



KN05: Netzwerk / Sicherheit

- A) Diagramm erstellen
- B) Subnetz und private IP wählen
- C) Objekte und Instanzen erstellen

KN05: Netzwerk / Sicherheit

Beachten Sie die [allgemeinen Informationen zu den Abgaben](#).

In dieser Kompetenz werden wir das Netzwerk bei AWS ein wenig genauer anschauen. [Lesen Sie zuerst die Theorie durch](#). Bisher wurden die Netzwerk-Eigenschaften weitgehend automatisch erstellt. Wir wollen nun die Kontrolle ausüben.

A) Diagramm erstellen

Im Modul 117 hatten Sie Diagramm über Netzwerke gezeichnet. Dies werden wir nun für Ihre AWS Umgebung wiederholen. Folgende Inhalte muss Ihr Diagramm zeigen

- Ihr VPC (Virtual Private Cloud) mit dem IP Range / CIDR Block
- Alle bestehende Subnetze mit dem IP Range / CIDR Block.
- Wissen Sie in welchem Subnetz Ihre Instanzen aus den vorherigen KNs lagen? Falls Sie Ihre Objekte schon gelöscht haben, können Sie einfach das Formular für eine neue Instanz aufrufen und nachschauen was per Default ausgewählt war. Zeichnen Sie die VMs, die Sie in KN03 benötigten im entsprechenden Subnetz ein. Die VMs müssen dazu nicht mehr existieren, sei können ja einfach die Namen "KN03-DB" und "KN03-Web" verwenden.

Das Ziel ist, dass Sie ihre Umgebung verstehen. Sie können sich an dem Diagramm orientieren aus der Theorie, Teil *Netzwerk*

Abgaben:

- Diagramm als Bild

B) Subnetz und private IP wählen

Sie haben nun herausgefunden in welchem Subnetz sich Ihre Server aus KN03 befanden. Geben Sie dem Subnetz einen Namen (z.B. Subnet-KN03).

Wählen Sie ein beliebiges anderes Subnetz und geben ihm ebenfalls einen Namen für diese aktuelle KN (z.B. Subnet-KN05).

In den folgenden Teilaufgaben werden Sie die Schritte für KN03 wiederholen mit ein paar Zusätzen. Dazu wählen Sie nun zwei IPs aus dem Subnetz, die Sie dann später Ihren Instanzen zuweisen werden (private IPs). Die IPs müssen durch 10 teilbar sein (z.B. xxx.xxx.xxx.10, xxx.xxx.xxx.150, etc).

Abgaben:

- Screenshot der Subnetzen, die die Namen zeigen
- Zwei definierte IPs für Web- und DB-Server/Instanz. Dazu braucht es keinen Screenshot, einfach nur die beiden IPs als Text.

C) Objekte und Instanzen erstellen

Nachdem Sie sich nun auf das Subnetz und IPs festgelegt haben, können Sie die restlichen Objekte anlegen.

- **Achtung:** Stellen sie sicher, dass Ihre Instanzen die beiden IPs aus B) verwendet werden.
- In KN03 wurden automatisch Security Groups erstellt. Das Problem dabei ist, dass diese keine sinnvollen Namen besitzen und so kaum wiedererkannt werden. Erstellen sie nun also zwei Security Groups (für Web und DB). Die Ports sind die gleichen wie bei KN03. Geben Sie sinnvolle Werte für die Felder *Name* und *Security group name*.
- Ändern Sie die Security Group für die DB und lassen Sie für den Port 3306 nur Zugriff innerhalb des **eigenen Subnetzes** zu.
- Erstellen Sie nun die beiden Instanzen für den Web- und DB-Server. Sie können die gleichen Cloud-Init-Dateien verwenden, aber müssen nun die IP anpassen für den Datenbankzugriff. Diese IP wird sich aber - im Gegensatz zu KN03 - nicht mehr ändern. Wenn Sie die Instanzen erstellen, müssen Sie die Netzwerk-Einstellungen genauer betrachten und wählen Sie die korrekten Objekte aus (Subnetz, IP, SG). **Achtung:** Zu diesem Zeitpunkt definieren Sie nur die private Adresse.
- Erstellen Sie zwei öffentliche IP Adressen (Elastic IPs). Geben Sie wieder sinnvolle Werte für das Feld *Name*. Weisen Sie die IP Adressen den beiden erstellten Instanzen zu (über das Aktionen-menu).
- Stoppen Sie die beiden Instanzen. Zeigen Sie, dass die IPs nicht verloren gehen, wenn die Instanz gestoppt ist.

Abgaben

- Screenshot der Liste der Sicherheitsgruppe mit sprechenden Namen/Feldern
- Screenshot der Inbound-Regel für die DB-Sicherheitsgruppe.
- Screenshot der Liste der Elastic IPs mit sprechenden Namen.
- Zeigen Sie, dass Sie nun **alle drei** Seiten aufrufen können (index.html, info.php und db.php).
- Screenshot der Liste der Instanzen, wenn beide Instanzen gestoppt sind. Das Feld der öffentlichen IP und der Status (gestoppt) müssen sichtbar sein.
- Screenshot der Details beider Instanzen, so dass die **Subnet ID** sichtbar ist.
- Laden Sie die aktualisierten Cloud-init Konfigurationen hoch in Git. Im Web-Konfig, sollte die IP angepasst sein.