AWS Networking, Databases, and Security

By Aditya Putra

me@adityaputra.com
https://github.com/adityaputra/praktisimengajar-cloudcomputing

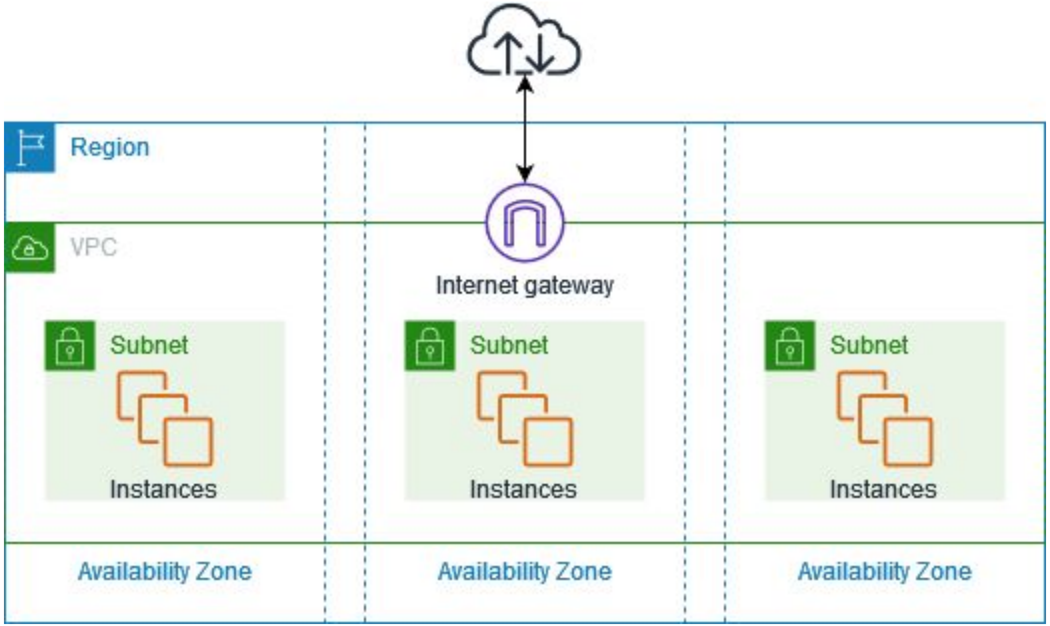
What we're learning today

- AWS Virtual Private Cloud (VPC) and subnets
- AWS Elastic Load Balancer (ELB) and Auto Scaling
- AWS Relational Database Service (RDS) and DynamoDB
- AWS CloudWatch monitoring, alarms, and logging
- AWS Identity and Access Management (IAM) and Security groups
- AWS Web Application Firewall (WAF) and Shield for security

AWS VPC (Virtual Private Cloud) and Subnets

AWS Virtual Private Cloud (VPC) is a service that allows you to create a virtual network within the AWS cloud.

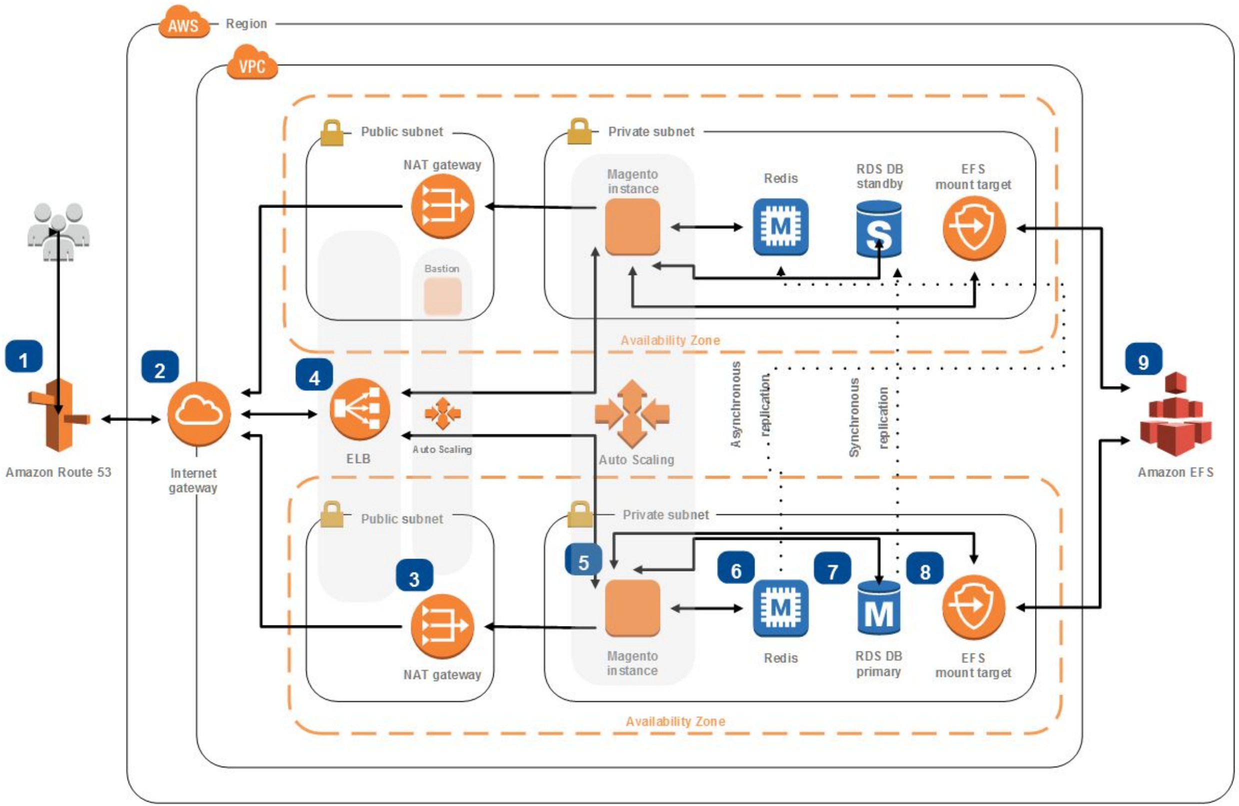
A subnet, is a subdivision of an IP address range within a VPC. -> same as traditional subnets.


Region
VPC
Internet gateway
Subnet
Instances
Subnet
Instances
Subnet
Instances
Availability Zone
Availability Zone
Availability Zone

Magento CE Hosting

Running Magento Community Edition (CE) on AWS

Magento Community Edition (CE) is a flexible, open-source commerce platform for developers and small businesses. This reference architecture simplifies the complexity of deploying a scalable and highly available Magento CE commerce platform on AWS.



1. **Amazon Route 53** provides DNS configuration and routes traffic to Elastic Load Balancing (ELB) endpoints.

2. An **internet gateway** allows communication between instances in your VPC and the internet.

3. **NAT gateways** in each public subnet enable Amazon EC2 instances in private subnets to access the internet.

4. Use an **ELB Load Balancer** to distribute web traffic across an Auto Scaling group of Amazon EC2 instances in multiple Availability Zones.

5. Run your Magento commerce site using an **Auto Scaling group** of **Amazon EC2 instances**. Install the latest versions of Magento CE, Nginx web server, and PHP 7. Then, build an Amazon Machine Image (AMI) that the Auto Scaling group launch configuration can use to launch new instances in the group.

6. If database access patterns are read-heavy, consider using a caching layer like **Amazon ElastiCache for Redis** in front of the database layer to cache frequently accessed data.

7. Simplify your database administration by running your database layer in **Amazon RDS** using either Aurora or MySQL.

8. Amazon EC2 instances access the shared Magento data in an Amazon EFS file system using **mount targets** in each Availability Zone in your VPC.

9. Use an **Amazon EFS** network file system so that Magento instances can access your shared, unstructured Magento data such as images, media files etc.

AWS Reference Architectures

Why using VPC and Subnets?

- Security and Isolation
- Network Architecture and Segmentation
- Connectivity and Internet Access
- Scalability and Availability
- Customization and Flexibility

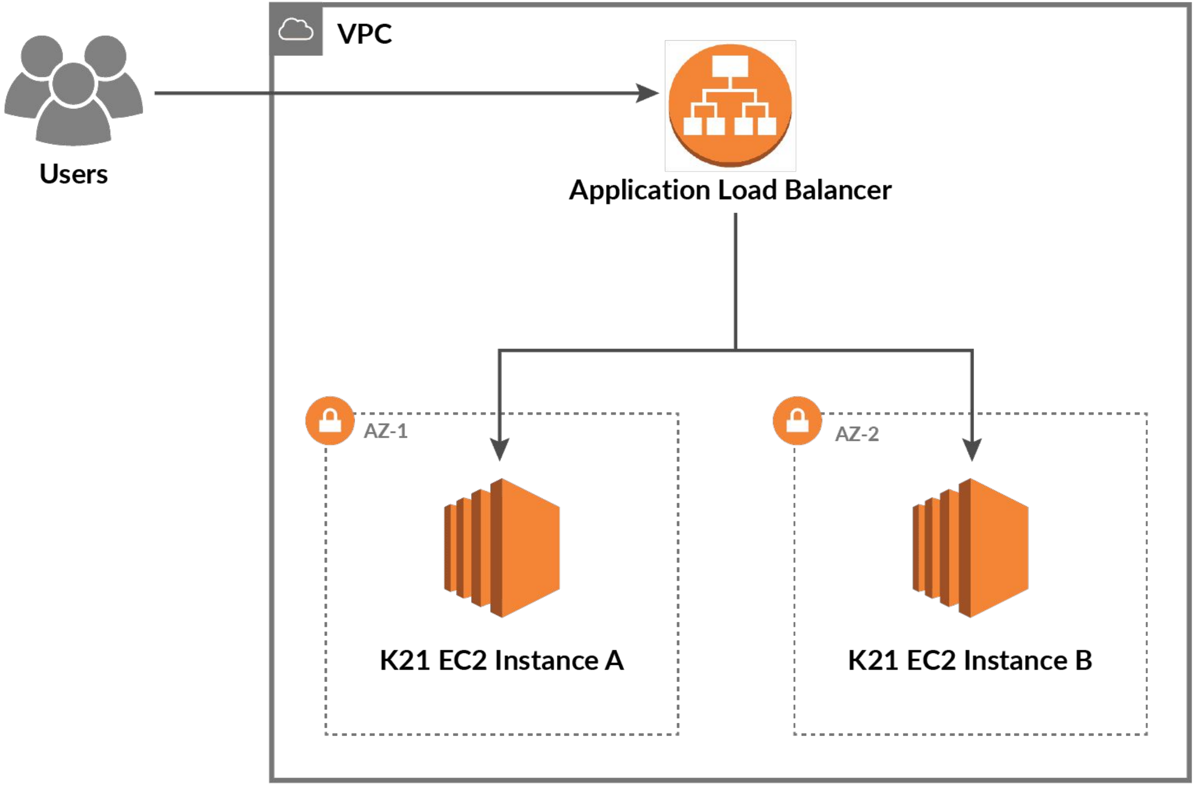
Public vs Private subnets

- Accessibility: Public subnets are accessible from the internet. They have a route to the internet through an Internet Gateway (IGW) or a NAT Gateway.
- Public IP Addresses: Instances in public subnets can be assigned public IP addresses, allowing them to communicate directly with the internet.
- Inbound Traffic: Public subnets can receive incoming traffic from the internet, making them suitable for hosting resources that need to be publicly accessible, such as web servers or APIs.
- Outbound Traffic: Instances in public subnets can initiate outbound connections to the internet.
- Network Address Translation (NAT): Public subnets do not require Network Address Translation for outbound internet connectivity.

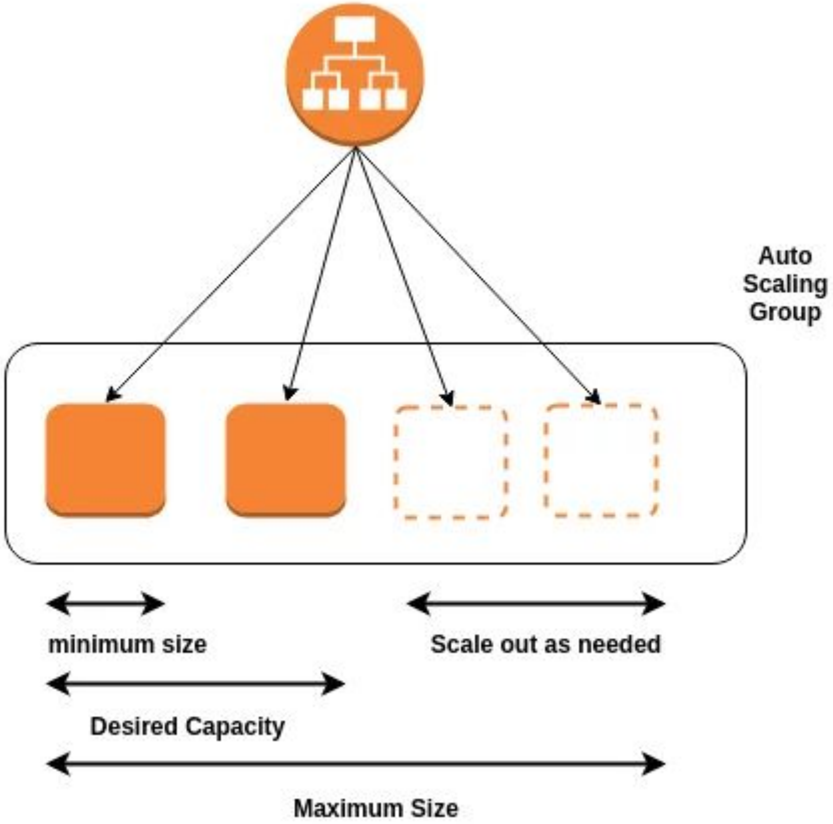
- Accessibility: Private subnets are not accessible from the internet by default. They do not have a route to the internet through an Internet Gateway. Communication with the internet is possible through a NAT Gateway or a proxy server.
- Private IP Addresses: Instances in private subnets are assigned private IP addresses only and cannot be directly reached from the internet.
- Inbound Traffic: Private subnets can receive inbound traffic only from within the VPC or from other resources within the same security group.
- Outbound Traffic: Instances in private subnets can initiate outbound connections to the internet through a NAT Gateway or a proxy server.
- Network Address Translation (NAT): Private subnets require Network Address Translation for outbound internet connectivity.
- Enhanced Security: Private subnets provide an additional layer of security as they are not directly accessible from the internet. This makes them suitable for hosting sensitive resources like databases or backend servers.

Demo and examples

Load balancing with EC2

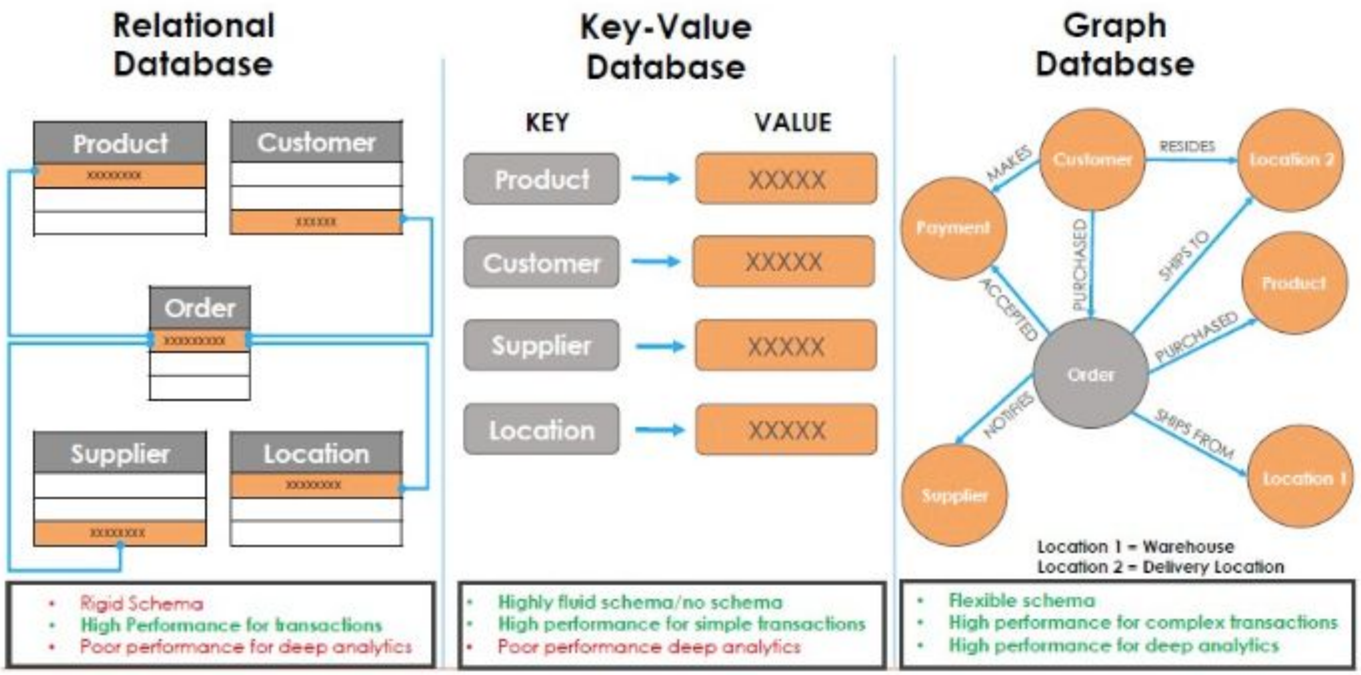


Auto-scaling with EC2



AWS database services

- Amazon RDS (Relational Database Service): MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB
- Amazon DynamoDB: NoSQL database, suitable for use cases that require fast and predictable performance for applications with large amounts of data.
- Amazon Aurora: Aurora is a MySQL and PostgreSQL-compatible relational database engine, cost efficient
- Amazon Redshift: data warehousing
- Amazon Neptune: graph database
- Amazon DocumentDB: MongoDB-compatible
- Amazon ElastiCache: caching service such as Redis and Memcached



Relational Database

- Rigid Schema
- High Performance for transactions
- Poor performance for deep analytics

Key-Value Database

- Highly fluid schema/no schema
- High performance for simple transactions
- Poor performance deep analytics

Graph Database

Location 1 = Warehouse
Location 2 = Delivery Location

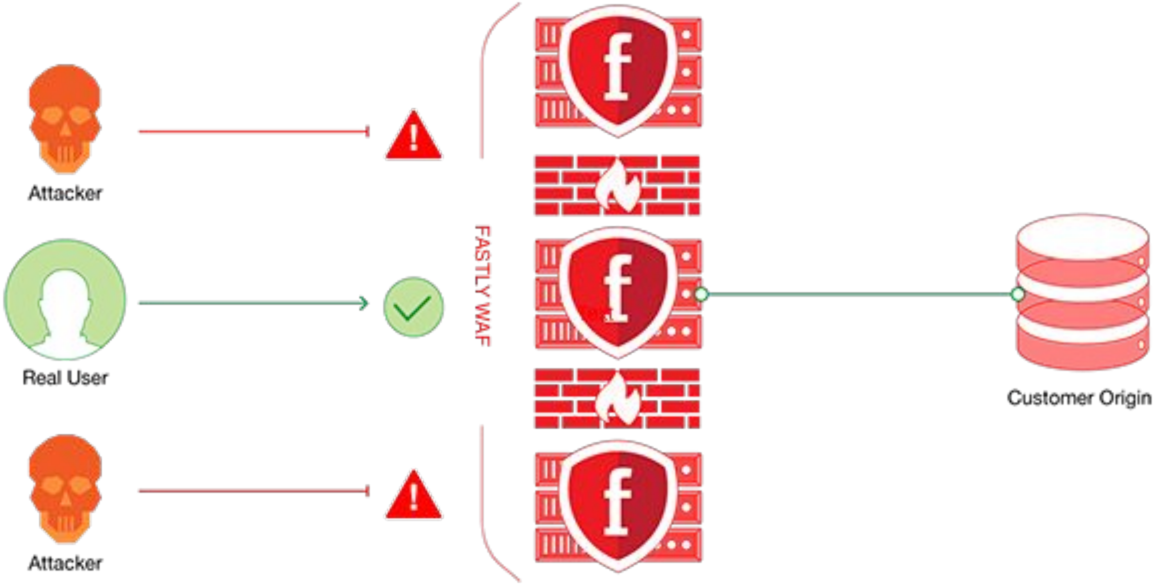
- Flexible schema
- High performance for complex transactions
- High performance for deep analytics

AWS Database demo

AWS security services

- AWS Identity and Access Management (IAM): user access and permissions
- AWS Key Management Service (KMS): manage encryption keys
- AWS Web Application Firewall (WAF): WAF protects your web applications
- AWS Firewall Manager: central management of AWS WAF rules
- Amazon GuardDuty: threat detection service with machine learning
- AWS Secrets Manager: manage sensitive information
- AWS Shield: Distributed Denial of Service (DDoS) protection service
- AWS CloudTrail: track user activity and resource changes in your AWS account
- AWS Security Hub: comprehensive view
- Amazon Macie: data security service

Production deployment



AWS WAF, Fastly, Cloudflare showcase