**Module 7 - Creating a Networking Environment**

Sebuah gambar berisi teks, cuplikan layar, Font, tampilan

Konten yang dihasilkan AI mungkin salah.

When

you design your network on AWS, you need to understand the AWS physical infrastructure components

and hierarchies. The AWS physical infrastructure is made up of multiple AWS Regions. Each

AWS Region

is a

separate geographic area located in a country.

An AWS Region is made up of at least three isolated and physically separate locations called Availability Zones

(AZs). The code for an AZ is its Region code followed by a letter identifier. For example, one of the AZs in the

Northern Virginia Region

us

-

east

-

1

in the US is called

us

-

east

-

1a

.

An AZ is made up of one or more data centers with redundant power, networking, and connectivity in an AWS

Region. AZs are connected with a wired, physical low latency network that allows synchronous data replication

between AZs. Inside a data center, there are thousands of servers and hosts built into racks. Physical network

devices, such as hardware routers, switches, firewalls, and load balancers, are connected to each rack.

Each

device in the network has an IP address that routers and switches can use to reach the device.

**A virtual network (sometimes called an overlay network) is created on top of a physical network.** To deploy a

resource in AWS, you select either a Region or an AZ depending on the service that you use. Data centers are

not logically identifiable.

**A virtual network emulates a physical network with software defined network components such as switches, routers, firewalls, and load balancers.** These components are created and managed programmatically. This

means that all devices on the virtual network are logically isolated through software definitions.

See course source reference list for more information about AWS global infrastructure.

Sebuah gambar berisi teks, cuplikan layar, Font, nomor

Konten yang dihasilkan AI mungkin salah.

AWS reserves the first four IP addresses and the last IP address in each subnet CIDR block. For example, in a

subnet with CIDR block 10.0.0.0/20, AWS reserves the following five IP addresses for:

• 10.0.0.0: Network address

• 10.0.0.1: VPC local router

• 10.0.0.2: DNS resolution

• 10.0.0.3: Future use

• 10.0.15.254: Network broadcast address

Sebuah gambar berisi teks, cuplikan layar, Font, nomor

Konten yang dihasilkan AI mungkin salah.

Data store instances and batch-processing instances should be placed into private subnets. You can put web-tier instances into a public subnet. However, AWS recommends that you place web-tier instances inside private subnets behind a load balancer. In some environments, you must attach web application instances to Elastic IP addresses directly (although you can also attach an Elastic IP address to a load balancer). In those cases, web application instances must be in a public subnet. A NAT gateway or instance must be placed in a public subnet to have access to an internet gateway.

Sebuah gambar berisi teks, cuplikan layar, nomor, tampilan

Konten yang dihasilkan AI mungkin salah.

Sebuah gambar berisi teks, cuplikan layar, Font, nomor

Konten yang dihasilkan AI mungkin salah.

Sebuah gambar berisi teks, cuplikan layar, Font

Konten yang dihasilkan AI mungkin salah.

**Ensure IP subnet allocation accounts for expansion and availability.** When allocating a VPC address CIDR block, AWS recommends to follow the following best practices:

•Within a VPC, allow CIDR block space for multiple subnets that span multiple Availability Zones (AZs).

•Always allocate unused CIDR block space within a VPC for future expansion.

•Take into account that each subnet CIDR block has five reserved IP addresses for AWS use.

•Be aware of services that allocate additional IP addresses, such as container services.

•Deploy large VPC CIDR blocks because a CIDR block can’t be changed or deleted after creation. You can add additional non-overlapping CIDR blocks to the VPC.

•Plan your subnet CIDR block ranges carefully as subnet IPv4 CIDRs can not be changed.

Sebuah gambar berisi teks, cuplikan layar, Font, nomor

Konten yang dihasilkan AI mungkin salah.

The users that use the workloads in your network can be located anywhere. In traditional security models, there tend to be too many access permissions to a network. AWS recommends to apply a Zero Trust approach to apply the principle of security at all layers. Zero Trust security is a model where application components are considered separate from each other and no component trusts any other component. The careful planning and management of your network design forms the foundation of how you provide isolation and boundaries for resources within your workload. Because many resources in your workload operate in a VPC and inherit the security properties, it’s critical that the design is supported with inspection and protection mechanisms.

**Create network layers**: AWS recommends to logically group workload components that share the same sensitivity requirement together in a layer. For example, a database in a VPC with no need for internet access should be placed in subnets with no route to or from the internet. Traffic should only flow from the adjacent next least sensitive resource.

**Control traffic at all layers**: AWSrecommends to apply multiple security controls with a defense in depth approach for inbound and outbound traffic. Define allowed traffic paths in the VPC with security groups, network ACLs, subnets, route tables, internet gateways, and NAT gateways.

**Implement inspection and protection:** AWSrecommends to inspect and filter your traffic at each layer. For example, you can inspect your VPC configurations for potential unintended access using the VPC Network Access Analyzer.

Sebuah gambar berisi teks, cuplikan layar, Font

Konten yang dihasilkan AI mungkin salah.

The performance efficiency pillar addresses best practices for managing production environments. You want to avoid scenarios where a workload on a network uses too much network bandwidth. Each workload that you deploy in a VPC has different requirements for latency, throughput, amount of jitter allowed, and bandwidth. Jitter occurs when there is a time delay caused by network congestion or route changes.

The following performance efficiency pillar best practices can help you to optimize your network design:

Understand how networking impacts performance: Analyze and understand how network-related decisions impact workload performance. For example, implementing database synchronous replication between AWS Regions is not possible due to double digit or more millisecond latency between Regions. Because latency between AZs are measured in single digit milliseconds, you can implement database synchronous replication between AZs.

Evaluate available networking features: Benchmark your workload performance metrics, including network metrics. You should continually evaluate the workload for areas to improve, such as removing performance bottlenecks. You can use Network Access Analyzer to help identify network paths and routes.

Choose network protocols to improve performance: Choose network protocols that will optimize your workload’s performance. For example, do not use TCP for all workloads regardless of performance requirements. As an alternative, use both TCP and UDP together for Virtual Desktop Infrastructure workloads. This can take advantage of the reliability of TCP for critical data and the speed of UDP for real-time data.

Sebuah gambar berisi teks, cuplikan layar, jam, Font

Konten yang dihasilkan AI mungkin salah.

A workload on a network should fully utilize all resources, achieve outcomes at the lowest possible price point, and meet functional requirements. Network costs should be included in the workload cost benchmark. The key to save costs is to select the best pricing model with appropriate network configurations for your workloads.

**Implement Regions based on cost:** AWSrecommends using the AWS Region that delivers the best overall global cost solution. Each AWS Region operates within local market conditions. Resource pricing is different in each Region due to differences such as the cost of land, fiber, electricity, and taxes. Choose a specific Region to operate a component of your entire solution so that you can run at the lowest possible price globally. When you architect your solutions, a best practice is to seek to place computing resources closer to users to provide lower latency and strong data sovereignty. Select the geographic location based on your business, data privacy, performance, and security requirements. For applications with global end users, use multiple locations.

There are four major network issues identified in the scenario. They align to the anti-patterns that are shown on this slide.

• Company A should not be using a single small VPC with limited IP addresses, but rather large VPCs with enough IP addresses for future growth.

• The website servers should have their own security group with internet access allowed in a public subnet. The database servers should have their own security group allowing access from the website server security group and database support.

• Database servers should be placed in a private subnet. No internet direct access to the database servers should be allowed. Maintenance access can be configured in the database security group and allow server patching with access to a NAT gateway.

• Instead of using an AWS Region in Europe, an AWS Region in the US closer to the customer base should be used for lower latency and strong data sovereignty.