15.8 Merksätze und Prüfungswissen zu Cloud und modernen Bereitstellungsmodellen

Diese Seite fasst die wichtigsten Inhalte zu Cloud, Bereitstellungsmodellen, Service-Modellen, Cloud-Netzwerken, Cloud-Sicherheit, Cloud-Speicher, Backup, Monitoring, Skalierung und Kostenkontrolle zusammen.

Cloud ist prüfungsrelevant, weil sie viele Themen verbindet:

- Netzwerktechnik
- Serverbetrieb
- Virtualisierung
- Sicherheit
- Datenschutz
- Backup
- Kosten
- Rechteverwaltung
- Hochverfügbarkeit
- Monitoring

Merksatz:

Cloud ist kein einzelnes Produkt,
sondern ein Betriebs- und Bereitstellungsmodell für IT-Ressourcen.

Cloud-Grundidee

Cloud bedeutet:

IT-Ressourcen werden über ein Netzwerk als Dienst bereitgestellt.

Beispiele:

virtuelle Server
Speicher
Datenbanken
Anwendungen

```
Plattformen
Container
Backup
Identitätsdienste
Netzwerkdienste
Sicherheitsdienste
```

Merksatz:

```
Cloud = IT-Ressourcen als Dienst.
```

Cloud ist nicht automatisch weniger Verantwortung

Ein häufiger Denkfehler:

```
Alles liegt in der Cloud,
also kümmert sich der Anbieter um alles.
```

Das ist falsch.

Der Anbieter übernimmt je nach Modell bestimmte Aufgaben.

Der Kunde bleibt verantwortlich für:

```
Benutzer
Rollen
Berechtigungen
Daten
sichere Konfiguration
Datenschutz
Zugriffsschutz
Backup-Konzept
Kostenkontrolle
Monitoring
Compliance
```

Merksatz:

Cloud verlagert Verantwortung,
sie beseitigt Verantwortung nicht.

On-Premises

On-Premises bedeutet:

IT wird lokal selbst betrieben.

Beispiele:

eigener Serverraum
eigenes Rechenzentrum
eigene Hardware
eigene Virtualisierung
eigene Netzwerkinfrastruktur

Vorteile:

hohe Kontrolle
direkte Verwaltung
eigene Vorgaben

Nachteile:

Hardwarekosten
Wartungsaufwand
eigene Verantwortung für Ausfallsicherheit

Merksatz:

On-Premises = lokal selbst betrieben.

Public Cloud

Public Cloud bedeutet:

Ein Anbieter stellt Cloud-Ressourcen für viele Kunden bereit.

Eigenschaften:

Anbieterplattform
viele Kunden
logische Mandantentrennung
nutzungsabhängige Abrechnung
schnelle Bereitstellung
hohe Skalierbarkeit

Merksatz:

Public Cloud = öffentliche Anbieterplattform für viele Kunden.

Private Cloud

Private Cloud bedeutet:

Cloud-Prinzipien werden für eine einzelne Organisation bereitgestellt.

Sie kann laufen:

im eigenen Rechenzentrum
bei einem Dienstleister
in einer dedizierten Umgebung

Wichtig:

Virtualisierung allein ist noch keine vollständige Private Cloud.

Typische Cloud-Merkmale sind:

Self-Service
Automatisierung
Ressourcenpooling

```
schnelle Bereitstellung
messbare Nutzung
zentrale Verwaltung
```

Merksatz:

```
Private Cloud = Cloud für eine Organisation.
```

Hybrid Cloud

Hybrid Cloud kombiniert lokale oder private IT mit Public Cloud.

Beispiele:

```
lokale Datenbank plus Cloud-Webanwendung

lokales Rechenzentrum plus Cloud-Backup

lokale Benutzerverwaltung plus Cloud-SaaS

lokale Systeme plus Cloud-Skalierung
```

Merksatz:

```
Hybrid Cloud = lokal oder privat plus Public Cloud.
```

Multi Cloud

Multi Cloud bedeutet:

```
Ein Unternehmen nutzt mehrere Cloud-Anbieter gleichzeitig.
```

Beispiel:

```
Anbieter A für virtuelle Maschinen

Anbieter B für Office und E-Mail
```

Anbieter C für Backup

Anbieter D für Datenanalyse

Merksatz:

Multi Cloud = mehrere Cloud-Anbieter parallel.

Hybrid Cloud und Multi Cloud unterscheiden

Begriff	Kerngedanke
Hybrid Cloud	lokale/private IT plus Public Cloud
Multi Cloud	mehrere Cloud-Anbieter
Hybrid und Multi Cloud kombiniert	lokale IT plus mehrere Cloud-Anbieter

Merksatz:

Hybrid beschreibt die Verbindung lokal plus Cloud.
Multi Cloud beschreibt mehrere Anbieter.

Community Cloud

Community Cloud bedeutet:

Eine Cloud wird von mehreren Organisationen mit ähnlichen Anforderungen genutzt.

Beispiele:

Behörden
Bildung
Forschung
Gesundheitswesen
bestimmte Branchen

Merksatz:

Community Cloud = Cloud für eine bestimmte Gemeinschaft.

Bereitstellungsmodelle im Überblick

Modell	Kurze Erklärung
On-Premises	lokal selbst betrieben
Public Cloud	Anbieterplattform für viele Kunden
Private Cloud	Cloud für eine Organisation
Hybrid Cloud	lokale/private IT plus Public Cloud
Multi Cloud	mehrere Cloud-Anbieter
Community Cloud	Cloud für Organisationen mit gemeinsamen Anforderungen

Merksatz:

Bereitstellungsmodell beschreibt,
wo und für wen Cloud betrieben wird.

Service-Modelle

Die wichtigsten Cloud-Service-Modelle sind:

- IaaS
- PaaS
- SaaS

Sie beschreiben, welche IT-Schichten der Anbieter bereitstellt und welche der Kunde selbst verwaltet.

Merksatz:

Service-Modell beschreibt,
was als Dienst bereitgestellt wird.

IaaS

IaaS steht für:

```
Infrastructure as a Service
```

Der Anbieter stellt virtuelle Infrastruktur bereit.

Beispiele:

```
virtuelle Maschinen
virtuelle Netzwerke
virtuelle Festplatten
Load Balancer
Firewalls
IP-Adressen
Storage
```

Der Kunde verwaltet typischerweise:

```
Betriebssystem
Anwendungen
Daten
Patches innerhalb der VM
Benutzer
Sicherheitskonfiguration
```

Merksatz:

```
IaaS = virtuelle Infrastruktur statt eigener Hardware.
```

PaaS

PaaS steht für:

```
Platform as a Service
```

Der Anbieter stellt eine Plattform bereit, auf der Anwendungen laufen können.

Beispiele:

```
Web-App-Plattform
verwaltete Datenbank
Laufzeitumgebung
Containerplattform
API-Plattform
Entwicklungsplattform
```

Der Kunde verwaltet typischerweise:

```
Anwendung
Daten
Konfiguration
Benutzer
Berechtigungen
```

Merksatz:

```
PaaS = Plattform für eigene Anwendungen.
```

SaaS

SaaS steht für:

```
Software as a Service
```

Der Kunde nutzt eine fertige Anwendung.

Beispiele:

```
E-Mail
Online-Office
CRM
Ticketsystem
Cloud-Speicher
Videokonferenzdienst
Projektmanagement
```

Der Kunde verwaltet typischerweise:

Benutzer
Rollen
Berechtigungen
Daten
Freigaben
Einstellungen
MFA

Merksatz:

SaaS = fertige Software aus der Cloud.

IaaS, PaaS und SaaS vergleichen

Modell	Anbieter stellt bereit	Kunde verwaltet vor allem
IaaS	virtuelle Infrastruktur	Betriebssystem, Anwendung, Daten
PaaS	Plattform und Laufzeitumgebung	Anwendung, Daten, Konfiguration
SaaS	fertige Anwendung	Benutzer, Rechte, Daten, Einstellungen

Merksatz:

IaaS gibt viel Kontrolle.
SaaS nimmt viel Betrieb ab.
PaaS liegt dazwischen.

Shared Responsibility Model

Shared Responsibility Model bedeutet:

Anbieter und Kunde teilen sich die Verantwortung.

Je nach Service-Modell verschiebt sich diese Verantwortung.

Bei IaaS:

Kunde hat viel technische Verantwortung.

Bei PaaS:

```
Anbieter übernimmt Plattform,
Kunde bleibt für Anwendung und Daten verantwortlich.
```

Bei SaaS:

```
Anbieter betreibt Anwendung,
Kunde bleibt für Nutzung,
Benutzer,
Rechte
und Daten verantwortlich.
```

Merksatz:

```
Cloud-Sicherheit ist gemeinsame Verantwortung.
```

Wichtigste Regel zur Verantwortung

Daten, Benutzer und Rechte bleiben fast immer Kundenthema.

Auch bei SaaS muss der Kunde prüfen:

```
Wer darf zugreifen?
Welche Rollen gibt es?
Ist MFA aktiv?
Welche Daten liegen im Dienst?
Welche Freigaben existieren?
Wie werden Benutzer deaktiviert?
Wie werden Daten gesichert oder exportiert?
```

Merksatz:

```
Je fertiger der Dienst,
desto weniger Technikbetrieb,
aber Daten und Zugriffe bleiben wichtig.
```

Virtualisierung

Virtualisierung bedeutet:

```
physische Ressourcen werden in virtuelle Ressourcen aufgeteilt.
```

Beispiele:

```
virtuelle Maschinen
virtuelle Netzwerke
virtuelle Festplatten
virtuelle Firewalls
virtuelle Load Balancer
```

Merksatz:

```
Virtualisierung ist eine technische Grundlage vieler Cloud-Dienste.
```

Container

Container verpacken Anwendungen mit ihren Abhängigkeiten.

Sie enthalten typischerweise:

```
Anwendung
Bibliotheken
Laufzeitumgebung
Konfiguration
```

Sie teilen sich den Kernel des Hosts.

Merksatz:

```
Container sind leichtgewichtige,
portable Anwendungseinheiten.
```

Kubernetes

Kubernetes ist eine Plattform zur Container-Orchestrierung.

Es verwaltet:

```
Container
Pods
Services
Deployments
Skalierung
Rollouts
Netzwerke
Konfigurationen
```

Merksatz:

```
Kubernetes orchestriert Container in Clustern.
```

Serverless

Serverless bedeutet nicht, dass keine Server existieren.

Es bedeutet:

```
Der Kunde verwaltet keine einzelnen Server.
```

Der Anbieter betreibt die Infrastruktur.

Der Kunde stellt Code, Funktionen oder Konfiguration bereit.

Merksatz:

```
Serverless = keine Serververwaltung durch den Kunden.
```

FaaS

FaaS steht für:

```
Function as a Service
```

Dabei werden einzelne Funktionen ereignisgesteuert ausgeführt.

Beispiele:

```
Datei hochgeladen
API-Aufruf
Zeitplan
Nachricht in Warteschlange
```

Merksatz:

```
FaaS führt Funktionen bei Ereignissen aus.
```

Cloud-Netzwerke

Cloud-Netzwerke bestehen aus virtuellen Netzwerkkomponenten.

Typische Bestandteile:

```
VPC
VNet
Subnetze
Routingtabellen
Security Groups
Network ACLs
NSGs
Internet Gateway
NAT-Gateway
VPN-Gateway
Load Balancer
DNS
Peering
```

Merksatz:

```
Cloud-Netzwerke sind virtuell,
brauchen aber echte Netzplanung.
```

VPC und VNet

VPC steht für:

```
Virtual Private Cloud
```

VNet steht für:

```
Virtual Network
```

Beide beschreiben ein logisch getrenntes Cloud-Netzwerk.

Darin werden festgelegt:

```
IP-Bereich
Subnetze
Routen
Sicherheitsregeln
Gateways
Ressourcen
```

Merksatz:

```
VPC oder VNet = eigenes virtuelles Cloud-Netz.
```

Public Subnet und Private Subnet

Subnetztyp	Zweck
Public Subnet	öffentlich erreichbare Komponenten
Private Subnet	interne Komponenten ohne direkten Internetzugriff

Beispiele:

```
Public Subnet:
Load Balancer,
Bastion Host,
Reverse Proxy

Private Subnet:
Datenbank,
Backend,
```

interne API,
Verarbeitungssystem

Merksatz:

Öffentlich nur,
was wirklich öffentlich sein muss.

Internet Gateway und NAT-Gateway

Internet Gateway:

verbindet Cloud-Netz mit dem Internet

NAT-Gateway:

erlaubt privaten Ressourcen ausgehenden Internetzugriff,
ohne direkt eingehend erreichbar zu sein

Merksatz:

Internet Gateway verbindet öffentlich.
NAT-Gateway erlaubt ausgehend für private Ressourcen.

Security Group

Eine Security Group ist eine virtuelle Firewall-Regelgruppe.

Sie steuert:

eingehenden Verkehr
ausgehenden Verkehr
Ports
Protokolle
Quellen
Ziele

Merksatz:

Security Group = Firewall-Regeln an Cloud-Ressourcen.

Network ACL und NSG

Network ACL:

Zugriffsliste auf Netzwerk- oder Subnetzebene

NSG:

Network Security Group,
Regelgruppe für Netzwerkzugriffe

Wichtig:

Je nach Plattform können Regeln stateful oder stateless sein.

Merksatz:

Security Groups,
ACLs
und NSGs können alle Zugriff beeinflussen.

Stateful und Stateless

Stateful bedeutet:

Rückverkehr zu erlaubten Verbindungen wird automatisch zugeordnet.

Stateless bedeutet:

Rückverkehr muss separat erlaubt werden.

Merksatz:

```
Stateful merkt sich Verbindungen.
Stateless prüft jedes Paket einzeln.
```

Load Balancer

Ein Load Balancer verteilt Anfragen auf mehrere Ziele.

Vorteile:

```
Lastverteilung
höhere Verfügbarkeit
Skalierung
Wartung einzelner Backends
Health Checks
```

Merksatz:

```
Load Balancer verteilt Verkehr auf gesunde Ziele.
```

Health Check

Ein Health Check prüft, ob ein Backend gesund ist.

Beispiele:

```
TCP-Port erreichbar
HTTP-Status 200
Anwendung meldet gesund
Antwortzeit akzeptabel
```

Merksatz:

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

Peering

Peering verbindet zwei Cloud-Netze privat miteinander.

Wichtig:

```
IP-Netze dürfen sich nicht überschneiden.
Routen müssen passen.
Sicherheitsregeln müssen passen.
Peering ist nicht automatisch transitiv.
```

Merksatz:

```
Peering verbindet Netze,
leitet aber nicht automatisch zu dritten Netzen weiter.
```

Cloud-VPN

Cloud-VPN verbindet Cloud-Netze mit anderen Netzen.

Beispiele:

```
Cloud ↔ lokales Rechenzentrum

Cloud ↔ Niederlassung

Cloud ↔ andere Cloud
```

Wichtig:

```
IP-Planung
Routing
Firewall-Regeln
Verschlüsselung
Monitoring
Rückrouten
```

Merksatz:

```
Cloud-VPN braucht Regeln und Routen auf beiden Seiten.
```

Cloud-Speicherarten

Die wichtigsten Cloud-Speicherarten sind:

- Objektspeicher
- Blockspeicher
- Dateispeicher
- Archivspeicher

Merksatz:

Speicherart nach Einsatzzweck auswählen.

Objektspeicher

Objektspeicher speichert Daten als Objekte.

Ein Objekt enthält:

Inhalt
Metadaten
eindeutigen Schlüssel

Typische Nutzung:

Backups
Bilder
Videos
Logs
Archive
Dokumente
große unstrukturierte Datenmengen

Merksatz:

Objektspeicher eignet sich für viele unstrukturierte Daten.

Bucket

Ein Bucket ist ein Speicherbehälter für Objekte.

Wichtig:

```
Bucket-Berechtigungen sind sicherheitskritisch.
```

Fehler:

```
Bucket öffentlich lesbar
```

Folge:

```
vertrauliche Daten können offenliegen.
```

Merksatz:

```
Öffentliche Buckets vermeiden.
```

Blockspeicher

Blockspeicher verhält sich wie eine virtuelle Festplatte.

Typische Nutzung:

```
virtuelle Maschinen
Betriebssystemplatten
Datenbanken
Anwendungen mit Dateisystem
```

Merksatz:

```
Blockspeicher = virtuelle Festplatte.
```

Dateispeicher

Dateispeicher stellt klassische Datei- und Ordnerfreigaben bereit.

Typische Protokolle:

```
SMB
NFS
```

Typische Nutzung:

```
gemeinsame Dateien
Benutzerdateien
klassische Anwendungen
zentrale Ablagen
```

Merksatz:

```
Dateispeicher = Freigabe mit Dateien und Ordnern.
```

Backup in der Cloud

Cloud ersetzt kein Backup.

Auch Cloud-Daten können verloren gehen durch:

```
Benutzerfehler
Ransomware
Fehlkonfiguration
falsche Synchronisation
gelöschte Benutzer
kompromittierte Adminzugänge
Anbieterproblem
fehlerhafte Anwendung
```

Merksatz:

```
Cloud ist kein Backup.
```

RPO und RTO

RPO steht für:

Recovery Point Objective

Frage:

Wie viel Datenverlust ist maximal erlaubt?

RTO steht für:

Recovery Time Objective

Frage:

Wie lange darf Wiederherstellung dauern?

Merksatz:

RPO = Datenverlust.
RTO = Wiederherstellungszeit.

Backup und Replikation

Backup:

dient der Wiederherstellung alter oder gesicherter Zustände

Replikation:

kopiert Daten auf ein anderes System oder in eine andere Region

Wichtig:

Replikation ist kein vollständiger Backup-Ersatz,
weil Fehler und Löschungen mitkopiert werden können.

Merksatz:

Backup schützt Wiederherstellung.
Replikation schützt eher Verfügbarkeit.

3-2-1-Regel

Die 3-2-1-Regel bedeutet:

3 Kopien der Daten

2 unterschiedliche Speichermedien oder Speicherarten

1 Kopie außer Haus oder getrennt vom Hauptsystem

Merksatz:

Mehrere getrennte Kopien schützen besser.

Immutable Backup

Immutable bedeutet:

unveränderlich

Ein Immutable Backup kann für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Vorteile:

Schutz vor Ransomware
Schutz vor versehentlicher Löschung
Schutz vor kompromittierten Konten

Merksatz:

Immutable Backup schützt vor Manipulation und Löschung.

IAM

IAM steht für:

```
Identity and Access Management
```

IAM regelt:

```
Benutzer
Gruppen
Rollen
Berechtigungen
Richtlinien
Servicekonten
API-Schlüssel
MFA
```

Merksatz:

```
IAM entscheidet,
wer was in der Cloud darf.
```

Authentifizierung und Autorisierung

Authentifizierung:

```
Wer bist du?
```

Autorisierung:

```
Was darfst du?
```

Beispiel:

```
Benutzer meldet sich an:
Authentifizierung

Benutzer darf eine VM löschen:
Autorisierung
```

Merksatz:

```
Anmeldung und Berechtigung unterscheiden.
```

MFA

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

MFA ist besonders wichtig für:

```
Administratoren
externe Benutzer
Cloud-Portale
IAM
Abrechnung
Produktion
sensible Daten
```

Merksatz:

```
Cloud-Adminzugänge ohne MFA sind ein hohes Risiko.
```

Least Privilege

Least Privilege bedeutet:

```
nur die Rechte vergeben,
die wirklich benötigt werden.
```

In der Cloud besonders wichtig, weil einzelne Rechte große Auswirkungen haben können.

Beispiele:

```
Speicher öffentlich machen
Firewall öffnen
```

VM löschen
Backup löschen
Rollen vergeben
API-Schlüssel erstellen

Merksatz:

Cloud-Rechte minimal vergeben.

Servicekonten und API-Schlüssel

Servicekonten sind Identitäten für Dienste oder Anwendungen.

API-Schlüssel erlauben Programmen Zugriff auf Cloud-Dienste.

Risiken:

zu viele Rechte
Schlüssel im Quellcode
keine Rotation
keine Löschung nach Projektende
Veröffentlichung in Repositories

Merksatz:

Servicekonten und API-Schlüssel wie kritische Zugangsdaten behandeln.

Secrets

Secrets sind geheime Informationen.

Beispiele:

Passwörter
Tokens
API-Schlüssel
private Schlüssel
Zertifikate

Datenbankkennwörter

Merksatz:

Secrets gehören nicht in Quellcode,
Tickets,
Chats
oder ungeschützte Dokumente.

RBAC und ABAC

RBAC:

rollenbasierte Zugriffskontrolle

ABAC:

attributbasierte Zugriffskontrolle

Modell	Grundlage
RBAC	Rollen
ABAC	Attribute

Merksatz:

RBAC arbeitet mit Rollen.
ABAC arbeitet mit Eigenschaften.

Tenant und Mandantentrennung

Ein Tenant ist ein logisch getrennter Verwaltungsbereich.

Mandantentrennung bedeutet:

Daten und Ressourcen verschiedener Kunden oder Organisationseinheiten werden logisch getrennt.

Merksatz:

Tenant = eigener Cloud-Verwaltungsbereich.

SSO, SAML, OAuth 2.0 und OpenID Connect

SSO:

einmal anmelden,
mehrere Dienste nutzen

SAML:

häufig für Single Sign-On genutzt

OAuth 2.0:

delegierte Autorisierung

OpenID Connect:

ergänzt OAuth 2.0 um Authentifizierung

Merksatz:

OAuth 2.0 ist Autorisierung.
OpenID Connect ergänzt Authentifizierung.

Verschlüsselung

Cloud-Daten sollten geschützt werden:

bei Übertragung

und

im Ruhezustand

Bei Übertragung:

```
TLS
```

Im Ruhezustand:

```
Speicherverschlüsselung
Datenbankverschlüsselung
Backup-Verschlüsselung
```

Merksatz:

```
Verschlüsselung schützt Daten,
ersetzt aber keine Rechteverwaltung.
```

KMS

KMS steht für:

```
Key Management Service
```

Ein KMS verwaltet kryptografische Schlüssel.

Aufgaben:

```
Schlüssel erzeugen
Schlüssel speichern
Schlüssel rotieren
Zugriff steuern
Nutzung protokollieren
Schlüssel deaktivieren
```

Merksatz:

```
KMS verwaltet Schlüssel für Cloud-Verschlüsselung.
```

Logging und Monitoring

Monitoring:

```
zeigt aktuelle Zustände und Messwerte
```

Logging:

```
zeigt Ereignisse und Änderungen
```

Beispiele für Logs:

```
Audit-Logs
Flow Logs
Firewall-Logs
Anwendungslogs
IAM-Logs
Load-Balancer-Logs
```

Merksatz:

```
Monitoring zeigt Zustand.
Logging zeigt Ereignisse.
```

SIEM

SIEM steht für:

```
Security Information and Event Management
```

Ein SIEM sammelt und analysiert Sicherheitslogs.

Ziele:

```
Angriffe erkennen
Alarme erzeugen
Ereignisse korrelieren
Nachweise liefern
```

Merksatz:

SIEM hilft bei zentraler Sicherheitsüberwachung.

Kostenkontrolle

Cloud-Kosten entstehen durch:

Rechenleistung
Speicher
Datenbanken
Backups
Snapshots
Logs
Monitoring
Netzwerkverkehr
Load Balancer
Lizenzen
öffentliche IP-Adressen
Support

Merksatz:

Cloud-Kosten entstehen nicht nur durch Server.

Pay as you go

Pay as you go bedeutet:

Abrechnung nach Nutzung.

Vorteil:

flexibel

Risiko:

Fehlkonfiguration,
Dauerbetrieb
oder unerwartete Last können teuer werden.

Merksatz:

Pay as you go braucht Kostenüberwachung.

Tagging

Tagging bedeutet:

Cloud-Ressourcen werden mit Metadaten markiert.

Beispiele:

Projekt
Kostenstelle
Verantwortlicher
Umgebung
Ablaufdatum
Schutzbedarf

Merksatz:

Tags helfen bei Kosten,
Verantwortung
Ordnung
und Automatisierung.

Rightsizing

Rightsizing bedeutet:

Ressourcen passend dimensionieren.

Zu groß:

unnötige Kosten

Zu klein:

schlechte Leistung oder Ausfälle

Merksatz:

Rightsizing sucht die passende Ressourcengröße.

Auto Scaling

Auto Scaling passt Ressourcen automatisch an die Last an.

Beispiel:

mehr Instanzen bei hoher Last

weniger Instanzen bei geringer Last

Merksatz:

Auto Scaling skaliert automatisch nach Regeln.

Horizontale und vertikale Skalierung

Skalierung	Bedeutung
horizontal	mehr Instanzen
vertikal	größere Instanz

Merksatz:

Horizontal = mehr Systeme.
Vertikal = stärkeres System.

Hochverfügbarkeit

Hochverfügbarkeit bedeutet:

Dienste bleiben möglichst verfügbar,
auch wenn einzelne Komponenten ausfallen.

Mittel:

mehrere Instanzen
mehrere Verfügbarkeitszonen
Load Balancer
Replikation
Monitoring
Auto Scaling
Backup
Notfallplan

Merksatz:

Cloud ist nicht automatisch hochverfügbar.

Region und Verfügbarkeitszone

Region:

geografischer Standort des Cloud-Anbieters

Verfügbarkeitszone:

getrenntes Rechenzentrumssegment innerhalb einer Region

Merksatz:

Region beeinflusst Datenstandort und Latenz.
Zone beeinflusst Ausfallsicherheit innerhalb einer Region.

SLA, SLO und SLI

Begriff	Bedeutung
SLA	vertragliche Servicezusage
SLO	Zielwert für Servicequalität
SLI	Messwert für Servicequalität

Merksatz:

```
SLI misst.
SLO setzt Ziel.
SLA ist Zusage.
```

Infrastructure as Code

Infrastructure as Code wird abgekürzt:

```
IaC
```

Dabei wird Infrastruktur als Code beschrieben.

Beispiele:

```
Netzwerke
Subnetze
Firewalls
Rollen
VMs
Datenbanken
Load Balancer
Speicher
```

Vorteile:

```
wiederholbar
versionierbar
dokumentiert
automatisierbar
prüfbar
```

Merksatz:

IaC beschreibt Infrastruktur als Code.

Configuration Drift

Configuration Drift bedeutet:

Die echte Konfiguration weicht von der geplanten Konfiguration ab.

Ursachen:

manuelle Änderungen
Notfalländerungen
fehlende Dokumentation
unterschiedliche Umgebungen

Merksatz:

Configuration Drift erschwert Betrieb und Sicherheit.

Change Management und Rollback

Change Management bedeutet:

Änderungen werden geplant,
geprüft,
freigegeben,
umgesetzt
und dokumentiert.

Rollback bedeutet:

Änderung zurücknehmen.

Merksatz:

```
Jede kritische Änderung braucht Dokumentation und Rückweg.
```

Runbook

Ein Runbook ist eine Schritt-für-Schritt-Anleitung für Betriebsaufgaben.

Beispiele:

```
Backup wiederherstellen
Alarm bearbeiten
Zertifikat erneuern
Dienst neu starten
Failover auslösen
Benutzerzugriff prüfen
```

Merksatz:

```
Runbooks helfen bei wiederholbaren Betriebsabläufen.
```

Incident Response

Incident Response bedeutet:

```
Vorgehen bei Sicherheitsvorfällen oder größeren Störungen.
```

Schritte:

```
erkennen
bewerten
eindämmen
beseitigen
wiederherstellen
dokumentieren
verbessern
```

Merksatz:

Incident Response muss vor dem Vorfall vorbereitet sein.

Datenschutz und Compliance

Cloud-Nutzung muss rechtliche und organisatorische Vorgaben beachten.

Wichtige Fragen:

Welche Daten werden verarbeitet?
Wo werden Daten gespeichert?
Wer hat Zugriff?
Gibt es Auftragsverarbeitung?
Sind Daten verschlüsselt?
Gibt es Löschkonzepte?
Werden Logs personenbezogen?
Welche Verträge gelten?

Merksatz:

Cloud braucht Datenschutz- und Compliance-Prüfung.

Datenklassifizierung

Datenklassifizierung bedeutet:

Daten werden nach Schutzbedarf eingeteilt.

Beispiele:

öffentlich
intern
vertraulich
streng vertraulich
personenbezogen
geschäftskritisch

Merksatz:

Datenklasse bestimmt Schutzmaßnahmen.

Datenresidenz

Datenresidenz bedeutet:

Daten müssen in einem bestimmten Land oder einer bestimmten Region gespeichert werden.

Beispiel:

Speicherung innerhalb der EU

Merksatz:

Datenresidenz beschreibt,
wo Daten liegen dürfen.

Vendor Lock-in

Vendor Lock-in bedeutet:

starke Abhängigkeit von einem Anbieter.

Ursachen:

proprietäre Dienste
spezielle APIs
spezielle Datenformate
hohe Migrationskosten
fehlende Portabilität
Mitarbeitende kennen nur eine Plattform

Merksatz:

Vendor Lock-in früh beachten.

Exit-Strategie

Eine Exit-Strategie beschreibt, wie man einen Cloud-Dienst wieder verlassen kann.

Fragen:

```
Wie exportiere ich Daten?
In welchem Format?
Wie lange dauert Migration?
Welche Kosten entstehen?
Wie werden Daten beim Anbieter gelöscht?
Gibt es Alternativen?
```

Merksatz:

```
Cloud-Einstieg braucht auch Cloud-Ausstiegsplan.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was bedeutet Cloud Computing?
- Was ist On-Premises?
- Was ist Public Cloud?
- Was ist Private Cloud?
- Was ist Hybrid Cloud?
- Was ist Multi Cloud?
- Was ist der Unterschied zwischen Hybrid Cloud und Multi Cloud?
- Was bedeutet IaaS?
- Was bedeutet PaaS?
- Was bedeutet SaaS?
- Was ist das Shared Responsibility Model?
- Wer ist bei IaaS für Betriebssystemupdates verantwortlich?
- Wer verwaltet bei SaaS Benutzer und Rechte?
- Was ist eine VPC?
- Was ist ein Public Subnet?
- Was ist ein Private Subnet?
- Was ist eine Security Group?
- Was ist ein Load Balancer?
```

- Was ist IAM?
- Was bedeutet Least Privilege?
- Was ist MFA?
- Was ist ein API-Schlüssel?
- Was ist ein Secret?
- Was ist Objektspeicher?
- Was ist Blockspeicher?
- Was ist Dateispeicher?
- Warum ist Cloud-Speicher kein Backup?
- Was bedeutet RPO?
- Was bedeutet RTO?
- Was ist Auto Scaling?
- Was ist horizontale Skalierung?
- Was ist vertikale Skalierung?
- Was ist ein SLA?
- Warum ist Cloud nicht automatisch sicher?
- Warum ist Cloud nicht automatisch günstiger?

Typische Prüfungsfallen

Cloud ist nicht automatisch günstiger.

Cloud ist nicht automatisch sicher.

Cloud ist nicht automatisch hochverfügbar.

Cloud ist nicht automatisch Backup.

Anbieter übernimmt nicht automatisch alles.

Daten,
Benutzer
und Rechte bleiben Kundenthema.

Public Cloud ist nicht automatisch unsicher.

Private Cloud ist nicht automatisch günstiger.

Hybrid Cloud ist nicht Multi Cloud.

Multi Cloud ist nicht automatisch Hybrid.

Virtualisierung allein ist keine Private Cloud.

IaaS ist Infrastruktur.

PaaS ist Plattform.

SaaS ist fertige Software.

Cloud-VM muss Kunde oft selbst patchen.

SaaS-Rechte bleiben Kundenthema.

Serverless heißt nicht serverfrei.

VPC und VNet sind virtuelle Cloud-Netze.

Public Subnet nicht für Datenbanken nutzen.

Private Subnet schützt vor direkter öffentlicher Erreichbarkeit.

Security Group ist virtuelle Firewall.

Öffentliche Buckets vermeiden.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Snapshot ist nicht immer Backup.

Backup ohne Restore-Test ist unsicher.

RPO und RTO nicht verwechseln.

IAM ist zentral für Cloud-Sicherheit.

Authentifizierung ist nicht Autorisierung.

MFA für Admins ist wichtig.

API-Schlüssel wie Passwörter behandeln.

Secrets nicht im Code speichern.

Verschlüsselung ersetzt keine Rechteverwaltung.

Monitoring und Logging unterscheiden.

Pay as you go braucht Kostenkontrolle.

Tags helfen bei Kosten und Verantwortung.

Horizontal und vertikal unterscheiden.

SLA,
SLO
und SLI nicht verwechseln.

Exit-Strategie früh planen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Cloud	IT-Ressourcen als Dienst
On-Premises	lokal selbst betrieben
Public Cloud	Anbieterplattform für viele Kunden
Private Cloud	Cloud für eine Organisation
Hybrid Cloud	lokale/private IT plus Cloud
Multi Cloud	mehrere Cloud-Anbieter
Community Cloud	Cloud für bestimmte Gemeinschaft
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
Shared Responsibility	geteilte Verantwortung

Begriff	Kurze Erklärung
Virtualisierung	Aufteilung physischer Ressourcen
Container	portable Anwendungseinheit
Kubernetes	Container-Orchestrierung
Serverless	keine Serververwaltung durch Kunden
FaaS	Function as a Service
VPC	Virtual Private Cloud
VNet	Virtual Network
Public Subnet	öffentlich angebundenes Subnetz
Private Subnet	internes Subnetz
Security Group	virtuelle Firewall-Regelgruppe
Load Balancer	verteilt Anfragen
Health Check	prüft Dienstgesundheit
Peering	Verbindung zwischen Cloud-Netzen
Cloud-VPN	VPN zu Cloud-Netz
Objektspeicher	Speicher für Objekte
Bucket	Speicherbehälter
Blockspeicher	virtuelle Festplatte
Dateispeicher	Datei- und Ordnerfreigabe
Backup	zusätzliche Sicherung
Restore	Wiederherstellung
RPO	maximaler Datenverlust
RTO	maximale Wiederherstellungszeit
Immutable Backup	unveränderliches Backup
IAM	Identity and Access Management
MFA	Multi-Faktor-Authentifizierung
Least Privilege	minimale notwendige Rechte
API-Schlüssel	Zugriffsschlüssel für Programme
Secret	geheime Information
RBAC	rollenbasierte Zugriffskontrolle
ABAC	attributbasierte Zugriffskontrolle
Tenant	Cloud-Verwaltungsbereich
SSO	Single Sign-On

Begriff	Kurze Erklärung
OAuth 2.0	delegierte Autorisierung
OpenID Connect	Authentifizierungserweiterung
KMS	Key Management Service
Monitoring	Zustandsüberwachung
Logging	Ereignisprotokollierung
SIEM	Sicherheitslog-Auswertung
Pay as you go	Abrechnung nach Nutzung
Tagging	Metadaten für Ressourcen
Rightsizing	passende Ressourcengröße
Auto Scaling	automatische Skalierung
SLA	vertragliche Servicezusage
SLO	Serviceziel
SLI	Servicemesswert
IaC	Infrastructure as Code
Configuration Drift	Abweichung von Soll-Konfiguration
Runbook	Betriebsanleitung
Incident Response	Reaktion auf Vorfälle
Compliance	Einhaltung von Vorgaben
Datenresidenz	erlaubter Speicherort
Vendor Lock-in	Anbieterabhängigkeit
Exit-Strategie	Plan zum Verlassen eines Dienstes

IHK-sichere Gesamtformulierung

Cloud Computing bedeutet, dass IT-Ressourcen wie Rechenleistung, Speicher, Netzwerke, Plattformen oder Anwendungen über ein Netzwerk als Dienst bereitgestellt werden. Bei On-Premises betreibt ein Unternehmen seine IT lokal selbst. Public Cloud wird von einem Anbieter für viele Kunden bereitgestellt, Private Cloud für eine einzelne Organisation, Hybrid Cloud kombiniert lokale oder private IT mit Public Cloud, und Multi Cloud nutzt mehrere Cloud-Anbieter. Die wichtigsten Service-Modelle sind IaaS, PaaS und SaaS. Das Shared Responsibility Model beschreibt die geteilte Verantwortung zwischen Anbieter und Kunde. Auch in der Cloud bleiben Benutzer, Rechte, Daten, sichere Konfiguration, Backup, Monitoring, Kostenkontrolle, Datenschutz und Compliance wichtige Aufgaben des Kunden.

Wichtigste Merksätze

Cloud = IT-Ressourcen als Dienst.

Cloud ist kein einzelnes Produkt.

Cloud ist nicht automatisch sicher.

Cloud ist nicht automatisch günstig.

Cloud ist nicht automatisch hochverfügbar.

Cloud ist kein Backup.

On-Premises = lokal selbst betrieben.

Public Cloud = Anbieterplattform für viele Kunden.

Private Cloud = Cloud für eine Organisation.

Hybrid Cloud = lokal plus Cloud.

Multi Cloud = mehrere Anbieter.

IaaS = Infrastruktur.

PaaS = Plattform.

SaaS = fertige Software.

Shared Responsibility = geteilte Verantwortung.

Daten bleiben Kundenthema.

Benutzer bleiben Kundenthema.

Rechte bleiben Kundenthema.

Cloud-VM muss Kunde oft selbst patchen.

SaaS braucht Rechteverwaltung.

Serverless heißt keine Serververwaltung durch Kunden.

VPC und VNet sind virtuelle Cloud-Netze.

Public Subnet nur für öffentliche Komponenten.

Private Subnet für interne Ressourcen.

Datenbanken nicht öffentlich bereitstellen.

Security Groups sind virtuelle Firewall-Regeln.

Cloud-VPN braucht Routen beidseitig.

Objektspeicher für unstrukturierte Daten.

Blockspeicher für VMs und Datenbanken.

Dateispeicher für Freigaben.

Öffentliche Buckets vermeiden.

Backup regelmäßig testen.

RPO = Datenverlust.

RTO = Wiederherstellungszeit.

IAM entscheidet,
wer was darf.

MFA für Admins erzwingen.

Least Privilege immer beachten.

API-Schlüssel schützen.

Secrets sicher verwalten.

Verschlüsselung ersetzt keine Rechte.

Monitoring zeigt Zustand.

Logging zeigt Ereignisse.

Kosten aktiv überwachen.

Tags pflegen.

Auto Scaling braucht Regeln.

Horizontal = mehr Instanzen.

Vertikal = größere Instanz.

IaC macht Infrastruktur wiederholbar.

Configuration Drift vermeiden.

Runbooks helfen im Betrieb.

Incident Response vorbereiten.

Datenschutz und Compliance prüfen.

Exit-Strategie früh planen.