AWS Aufgabe 03.04.2024

Beantworte mir die folgenden Fragen zu den Services/Bestandteilen:

- Erkläre mir, was der Service macht / Wie er funktioniert?
- Welches Problem löst der Service/Bestandteil?
- Vergleiche die farbigen Service/Bestandteil miteinander (was macht ROT, was macht BLAU, was macht GELB, was macht GRÜN)

Antworten in eigenen Worten und 3 - 5 Sätzen oder Stichpunkte

Services Begriffe:

- ENI
- AWS Cloud
- AWS Region
- AWS AZ
- VPC
- Subnet
- privates Subnet (blau)
- öffentliches Subnet (blau)
- Switch (grün)
- Router (grün)
- Netzwerkinterface
- CIDR Notation
- ACL (rot)
- NACL (rot)
- Logging
- Security Groups
- statefull rules (gelb)
- stateless rules (gelb)

Optionale Bonusaufgabe:

- Was ist dhcp? 😀

Service/Bestandteil	Erklärung	Problem, das gelöst wird

ENI **Elastic Network Interface**	eine virtuelle Netzwerkschnittstelle (auch Netzwerkkarte genannt),die einer EC2-Instanz in der AWS Cloud zugeordnet ist. Unterstützt Flexible Netzwerkkonfiguration	Ermöglicht einer EC2-Instanz die Kommunikation mit anderen Ressourcen im Netzwerk und den Zugang zum Internet. Schneller einsetzbar als physische Netzwerkkarten. Nur in der gleichen AZ
AWS Cloud	Die AWS Cloud ist eine Plattform von Amazon Web Services (AWS), die eine breite Palette von Cloud-basierten Diensten und Ressourcen bietet.	Bietet skalierbare, flexible und kostengünstige Infrastruktur- und IT-Services, ohne dass physische Hardware vor Ort verwaltet werden muss. Bereitstellung in Sekunden statt Wochen.
AWS Region	Eine geografische Region, in der AWS-Rechenzentren angesiedelt sind und Ressourcen bereitgestellt werden können. Besteht aus mehreren AZs.	Ermöglicht die Lokalisierung von Ressourcen in geografischen Gebieten, um Latenzzeiten zu minimieren und regulatorische Anforderungen(Compliance) zu erfüllen.
AWS AZ **Availability Zone**	Eine Availability Zone (AZ) ist ein isolierter Bereich innerhalb einer AWS-Region, der über unabhängige Stromversorgung, Kühlung und Netzwerkanbindung verfügt. Sind mit high-speed Verbindung mit den anderen AZs in der gleichen Region verbunden.	Verbessert die Verfügbarkeit und Ausfallsicherheit von Anwendungen, indem sie Redundanz und Failover-Möglichkeiten innerhalb einer Region bietet.
VPC **Virtual Private Cloud**	Eine Virtual Private Cloud (VPC) ist ein logisch isoliertes Netzwerk in der AWS Cloud, das Ihnen ermöglicht, Ressourcen (S3, EC2, etc.) in einem von Ihnen definierten virtuellen Netzwerk zu betreiben.	Ermöglicht die Einrichtung und Verwaltung einer eigenen Netzwerkinfrastruktur in der AWS Cloud, um Ressourcen sicher und isoliert zu betreiben. Ohne Cloud müssten wir ein Firmennetzwerk vor Ort verwenden.
Subnet	Ein Subnetz ist eine Unterteilung eines VPCs, das es ermöglicht, Ressourcen in logisch isolierten Netzwerksegmenten zu organisieren und zu verwalten und technisch betrachtet ein IP-Adressenbereich. https://cidr.xyz/	Ermöglicht die Organisation von Ressourcen innerhalb eines VPCs in logisch getrennten Bereichen, um Sicherheit zu gewährleisten und den Datenverkehr zu steuern

Privates Subnetz	• Ein privates Subnetz in einem VPC hat keine direkte Verbindung zum Internet. • kann nur interne Ressourcen innerhalb des VPCs kommunizieren. - über NAT-Gateway ans internet anbindbar (z.b. für Update) - anders als öffentliches Subnetz	• Schutz sensibler Daten vor unbefugtem Zugriff, • Sicherstellung der internen Kommunikation innerhalb des VPCs.
Öffentliches Subnetz	• Ein öffentliches Subnetz in einem VPC hat eine direkte Verbindung zum Internet. • macht Ressourcen innerhalb des Subnetzes über eine öffentliche IP-Adresse erreichbar. - anders als privates Subnetz	• Externe Zugriff auf Ressourcen im VPC. • erleichtert die Kommunikation mit dem Internet.
Switch	Ein Switch leitet den Datenverkehr innerhalb eines lokalen Netzwerks weiter, indem er die MAC-Adressen der angeschlossenen Geräte verwendet. Es gibt virtuelle und physische Switches. (Bsp. MAC-adresse: 00-B0-D0-63-C2-26)	Effiziente und schnelle Datenübertragung zwischen den Geräten im Netzwerk.
Router	Ein Router verbindet verschiedene Netzwerke (auch Subnetze) miteinander und leitet den Datenverkehr zwischen ihnen weiter. (Hat eine Routing Tabelle)	Ermöglicht die Kommunikation zwischen verschiedenen Netzwerken, einschließlich des *Zugangs zum Internet → Internet Gateway.*
Netzwerkinterface	Ein Netzwerkinterface ist eine Verbindungspunkt zwischen einem Gerät (z.B. einer EC2-Instanz) und einem Netzwerk, das Informationen senden und empfangen kann. Kann virtuell und physisch sein.	Ermöglicht die Kommunikation zwischen virtuellen Maschinen (z.B. EC2-Instanzen) und anderen Netzwerkressourcen innerhalb eines VPCs oder mit dem Internet.
CIDR Notation	Eine Darstellungsmethode für IP-Adressbereiche, die die Anzahl der Netzwerkbits in einer IP-Adresse angibt, gefolgt von einem	Ermöglicht die Definition von IP-Adressbereichen von VPCs und Subnetzen auf effiziente Weise, um Netzwerke in der AWS Cloud zu planen und zu konfigurieren.

	Schrägstrich (/) und der Anzahl der Bits, die das Netzwerk identifizieren. z.B. 10.88.135.144/28 https://cidr.xyz/	
ACL **Access Control Lists**	Access Control Lists sind Sicherheitsregeln auf Netzwerkebene (auch Subnetze), die den ein- und ausgehenden Datenverkehr anhand von IP-Adressen, Ports und Protokollen steuern. - in der Regel Stateless	● Granulare Kontrolle über den Datenverkehr. ● Schutz vor unerwünschtem Zugriff oder böswilligen Angriffen.
NACL **Network Access Control List**	Network Access Control Lists sind ähnlich wie ACLs, *aber auf Subnetzebene*. - in der Regel Stateless	● Zusätzliche Sicherheitsebene durch Kontrolle des Datenverkehrs zwischen verschiedenen Teilen eines VPCs. ● Segmentierung des Netzwerks.
Logging	Protokolliert Ereignisse und Aktivitäten in einem System oder einer Anwendung für Überwachung, Analyse und Sicherheitszwecke.	Unterstützt die Fehlerbehebung, Überwachung und Einhaltung von Sicherheitsrichtlinien, indem es eine Aufzeichnung von Aktivitäten und Ereignissen ermöglicht. Unterstützt Einhaltung von Compliance-Anforderungen. (z.B. DSGVO-Anfoderungen)
Security Groups	Eine Firewall für Ihre EC2-Instanzen, die den ein- und ausgehenden Datenverkehr steuert. - **Stateful** - Firewall für schützen einer Ressource - granularer Schutz	Bietet eine zusätzliche Sicherheitsebene, indem es den Datenverkehr auf Basis von Regeln zulässt oder blockiert, um unautorisierten Zugriff zu verhindern und die Einhaltung von Sicherheitsrichtlinien zu gewährleisten.
Stateful Rules	Sicherheitsregeln, die den Datenverkehr *aufgrund des Zustands der Verbindung* zulassen oder blockieren.	● Automatisierte Zulassung eingehender Antworten auf ausgehende Anfragen. ● einfache Implementierung von Sicherheitsrichtlinien.

Stateless Rules	Sicherheitsregeln, die den Datenverkehr *unabhängig von seinem Zustand* zulassen oder blockieren.	• Granulare Kontrolle über den Datenverkehr, basierend ausschließlich auf den Merkmalen einzelner Pakete. • Eventuell komplexere Konfiguration im Vergleich zu stateful rules.

Hier ist eine Tabelle, die den Vergleich der farbigen Service/Bestandteile darstellt:

Service/Bestandteil	Funktion
ACL (Access Control Lists)/NACL	Steuert den ein- und ausgehenden Datenverkehr auf Netzwerkebene(oder Subnetz Ebene) , basierend auf IP-Adressen, Ports und Protokollen.
privates Subnet / öffentliches Subnet	Organisiert Ressourcen innerhalb eines VPCs in abgeschirmten Bereichen. Private Subnetze bieten eine sicherere Umgebung ohne direkten Internetzugang, während öffentliche Subnetze direkten Internetzugang ermöglichen.
Stateful Rules / Stateless Rules (Sicherheitsregeln)	Sicherheitsregeln, die den Datenverkehr entweder basierend auf dem Verbindungszustand (stateful) oder unabhängig davon (stateless) zulassen oder blockieren.
Switch / Router (Netzwerkgeräte)	Switches leiten den Datenverkehr innerhalb eines Netzwerks weiter, während Router den Datenverkehr zwischen verschiedenen Netzwerken weiterleiten.

Optionale Bonusaufgabe:

- **Was ist dhcp?** 😀

- DHCP (Dynamic Host Configuration Protocol) ist ein Netzwerkprotokoll, das automatisch IP-Adressen und andere Netzwerkkonfigurationen an Geräte in einem Netzwerk verteilt.
- Es ermöglicht eine effiziente und automatisierte Zuweisung von Netzwerkkonfigurationen, was die Verwaltung und Skalierung von Netzwerken erleichtert und menschliche Fehler minimiert.