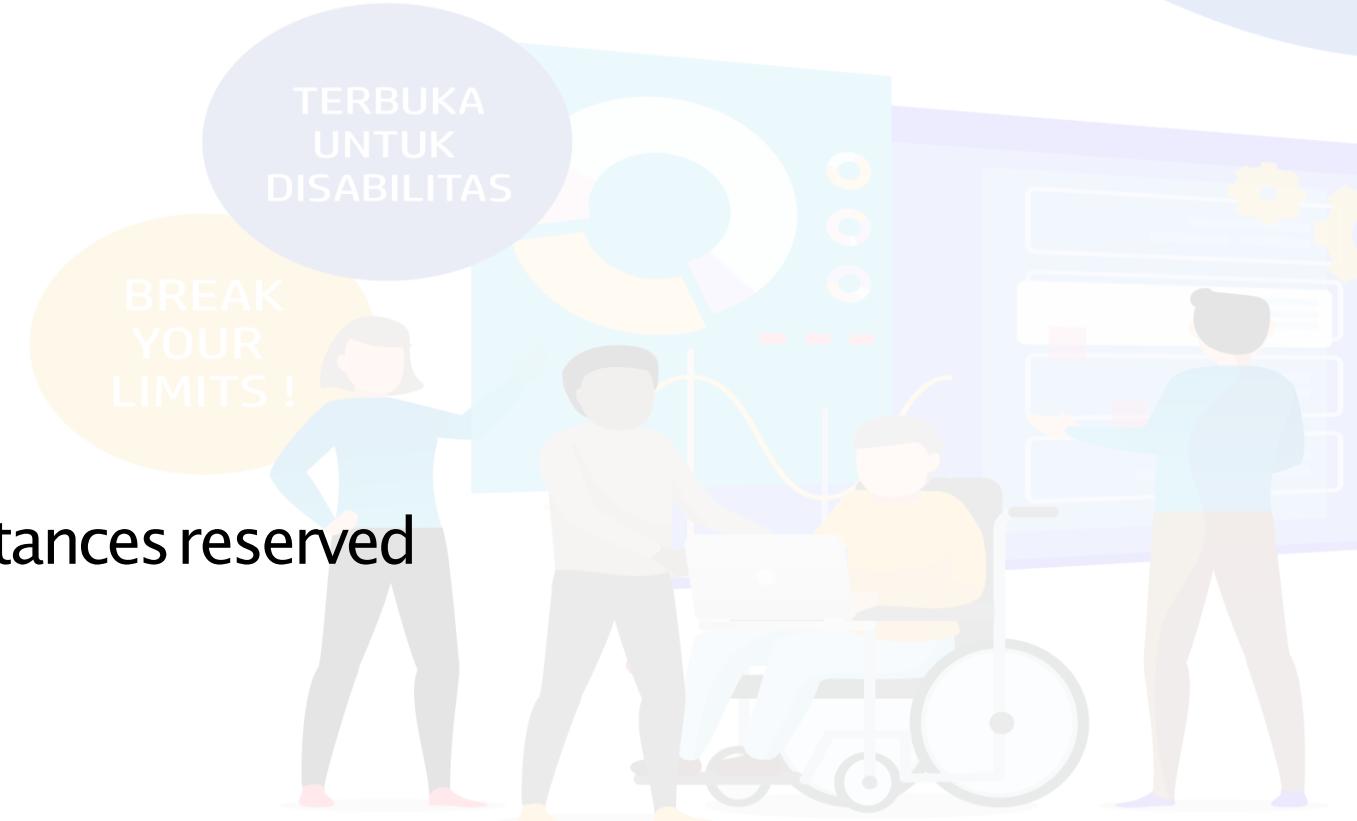
P By the hour

- Reserved database instances

P Up-front payment for database instances reserved

Multiple DB Instances

- Provision multiple DB instances to handle peak loads



Storage

Provisioned Storage

■ No charge

P Backup storage of up to 100% of database storage

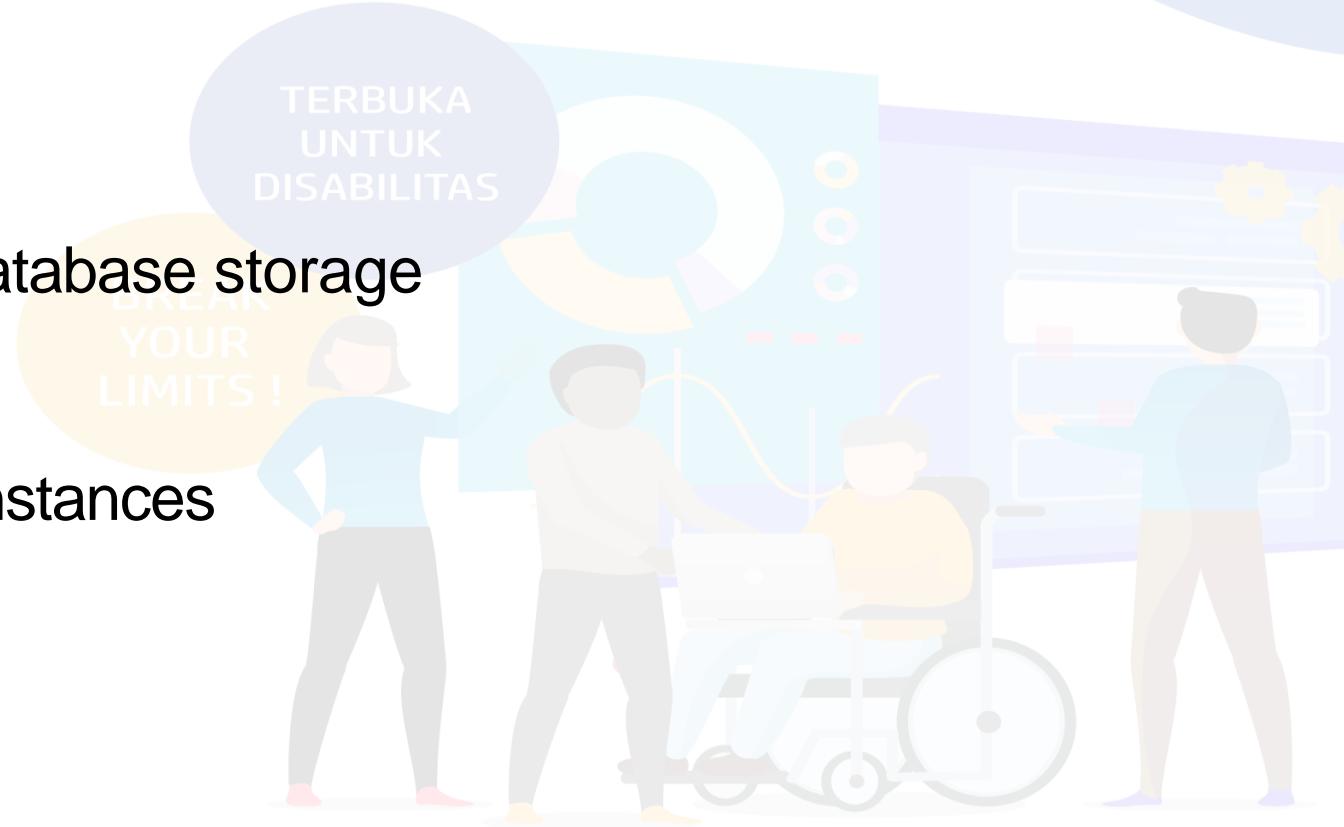
■ Charge (*GB/month*)

P Backup storage for terminated DB instances

Additional Storage

■ Charge (*GB/month*)

P Backup storage in addition to provisioned storage





Amazon RDS: Deployment Type and Data Transfer

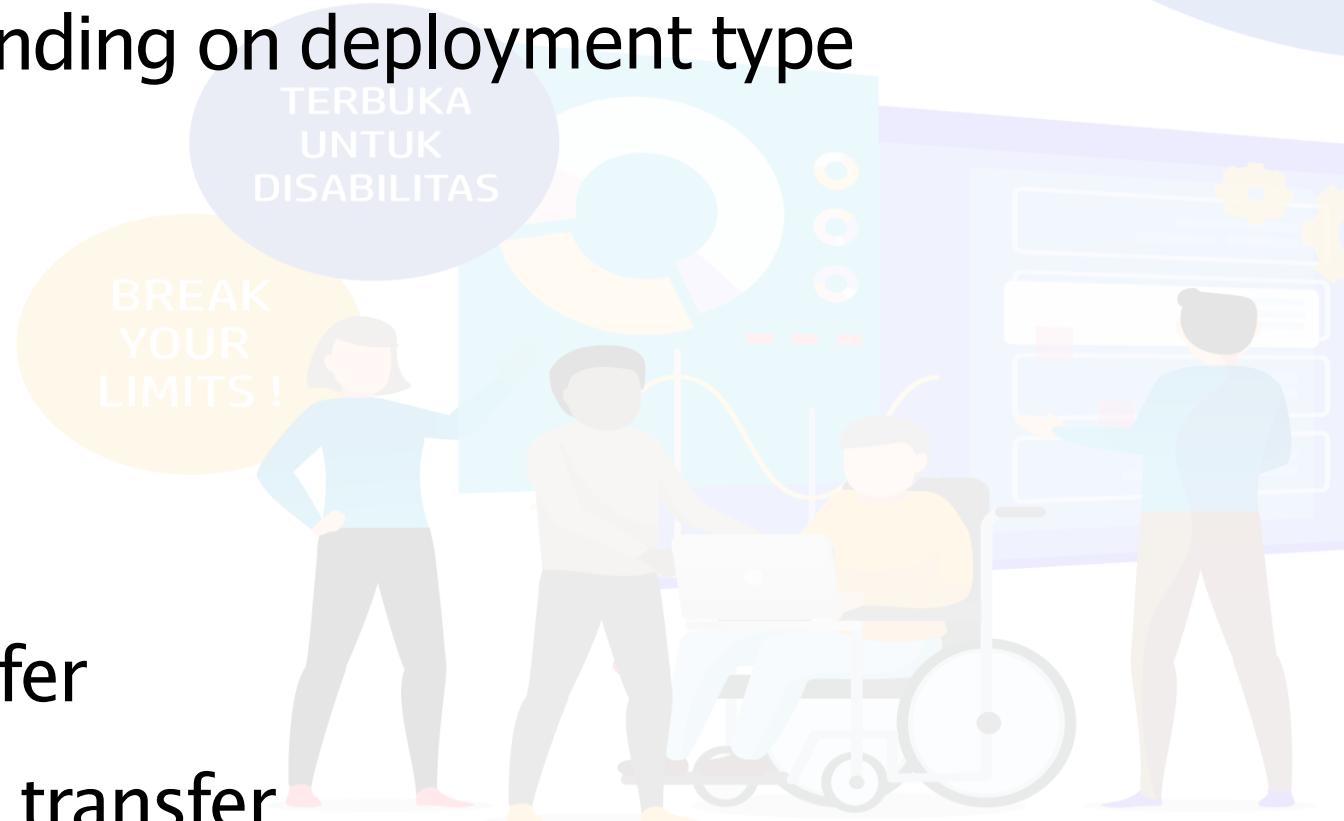


Storage and I/O charges vary depending on deployment type

- Single Availability Zones
- Multiple Availability Zones

Data Transfer

- No charge for Inbound data transfer
- Tiered charges for outbound data transfer



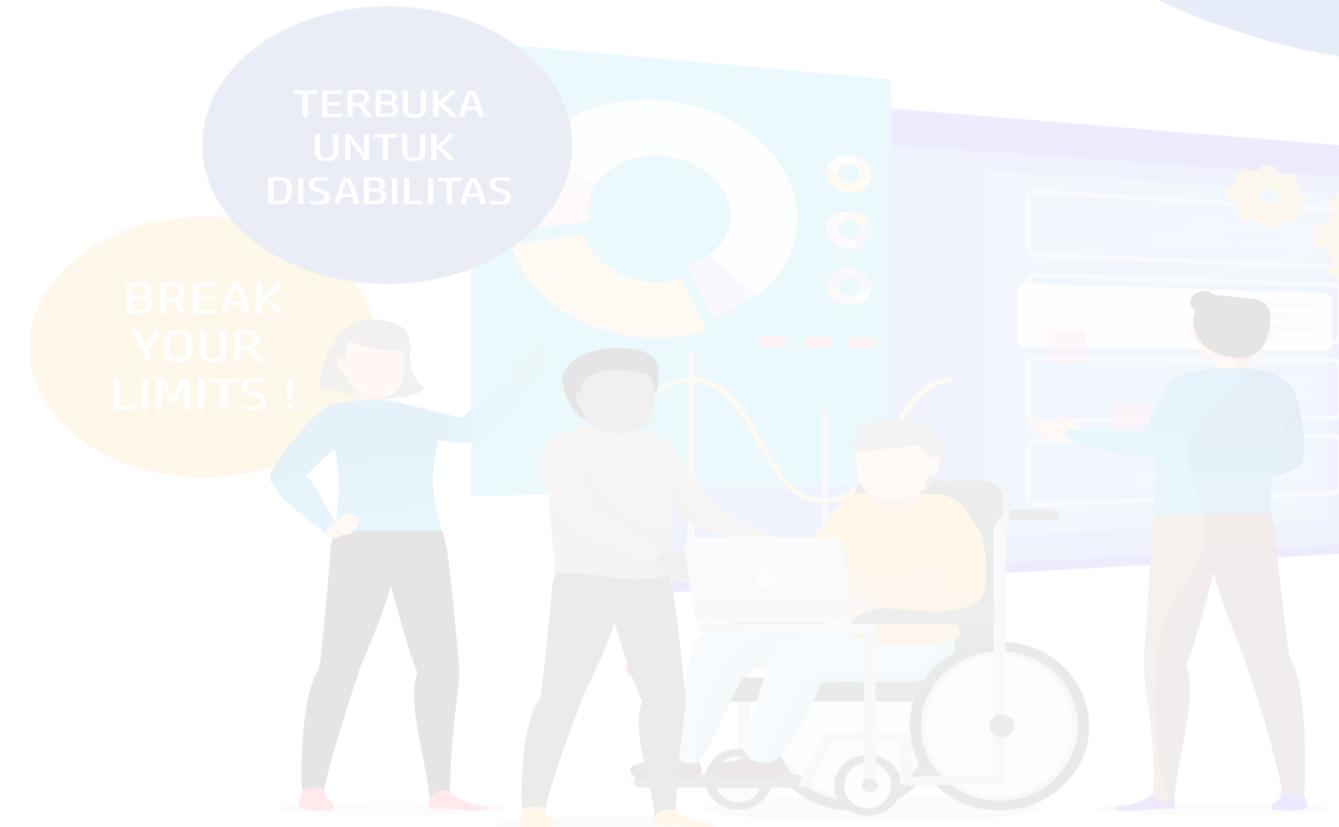
CloudFront

- Web service for content delivery
- Integration with other AWS services
- Low latency
- High data transfer speeds
- No minimum commitments



Pricing

- Vary across geographic regions



Amazon CloudFront: Requests and Data Transfer Out



Requests

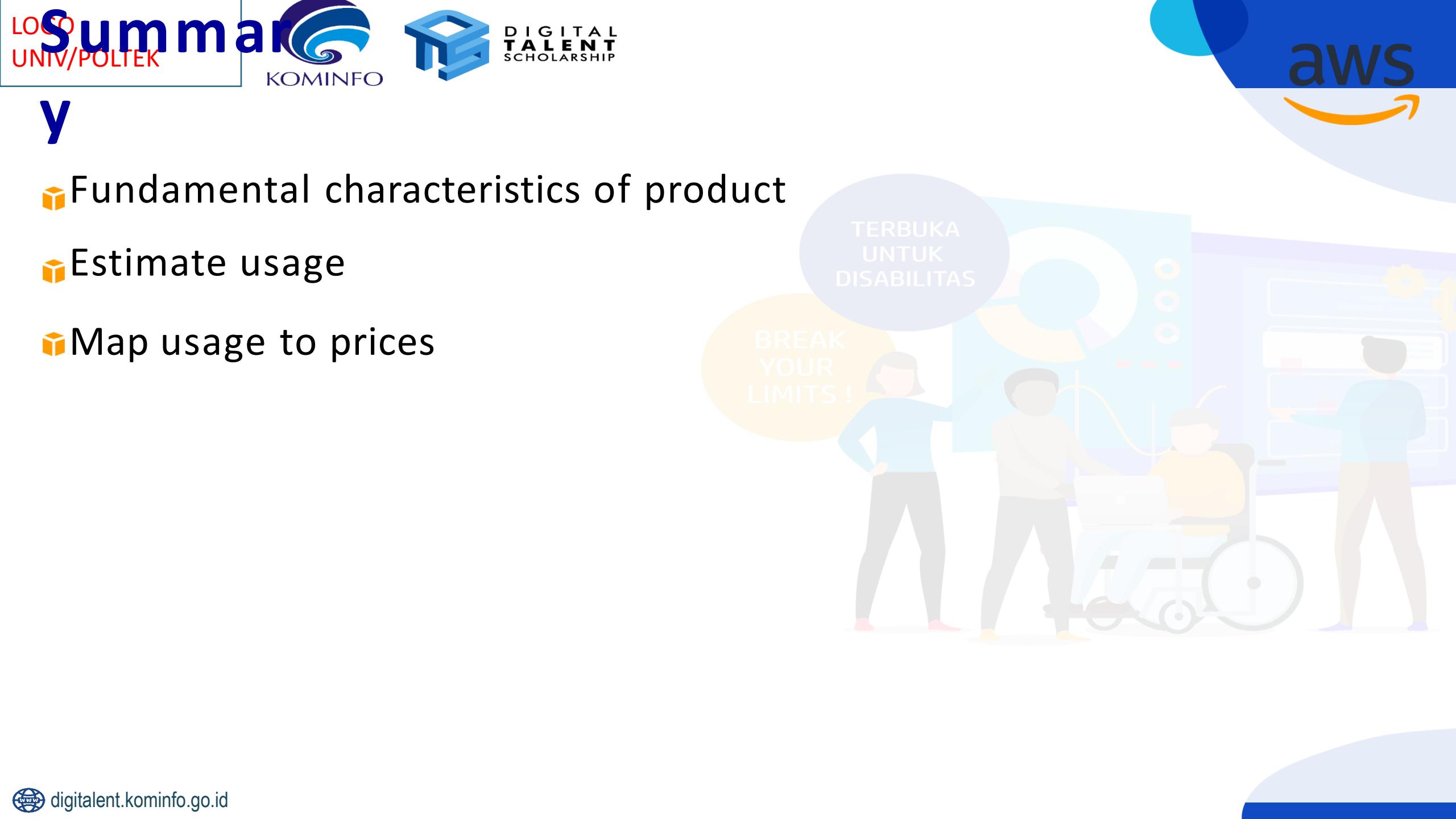
Pricing based on

- Number/type of requests
- Geographic region

Data Transfer Out

- Pricing is based on the amount of data transferred out of Amazon CloudFront edge locations





Overview of the Total Cost of Ownership Calculator

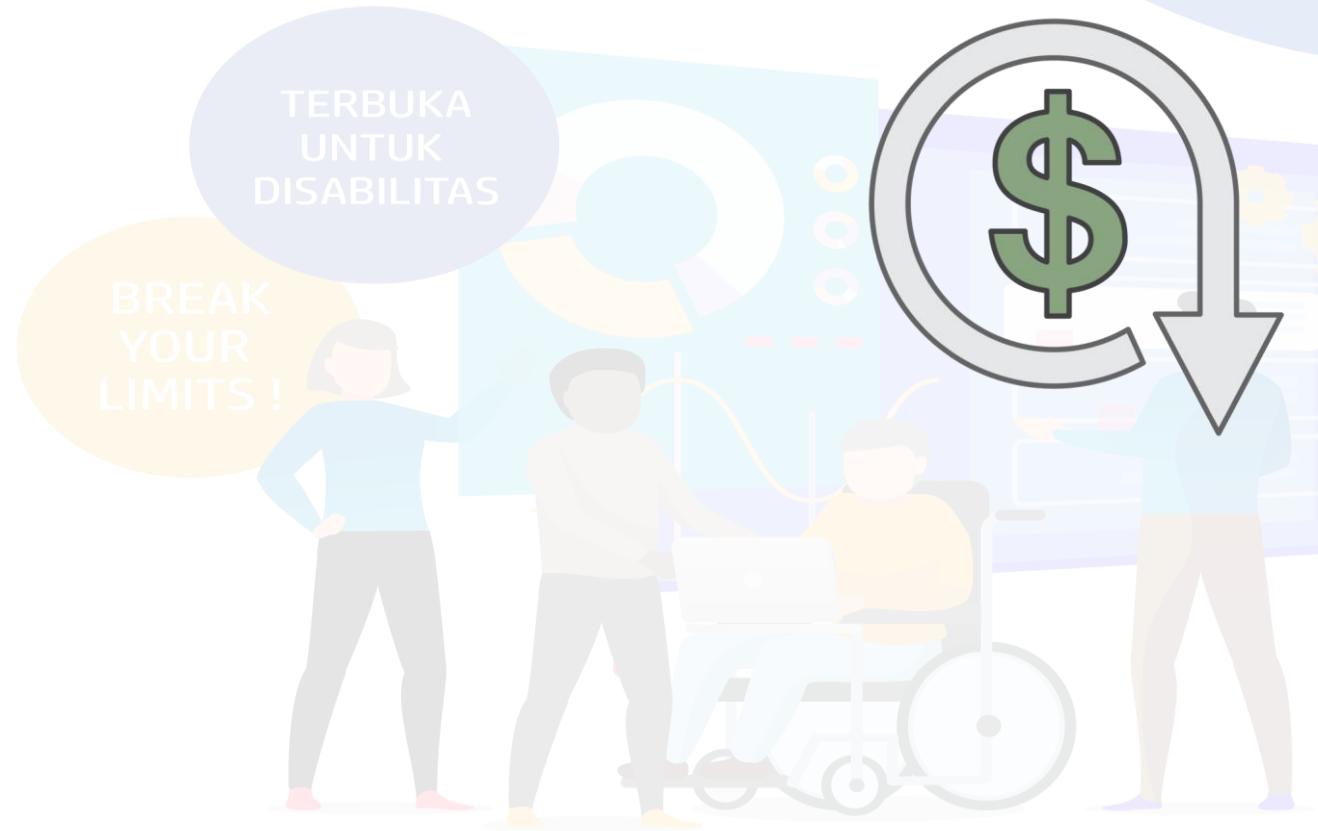


Use the TCO calculator to

- ▣ Estimate cost savings
- ▣ Use detailed reports
- ▣ Modify assumptions

Accessing the TCO Calculator:

- ▣ <https://awstcoccalculator.com>





y

- Estimate cost savings
- Use detailed set of reports
- Modify assumptions for business needs

