15.4 Cloud-Netzwerke, VPC, Subnetze und Security Groups

Cloud-Dienste brauchen genau wie lokale Systeme ein Netzwerk.

In der Cloud werden Netzwerke aber nicht mit physischen Switches und Routern aufgebaut, sondern überwiegend virtuell.

Typische Bestandteile eines Cloud-Netzwerks:

```
- virtuelles Netzwerk
- Subnetze
- Routingtabellen
- Security Groups
- Network Security Groups
- virtuelle Firewalls
- Load Balancer
- öffentliche IP-Adressen
- private IP-Adressen
- NAT-Gateways
- VPN-Gateways
- DNS
- Peering
```

Merksatz:

```
Cloud-Netzwerke sind virtuell,
müssen aber genauso sauber geplant werden wie lokale Netzwerke.
```

Warum Cloud-Netzwerke wichtig sind

Viele Cloud-Fehler entstehen nicht durch die Anwendung, sondern durch Netzwerk- oder Sicherheitskonfiguration.

Beispiele:

```
virtuelle Maschine nicht erreichbar
Datenbank öffentlich erreichbar
```

```
Webserver hat falsche Security Group
Subnetz hat keine passende Route
Cloud-Dienst kann Backend nicht erreichen
VPN zur Cloud funktioniert nicht
DNS zeigt auf falsches Ziel
Load Balancer erreicht keine Instanz
```

Merksatz:

```
Cloud-Probleme sind oft Netzwerk-,
Routing-
oder Firewall-Probleme.
```

Virtuelles Netzwerk

Ein virtuelles Netzwerk ist ein logisch getrenntes Netzwerk in der Cloud.

Je nach Anbieter heißt es zum Beispiel:

```
VPC
VNet
Virtual Network
Virtual Private Cloud
```

Es enthält Cloud-Ressourcen wie:

```
virtuelle Maschinen
Subnetze
Datenbanken
Load Balancer
Container
VPN-Gateways
NAT-Gateways
```

Merksatz:

```
Virtuelles Netzwerk = eigenes logisch getrenntes Cloud-Netz.
```

VPC

VPC steht für:

```
Virtual Private Cloud
```

Eine VPC ist ein virtuelles, logisch isoliertes Netzwerk innerhalb einer Public Cloud.

In einer VPC legt man fest:

```
IP-Adressbereich
Subnetze
Routing
Sicherheitsregeln
Gateways
Verbindungen zu anderen Netzen
```

Merksatz:

```
VPC ist ein privater Netzwerkbereich innerhalb der Cloud.
```

VNet

VNet steht für:

```
Virtual Network
```

Der Begriff wird in manchen Cloud-Plattformen für virtuelle Netzwerke verwendet.

Die Grundidee ist ähnlich wie bei VPC:

```
eigener IP-Bereich
Subnetze
Routing
Sicherheitsregeln
Cloud-Ressourcen
Verbindungen zu anderen Netzen
```

Merksatz:

VNet und VPC beschreiben ähnliche Cloud-Netzwerk-Konzepte.

IP-Adressbereich im Cloud-Netz

Beim Anlegen eines Cloud-Netzes wird ein IP-Adressbereich festgelegt.

Beispiel:

```
10.20.0.0/16
```

Daraus können mehrere Subnetze gebildet werden.

Beispiele:

```
10.20.1.0/24 Web-Subnetz

10.20.2.0/24 App-Subnetz

10.20.3.0/24 Datenbank-Subnetz
```

Wichtig:

Der Adressbereich darf sich nicht ungewollt mit lokalen Netzen überschneiden.

Merksatz:

Cloud-IP-Planung muss zu lokaler Netzplanung passen.

Subnetze in der Cloud

Subnetze teilen ein virtuelles Netzwerk in kleinere Bereiche auf.

Typische Subnetze:

```
Web-Subnetz
App-Subnetz
Datenbank-Subnetz
```

Management-Subnetz
Public Subnet
Private Subnet
Gateway-Subnetz

Vorteile:

bessere Struktur
gezielte Sicherheitsregeln
getrennte Routingtabellen
Trennung von öffentlichen und internen Ressourcen

Merksatz:

Subnetze strukturieren Cloud-Netze.

Public Subnet

Ein Public Subnet ist ein Subnetz, das direkt oder indirekt Zugang zum Internet haben kann.

Typische Ressourcen:

Load Balancer
öffentlich erreichbarer Webserver
Bastion Host
NAT-Gateway
Reverse Proxy

Wichtig:

Nicht jede Ressource in der Cloud gehört in ein Public Subnet.

Merksatz:

Public Subnet nur für Komponenten,
die wirklich öffentlich erreichbar sein müssen.

Private Subnet

Ein Private Subnet enthält interne Ressourcen, die nicht direkt aus dem Internet erreichbar sein sollen.

Typische Ressourcen:

> Datenbanken
> interne Backends
> interne APIs
> Anwendungssysteme
> Verarbeitungssysteme
> Container-Worker
> interne Dienste

Merksatz:

> Private Subnet schützt interne Cloud-Ressourcen vor direktem Internetzugriff.

Public und Private Subnet vergleichen

Merkmal	Public Subnet	Private Subnet
Internetzugriff eingehend	möglich	normalerweise nicht direkt
typische Systeme	Load Balancer, Bastion Host	Datenbank, Backend
Schutzbedarf	hoch	sehr hoch
Routing	oft zum Internet Gateway	oft über NAT oder interne Routen
Ziel	öffentliche Erreichbarkeit	interne Verarbeitung

Merksatz:

> Öffentlich erreichbare Systeme nach außen,
> interne Systeme nach innen trennen.

Internet Gateway

Ein Internet Gateway verbindet ein Cloud-Netz mit dem Internet.

Es ermöglicht:

eingehende Verbindungen aus dem Internet

ausgehende Verbindungen ins Internet

Ob eine Ressource wirklich erreichbar ist, hängt zusätzlich ab von:

öffentlicher IP-Adresse
Routingtabelle
Security Group
Firewall-Regeln
Dienststatus

Merksatz:

Internet Gateway allein macht eine Ressource nicht automatisch erreichbar.

NAT-Gateway

Ein NAT-Gateway erlaubt internen Ressourcen, Verbindungen ins Internet aufzubauen, ohne selbst direkt aus dem Internet erreichbar zu sein.

Beispiel:

Datenbankserver im Private Subnet
lädt Updates herunter

aber:
Internet kann nicht direkt zur Datenbank verbinden

Merksatz:

NAT-Gateway erlaubt ausgehenden Internetzugriff für private Ressourcen.

Internet Gateway und NAT-Gateway vergleichen

Merkmal	Internet Gateway	NAT-Gateway

Zweck	Verbindung Cloud-Netz ↔ Internet	ausgehender Zugriff aus privaten Netzen
eingehend aus Internet	möglich, wenn erlaubt	normalerweise nicht
typischer Einsatz	Public Subnet	Private Subnet
Schutzwirkung	keine alleinige Schutzmaßnahme	versteckt private Ressourcen vor direktem Zugriff

Merksatz:

```
Internet Gateway verbindet öffentlich.
NAT-Gateway ermöglicht ausgehend.
```

Routingtabellen in der Cloud

Routingtabellen legen fest, wohin Pakete gesendet werden.

Typische Ziele:

```
lokales Cloud-Netz
Internet Gateway
NAT-Gateway
VPN-Gateway
Peering-Verbindung
Firewall-Appliance
andere Subnetze
lokales Unternehmensnetz
```

Merksatz:

```
Routingtabellen bestimmen Wege im Cloud-Netz.
```

Lokale Route

Jedes Cloud-Netz hat normalerweise eine lokale Route.

Diese erlaubt Kommunikation innerhalb des virtuellen Netzwerks.

Beispiel:

```
10.20.0.0/16
local
```

Damit können Subnetze innerhalb des Cloud-Netzes grundsätzlich miteinander kommunizieren, sofern Sicherheitsregeln es erlauben.

Merksatz:

```
Lokale Route erlaubt Kommunikation innerhalb des Cloud-Netzes.
```

Route ins Internet

Für Internetzugriff braucht ein Public Subnet typischerweise eine Route wie:

```
0.0.0.0/0
über Internet Gateway
```

Für Private Subnets kann die Standardroute über ein NAT-Gateway gehen:

```
0.0.0.0/0
über NAT-Gateway
```

Merksatz:

```
Standardroute entscheidet,
wohin unbekannte Ziele gehen.
```

Route zum Firmennetz

Bei Hybrid Cloud braucht die Cloud eine Route zum lokalen Unternehmensnetz.

Beispiel:

```
lokales Firmennetz:
192.168.10.0/24

Route in Cloud:
```

```
192.168.10.0/24
über VPN-Gateway
```

Gleichzeitig braucht das Firmennetz eine Rückroute zum Cloud-Netz.

Merksatz:

```
Hybrid Cloud braucht Hin- und Rückroute.
```

Rückroute in Cloud-Szenarien

Viele Fehler entstehen, weil nur der Hinweg geplant wurde.

Beispiel:

```
Cloud-Server erreicht lokales System nicht.
```

Oder:

```
lokaler Client erreicht Cloud-Server,
aber Antwort kommt nicht zurück.
```

Mögliche Ursache:

```
Rückroute fehlt
Firewall blockiert Rückverkehr
NAT verändert Adressen
asymmetrisches Routing
```

Merksatz:

```
Auch in der Cloud gilt:
Ohne Rückweg keine funktionierende Verbindung.
```

Security Group

Eine Security Group ist eine virtuelle Firewall-Regelgruppe für Cloud-Ressourcen.

Sie steuert meist:

```
eingehenden Verkehr
ausgehenden Verkehr
Protokolle
Ports
Quellen
Ziele
```

Security Groups werden oft direkt einer Ressource zugeordnet, zum Beispiel einer virtuellen Maschine.

Merksatz:

```
Security Group = Firewall-Regeln direkt an der Cloud-Ressource.
```

Inbound und Outbound

Inbound bedeutet:

```
eingehender Verkehr zur Ressource
```

Outbound bedeutet:

```
ausgehender Verkehr von der Ressource
```

Beispiel Webserver:

```
Inbound:
TCP 443 von Internet erlaubt

Outbound:
Verbindung zur Datenbank oder zu Updateservern erlaubt
```

Merksatz:

```
Inbound und Outbound getrennt prüfen.
```

Stateful Security Group

Viele Security Groups arbeiten stateful.

Stateful bedeutet:

```
Wenn eine Verbindung erlaubt wurde,
ist der Rückverkehr automatisch erlaubt.
```

Beispiel:

```
Client verbindet zu Webserver TCP 443.

Antwortpakete des Webservers zurück zum Client
werden automatisch zugeordnet.
```

Merksatz:

```
Stateful-Regeln merken sich Verbindungen.
```

Network ACL

Eine Network ACL ist eine Zugriffsliste auf Netzwerk- oder Subnetzebene.

Je nach Cloud-Plattform kann sie:

```
eingehende Regeln prüfen
ausgehende Regeln prüfen
stateless arbeiten
Regelreihenfolge beachten
```

Stateless bedeutet:

```
Rückverkehr muss separat erlaubt werden.
```

Merksatz:

```
Network ACLs wirken oft näher am Subnetz und können stateless sein.
```

Security Group und Network ACL vergleichen

Merkmal	Security Group	Network ACL
Ebene	Ressource oder Instanz	Subnetz oder Netzwerkebene
Zustand	oft stateful	oft stateless
Rückverkehr	häufig automatisch erlaubt	häufig separat nötig
Einsatz	feine Ressourcenregeln	zusätzliche Netzgrenze
Fehlerquelle	falsche Quelle oder Port	fehlender Rückverkehr oder Regelreihenfolge

Merksatz:

```
Security Group und Network ACL können beide blockieren.
```

Network Security Group

Network Security Group wird oft abgekürzt:

```
NSG
```

Eine NSG ist eine Regelgruppe, die Netzwerkverkehr auf Subnetz- oder Ressourceneebene steuern kann.

Typische Angaben:

```
Quelle
Ziel
Port
Protokoll
Richtung
Priorität
Aktion
Beschreibung
```

Merksatz:

```
NSG ist eine Cloud-Regelgruppe für Netzwerkzugriffe.
```

Regelreihenfolge und Priorität

Manche Cloud-Regelwerke arbeiten mit Prioritäten.

Dabei gilt:

```
Regel mit höherer Priorität oder niedrigerer Nummer
wird zuerst geprüft
```

Je nach Plattform ist die genaue Logik unterschiedlich.

Wichtig:

```
spezifische Regeln vor allgemeinen Regeln
Deny-Regeln beachten
Standardregeln verstehen
```

Merksatz:

```
Regelreihenfolge kann entscheiden,
ob Verkehr erlaubt oder blockiert wird.
```

Quelle und Ziel in Cloud-Regeln

In Cloud-Regeln können Quellen und Ziele sein:

```
IP-Adressen
Subnetze
Security Groups
Tags
Service Accounts
Load Balancer
Cloud-Dienste
Internet
```

Beispiel:

```
Webserver-Security-Group darf zur Datenbank-Security-Group auf TCP 5432.
```

Das ist oft besser als:

```
gesamtes Netz darf zur Datenbank.
```

Merksatz:

```
Cloud-Regeln möglichst gezielt formulieren.
```

Öffentliche IP-Adresse

Eine öffentliche IP-Adresse macht eine Ressource grundsätzlich aus dem Internet adressierbar.

Aber erreichbar ist sie nur, wenn zusätzlich passen:

```
Routing
Security Group
Firewall
Dienst
Betriebssystem-Firewall
DNS
Load Balancer
Zertifikat
```

Merksatz:

```
Öffentliche IP allein reicht nicht für funktionierenden Zugriff.
```

Private IP-Adresse

Private IP-Adressen werden innerhalb des Cloud-Netzes genutzt.

Typisch für:

```
interne Kommunikation
Datenbanken
Backends
interne APIs
Server-zu-Server-Kommunikation
```

Hybrid-Cloud-Verbindungen

Merksatz:

Private IPs sind für interne Kommunikation im Cloud-Netz.

Öffentliche und private IP vergleichen

Merkmal	öffentliche IP	private IP
Erreichbarkeit	aus Internet möglich	nur intern oder über Verbindung
Einsatz	Webzugriff, Load Balancer	Backend, Datenbank, interne Dienste
Risiko	höher	geringer, aber nicht risikofrei
Schutz	Firewall, Security Group, TLS	Segmentierung, Regeln, IAM

Merksatz:

Öffentlich nur,
wenn es wirklich nötig ist.

Load Balancer in der Cloud

Ein Load Balancer verteilt Anfragen auf mehrere Ziele.

Ziele können sein:

virtuelle Maschinen
Container
App-Instanzen
Backends
Servergruppen

Aufgaben:

Lastverteilung
Health Checks
Hochverfügbarkeit
TLS-Terminierung

```
Weiterleitung
Skalierung unterstützen
```

Merksatz:

```
Load Balancer verteilt Anfragen und erhöht Verfügbarkeit.
```

Health Check

Ein Health Check prüft, ob ein Backend gesund ist.

Beispiele:

```
TCP-Port erreichbar?
HTTP-Status 200?
bestimmter Pfad antwortet?
Anwendung meldet gesund?
Antwortzeit akzeptabel?
```

Wenn ein Backend ungesund ist, leitet der Load Balancer keinen Verkehr mehr dorthin.

Merksatz:

```
Health Check entscheidet,
ob ein Backend Verkehr bekommt.
```

Typische Load-Balancer-Fehler

Häufige Fehler:

```
Backend-Port falsch
Health Check falscher Pfad
Security Group blockiert Load Balancer
Backend-Dienst läuft nicht
TLS-Zertifikat falsch
falscher Host-Header
falsches Protokoll
Backend in falschem Subnetz
```

```
keine gesunden Ziele
```

Merksatz:

```
502 oder 503 in der Cloud hängt oft mit Load Balancer oder Backend zusammen.
```

Cloud-DNS

Cloud-DNS verwaltet Namen für Cloud-Ressourcen.

Typische Aufgaben:

```
öffentliche DNS-Zonen
private DNS-Zonen
interne Namen
Load-Balancer-Namen
Service Discovery
Hybrid-DNS
Weiterleitung zu lokalen DNS-Servern
```

Merksatz:

```
Cloud-DNS verbindet Namen mit Cloud-Ressourcen.
```

Private DNS-Zone

Eine Private DNS-Zone ist nur innerhalb bestimmter Netzwerke sichtbar.

Beispiel:

```
app.internal.cloud
```

Nur Systeme im Cloud-Netz oder verbundenen Netzen können diesen Namen auflösen.

Merksatz:

```
Private DNS ist für interne Cloud-Namen.
```

Public DNS-Zone

Eine Public DNS-Zone ist öffentlich abfragbar.

Beispiel:

```
www.firma.de
```

Sie wird für öffentlich erreichbare Dienste genutzt.

Wichtig:

```
Öffentlicher DNS-Eintrag bedeutet nicht,
dass Zugriff auch erlaubt ist.
```

Merksatz:

```
Public DNS ist sichtbar,
Zugriff hängt trotzdem von Routing und Regeln ab.
```

Cloud Peering

Peering verbindet zwei virtuelle Netzwerke miteinander.

Beispiel:

```
VPC A
↔
VPC B
```

Oder:

```
VNet A
↔
VNet B
```

Ziel:

```
private Kommunikation zwischen Cloud-Netzen
```

Wichtig:

```
Routen
Security Groups
DNS
Überschneidung von IP-Netzen
Berechtigungen
```

Merksatz:

```
Peering verbindet Cloud-Netze privat miteinander.
```

Peering ist kein Transit automatisch

Ein häufiger Denkfehler:

```
Wenn Netz A mit B verbunden ist
und B mit C verbunden ist,
kann A automatisch C erreichen.
```

Das stimmt nicht immer.

Viele Peering-Verbindungen sind nicht automatisch transitiv.

Merksatz:

```
Peering bedeutet nicht automatisch Durchleitung zu dritten Netzen.
```

Transit Gateway oder Hub-and-Spoke

In größeren Cloud-Netzen nutzt man oft zentrale Netzwerkarchitekturen.

Beispiel:

```
Hub-Netz
mit Firewall,
VPN,
Internetzugang
und zentralen Diensten

Spoke-Netze
für Anwendungen,
Abteilungen
oder Umgebungen
```

Vorteil:

```
zentrale Kontrolle
einheitliches Routing
bessere Segmentierung
übersichtliche Sicherheitsregeln
```

Merksatz:

```
Hub-and-Spoke ordnet viele Cloud-Netze zentral.
```

Cloud-VPN

Cloud-VPN verbindet Cloud-Netze mit anderen Netzen.

Beispiele:

```
Cloud ↔ lokales Rechenzentrum

Cloud ↔ Niederlassung

Cloud ↔ andere Cloud
```

Wichtig:

```
passende IP-Netze
Routing auf beiden Seiten
```

```
Firewall-Regeln
Verschlüsselung
Monitoring
Redundanz
```

Merksatz:

```
Cloud-VPN braucht Planung auf Cloud-Seite und lokaler Seite.
```

Direktverbindung zur Cloud

Neben VPN kann es direkte private Verbindungen zu Cloud-Anbietern geben.

Eigenschaften:

```
private Verbindung
meist stabilere Leistung
geringere Latenz möglich
höhere Bandbreite möglich
kein normaler Internetweg
oft teurer und aufwendiger
```

Merksatz:

```
Direktverbindung kann für kritische Hybrid-Cloud-Szenarien sinnvoll sein.
```

Bastion Host in der Cloud

Ein Bastion Host ist ein besonders geschützter Sprungserver.

Zweck:

```
Adminzugriffe auf private Cloud-Ressourcen ermöglichen,
ohne diese direkt ins Internet zu stellen.
```

Beispiel:

```
Admin
→ Bastion Host
→ private VM
```

Wichtig:

```
MFA
Logging
beschränkte Quellen
regelmäßige Updates
keine Dauerzugänge
starke Härtung
```

Merksatz:

```
Bastion Host reduziert direkte öffentliche Adminzugriffe.
```

Managementports nicht öffentlich öffnen

Kritische Managementports sollten nicht offen im Internet liegen.

Beispiele:

```
SSH TCP 22
RDP TCP 3389
Datenbankports
Admin-Weboberflächen
Kubernetes-API
Storage-Adminzugänge
```

Besser:

```
VPN
Bastion Host
Zero-Trust-Zugang
private Subnetze
eingeschränkte Quell-IP
MFA
```

Merksatz:

```
Managementzugänge gehören nicht breit ins Internet.
```

Cloud-Firewall

Eine Cloud-Firewall kann zentrale Filterung übernehmen.

Sie schützt zum Beispiel:

```
Internetzugang
Verbindungen zwischen Subnetzen
Verbindung zu lokalen Netzen
Cloud-zu-Cloud-Verkehr
DMZ-ähnliche Bereiche
```

Funktionen können sein:

```
Paketfilter
Stateful Inspection
Anwendungskontrolle
IDS/IPS
URL-Filter
Logging
```

Merksatz:

```
Cloud-Firewall ergänzt Security Groups und Netzsegmentierung.
```

Cloud-Netzsegmentierung

Auch in der Cloud sollte man Systeme trennen.

Beispiele:

```
Web-Schicht
App-Schicht
Datenbank-Schicht
```

```
Management-Schicht
Entwicklungsumgebung
Testumgebung
Produktionsumgebung
DMZ-ähnliche Zone
```

Merksatz:

```
Cloud braucht Segmentierung wie lokale Netze.
```

Drei-Schichten-Architektur in der Cloud

Ein typisches Muster:

```
Web-Schicht:
öffentlich erreichbar über Load Balancer

App-Schicht:
nur intern vom Webserver erreichbar

Datenbank-Schicht:
nur von App-Servern erreichbar
```

Vorteil:

```
bessere Sicherheit
klare Kommunikationswege
weniger Angriffsfläche
```

Merksatz:

```
Datenbanken gehören normalerweise nicht direkt ins Internet.
```

Umgebungen trennen

Cloud-Ressourcen sollten nach Umgebung getrennt werden.

Typische Umgebungen:

```
Entwicklung
Test
Staging
Produktion
```

Warum?

```
Testfehler sollen Produktion nicht stören.
Rechte können getrennt werden.
Kosten können getrennt werden.
Änderungen werden kontrollierter.
Sicherheitsregeln sind klarer.
```

Merksatz:

```
Entwicklung,
Test
und Produktion sauber trennen.
```

Cloud-Netzwerk und IAM

Netzwerkregeln allein reichen nicht.

Auch Identitäten und Rechte sind wichtig.

Beispiel:

```
Benutzer darf Security Group ändern.
Benutzer darf öffentliche IP vergeben.
Benutzer darf Route zum Internet setzen.
Benutzer darf Firewall-Regel öffnen.
```

Diese Rechte können sicherheitskritisch sein.

Merksatz:

```
Wer Cloud-Netzwerke ändern darf,
kann Sicherheit stark beeinflussen.
```

Cloud-Netzwerk-Fehlkonfigurationen

Häufige Fehler:

Datenbank öffentlich erreichbar
SSH offen für das ganze Internet
RDP offen für das ganze Internet
Security Group zu breit
falsche Route ins Internet
Private Subnet versehentlich öffentlich
fehlende Rückroute
falscher Load-Balancer-Health-Check
keine Logs
veraltete Bastion Hosts
Peering ohne Sicherheitsprüfung

Merksatz:

Viele Cloud-Sicherheitsprobleme sind Netzwerk-Fehlkonfigurationen.

Cloud-Netzwerk-Logging

Wichtige Logquellen:

Flow Logs
Firewall-Logs
Load-Balancer-Logs
DNS-Logs
VPN-Logs
IAM-Logs
Routing-Änderungen
Security-Group-Änderungen
WAF-Logs

Merksatz:

Netzwerklogs zeigen,
welcher Verkehr erlaubt oder blockiert wurde.

Flow Logs

Flow Logs zeigen Netzwerkverbindungen auf Ebene von Metadaten.

Sie enthalten typischerweise:

```
Quelle
Ziel
Port
Protokoll
Aktion
Zeit
Datenmenge
Interface oder Ressource
```

Sie zeigen normalerweise nicht den vollständigen Paketinhalt.

Merksatz:

```
Flow Logs zeigen Verbindungsdaten,
aber keinen kompletten Paketmitschnitt.
```

Cloud-Netzwerk-Monitoring

Überwacht werden sollten:

```
VPN-Tunnelstatus
Load Balancer
Backend-Gesundheit
Paketverlust
Latenz
Bandbreite
Firewall-Drops
DNS-Fehler
öffentliche IPs
ungewöhnlicher Datenverkehr
Kosten durch Traffic
```

Merksatz:

Cloud-Netzwerk-Monitoring schützt Betrieb und Kosten.

Cloud-Netzwerk-Fehlersuche

Sinnvolle Reihenfolge:

1. Quelle und Ziel bestimmen.
2. IP-Adressen prüfen.
3. DNS prüfen.
4. Subnetz prüfen.
5. Routingtabelle prüfen.
6. Security Group prüfen.
7. Network ACL oder NSG prüfen.
8. Load Balancer prüfen.
9. Zielsystem und Dienst prüfen.
10. Host-Firewall prüfen.
11. Logs prüfen.
12. Rückweg prüfen.

Merksatz:

Auch in der Cloud gilt:
DNS,
Route,
Firewall,
Dienst
und Rückweg prüfen.

Fehlerbild: Cloud-VM nicht per SSH erreichbar

Mögliche Ursachen:

keine öffentliche IP
DNS zeigt falsch
Routing zum Internet fehlt
Security Group blockiert TCP 22
Network ACL blockiert

SSH-Dienst läuft nicht
Host-Firewall blockiert
falscher Benutzer oder Schlüssel
Bastion Host nötig
Quell-IP nicht erlaubt

Merksatz:

SSH-Fehler in Cloud mit IP,
Route,
Security Group,
Dienst
Schlüssel
und Bastion prüfen.

Fehlerbild: Webdienst in Cloud nicht erreichbar

Mögliche Ursachen:

DNS falsch
Load Balancer falsch
Zertifikat falsch
Security Group blockiert TCP 443
Backend ungesund
Health Check falsch
Anwendung läuft nicht
falscher Port
private Ressource ohne öffentliche Freigabe
WAF blockiert

Merksatz:

Webfehler in Cloud mit DNS,
Load Balancer,
Security Group,
TLS
und Backend prüfen.

Fehlerbild: Cloud-Datenbank öffentlich erreichbar

Das ist meistens ein Sicherheitsproblem.

Mögliche Ursachen:

```
Datenbank in Public Subnet
öffentliche IP vergeben
Security Group zu breit
Firewall-Regel erlaubt 0.0.0.0/0
Authentifizierung schwach
kein Private Endpoint
falsches Routing
```

Besser:

```
Private Subnet
Zugriff nur von App-Schicht
Security Group gezielt
keine öffentliche IP
Verschlüsselung
starke Authentifizierung
```

Merksatz:

```
Datenbanken gehören normalerweise nicht öffentlich ins Internet.
```

Fehlerbild: Cloud und On-Premises erreichen sich nicht

Mögliche Ursachen:

```
VPN-Tunnel down
Route in Cloud fehlt
Route lokal fehlt
Firewall blockiert
Security Group blockiert
IP-Netze überschneiden sich
DNS falsch
NAT falsch
```

Rückroute fehlt

Cloud-Gateway falsch konfiguriert

Merksatz:

Hybrid-Verbindungen brauchen Regeln und Routen auf beiden Seiten.

Checkliste: Cloud-Netzwerk sicher planen

IP-Adressbereich eindeutig wählen.

Subnetze sauber trennen.

Public und Private Subnets unterscheiden.

Datenbanken nicht öffentlich bereitstellen.

Managementzugänge nicht breit öffnen.

Security Groups eng setzen.

Rückwege planen.

Hybrid-Routen dokumentieren.

DNS-Konzept erstellen.

Logging aktivieren.

Monitoring einrichten.

Änderungen dokumentieren.

Rechte zur Netzwerkänderung begrenzen.

Merksatz:

Cloud-Netzwerk zuerst planen,

dann Ressourcen bereitstellen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist ein virtuelles Netzwerk in der Cloud?
- Was bedeutet VPC?
- Was ist ein Subnetz in der Cloud?
- Was ist der Unterschied zwischen Public Subnet und Private Subnet?
- Was ist ein Internet Gateway?

- Was ist ein NAT-Gateway?
- Wofür nutzt man Routingtabellen in der Cloud?
- Was ist eine Security Group?
- Was ist eine Network ACL?
- Was ist eine NSG?
- Was ist der Unterschied zwischen öffentlicher und privater IP?
- Wofür nutzt man einen Load Balancer?
- Was ist ein Health Check?
- Was ist Cloud Peering?
- Warum ist Peering nicht automatisch transitiv?
- Warum sollte eine Datenbank nicht öffentlich erreichbar sein?
- Wie geht man bei Cloud-Netzwerk-Fehlersuche vor?

Typische Prüfungsfallen

Cloud-Netzwerke sind virtuell,
aber echte Netzplanung bleibt nötig.

VPC und VNet beschreiben virtuelle Cloud-Netze.

Public Subnet ist nicht für alle Systeme geeignet.

Private Subnet schützt vor direkter öffentlicher Erreichbarkeit.

Internet Gateway allein reicht nicht für Zugriff.

NAT-Gateway erlaubt typischerweise ausgehende Verbindungen.

Routingtabellen bestimmen Wege.

Rückroute nicht vergessen.

Security Groups wirken wie virtuelle Firewalls.

Network ACLs können zusätzlich blockieren.

Stateful und stateless unterscheiden.

Öffentliche IP bedeutet höheres Risiko.

Datenbanken nicht öffentlich freigeben.

Load Balancer braucht gesunde Backends.

Health Check muss zum Dienst passen.

Peering ist nicht automatisch transitiv.

Cloud-Firewall ersetzt nicht saubere Segmentierung.

Managementports nicht breit ins Internet öffnen.

Cloud-Netzwerkänderungen sind sicherheitskritisch.

Flow Logs zeigen Metadaten,
nicht vollständige Pakete.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
virtuelles Netzwerk	logisch getrenntes Cloud-Netz
VPC	Virtual Private Cloud
VNet	Virtual Network
Subnetz	Teilbereich eines Cloud-Netzes
Public Subnet	öffentlich angebundenes Subnetz
Private Subnet	internes Subnetz ohne direkte öffentliche Erreichbarkeit
Internet Gateway	Verbindung eines Cloud-Netzes zum Internet
NAT-Gateway	ausgehender Internetzugriff für private Ressourcen
Routingtabelle	Wege zu Zielnetzen
lokale Route	Route innerhalb des Cloud-Netzes
Security Group	virtuelle Firewall-Regelgruppe
Network ACL	Zugriffsliste auf Netzwerk- oder Subnetzebene
NSG	Network Security Group
Stateful	Rückverkehr wird automatisch zugeordnet
Stateless	Rückverkehr muss separat erlaubt werden

Begriff	Kurze Erklärung
öffentliche IP	aus dem Internet adressierbare IP
private IP	interne Adresse im Cloud-Netz
Load Balancer	verteilt Anfragen auf Ziele
Health Check	Prüfung der Backend-Gesundheit
Cloud-DNS	Namensauflösung für Cloud-Ressourcen
Private DNS-Zone	interne DNS-Zone
Public DNS-Zone	öffentlich sichtbare DNS-Zone
Peering	Verbindung zwischen Cloud-Netzen
Hub-and-Spoke	zentrale Netzwerkarchitektur
Cloud-VPN	VPN-Verbindung zu Cloud-Netz
Bastion Host	gehärteter Sprungserver
Flow Logs	Metadaten zu Netzwerkverbindungen

IHK-sichere Kurzformulierung

Cloud-Netzwerke bestehen aus virtuellen Netzwerken wie VPC oder VNet, Subnetzen, Routingtabellen, Security Groups, Network ACLs, Gateways, Load Balancern und DNS. Public Subnets sind für öffentlich erreichbare Komponenten wie Load Balancer oder Bastion Hosts gedacht, während Private Subnets interne Ressourcen wie Datenbanken oder Backends schützen. Ein Internet Gateway verbindet ein Cloud-Netz mit dem Internet, während ein NAT-Gateway privaten Ressourcen ausgehenden Internetzugriff ermöglicht. Security Groups und NSGs wirken als virtuelle Firewall-Regeln. Bei Cloud-Netzwerk-Fehlern müssen DNS, IP-Adressen, Routing, Security Groups, Network ACLs, Load Balancer, Zielsysteme, Host-Firewalls und Rückwege geprüft werden.

Merksätze

```
Cloud-Netzwerke sind virtuell,
aber echte Netzplanung bleibt nötig.

VPC = Virtual Private Cloud.

VNet = Virtual Network.

Virtuelles Netzwerk ist logisch getrennt.

IP-Bereiche sauber planen.
```

Cloud-Netze dürfen sich nicht ungewollt überschneiden.

Subnetze strukturieren Cloud-Ressourcen.

Public Subnet für öffentliche Komponenten.

Private Subnet für interne Komponenten.

Datenbank nicht öffentlich erreichbar machen.

Internet Gateway verbindet zum Internet.

NAT-Gateway ermöglicht ausgehenden Zugriff.

Routingtabellen bestimmen Wege.

Standardroute entscheidet bei unbekannten Zielen.

Hybrid Cloud braucht Hin- und Rückrouten.

Security Group ist virtuelle Firewall.

Inbound und Outbound getrennt prüfen.

Stateful merkt sich Verbindungen.

Stateless braucht separate Rückregeln.

Network ACL kann zusätzlich blockieren.

NSG steuert Netzwerkzugriffe.

Öffentliche IP nur wenn nötig.

Private IP für interne Kommunikation.

Load Balancer verteilt Anfragen.

Health Check prüft Backend-Gesundheit.

Cloud-DNS kann öffentlich oder privat sein.

Peering verbindet Cloud-Netze.

Peering ist nicht automatisch transitiv.

Hub-and-Spoke schafft zentrale Kontrolle.

Cloud-VPN braucht Routen beidseitig.

Bastion Host schützt Adminzugriffe.

Managementports nicht breit öffnen.

Segmentierung gilt auch in der Cloud.

IAM beeinflusst Netzwerksicherheit.

Flow Logs zeigen Verbindungsmetadaten.

Cloud-Fehlersuche:
DNS,
Route,
Security Group,
Dienst,
Rückweg.