



KN05: Netzwerk / Sicherheit

A) Vorbereitung

B) Netzwerk und Sicherheit Einrichten

KN05: Netzwerk / Sicherheit

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

In dieser Kompetenz werden wir das Netzwerk, Firewall und Applikationseinstellungen anschauen.
[Lesen Sie zuerst die Theorie durch](#).

A) Vorbereitung

Führen Sie folgende Aufgaben durch zur Vorbereitung:

- Terminieren Sie alle Instanzen, die Sie noch haben. Stellen Sie sicher, dass Sie die vorherige Aufgabe korrekt dokumentiert haben, so dass die Abnahme trotzdem klappt!
- Gehen Sie zu den *Network Interfaces* und löschen Sie alle. Sie finden diese im Bereich EC2, aber weiter unten in der Navigation
- Gehen Sie zu den *Security Groups* und löschen Sie all (ausser die mit dem Name *default*)
- Gehen zu den **Subnetzen** und löschen Sie alle. Sie finden diese unter *Services -> Networking & Content Delivery -> VPC*. Behalten Sie aber ihr VPC!

Abgabe: Erstellen Sie Screenshots der leeren Bereiche bevor Sie weiterfahren.

B) Netzwerk und Sicherheit Einrichten

Sie werden wieder Web- und Datenbankserver installieren und können die Cloud-init Konfigurationen aus KN04 verwenden.

Anstatt, dass Sie eine Instanz erstellen und die Standard-Eigenschaften verwenden, erstellen Sie die virtuellen Objekte zuerst und wählen diese dann während der Instanz-Erstellung aus. Gehen Sie wie folgt vor:

1. Erstellen Sie ein Subnetz welches von x.x.10.0 - x.x.10.255 reicht. Die x sind definiert in ihrer VPC-Einstellung. Verwenden Sie einen Subnetz-Generator, wenn Sie sich unsicher sind. **Verwenden Sie sprechende Namen.**

Wichtig: Sie müssen die Option "*Enable auto-assign public IPv4 address*" aktivieren, sonst kriegen Sie keine öffentliche IP

2. Erstellen Sie die *Security Groups*. Diese müssen bereit stehen, wenn Sie die privaten IPs erstellen. Stellen Sie sicher, dass Sie für den Datenbank-Port nur das Subnetz zulassen. **Verwenden Sie sprechende Namen.**
3. Erstellen Sie **eine** *Elastic IPs*. Diese finden Sie in der Navigation im Bereich EC2. Diese stellen die öffentlichen IPs dar, die wir für die beiden Server verwenden werden.
4. Erstellen Sie zwei *Network Interfaces* mit IPs in dem entsprechenden Subnetz. Weisen Sie **spezifische** IPs des Subnetzes zu. Sie werden diese den beiden Servern später zuweisen. Nun können sie endlich auch die IP in die Cloud-init Konfiguration eintragen für die IP des Datenbankservers. Sie werden nun immer die gleiche IP haben! **Verwenden Sie sprechende Namen.**
Wenn Sie die zwei Netzwerk-Interfaces mit private IPs erstellt haben, müssen Sie die öffentliche IP noch assoziieren. Wählen Sie dazu das Netzwerk-Interface für den Web Server aus und assoziieren Sie die eine öffentliche IP über das *Actions*-Menu.
5. Setzen Sie der Cloud-init Konfiguration für den Web Server die korrekte IP für die Datenbankabfrage.
6. Fügen Sie der Cloud-init Konfiguration für den Datenbank Server zwei neue Befehle hinzu. Der erste ersetzt die Limitierung des Pakets auf die lokale IP. Der zweite startet den Service neu.

```
sudo sed -i 's/127.0.0.1/0.0.0.0/g' /etc/mysql/mariadb.conf.d/50-server.cnf
sudo systemctl restart mariadb.service
```

7. Erstellen Sie nun die Instanz. Bei den *Netzwerk settings* müssen Sie nun "Edit" drücken und die korrekten Objekte auswählen. **ACHTUNG:** Bevor Sie die Instanz starten, stellen Sie sicher, dass sie die notwendigen Screenshots gemacht haben.

Abgabe:

- Subnetz: Screenshot und Begleittext. Zeigen Sie, dass Sie das neue Subnetz erstellt haben.
- Elastic IPs: Screenshot der Liste.
- Security Groups. Screenshot und Begleittext. Zeigen Sie die Inbound-Rules und die Namen der Security-Groups.
- Netzwerk-Interfaces: Screenshots und Begleittext. Zeigen Sie die private und öffentliche IP und die zugewiesene Security-Gruppe
- Laden Sie die aktualisierten Cloud-init Konfigurationen hoch. Im Web-Konfig, sollte die IP angepasst sein. Im DB-Konfig sollten die beiden neuen Befehl drin stehen.
- Erstellung der Instanz. Zeigen Sie **alle** Einstellungen des Bereichs "**Network settings**" **bevor** Sie die Instanz starten.
- Zeigen Sie, dass Sie nun **alle drei** Seiten aufrufen können (index.html, info.php und db.php).