

15.3 Public Cloud, Private Cloud, Hybrid Cloud und Multi Cloud

Cloud kann unterschiedlich bereitgestellt werden.

Die wichtigsten Cloud-Bereitstellungsmodelle sind:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Multi Cloud
- Community Cloud

Diese Modelle beschreiben, wo die Cloud betrieben wird, wer sie nutzt und wie stark sie vom Unternehmen selbst kontrolliert wird.

Merksatz:

Service-Modelle beschreiben,
was bereitgestellt wird.
Bereitstellungsmodelle beschreiben,
wo und für wen es bereitgestellt wird.

Warum Bereitstellungsmodelle wichtig sind

Nicht jede Cloud ist gleich aufgebaut.

Ein Unternehmen muss entscheiden:

Sollen Dienste beim öffentlichen Anbieter laufen?
Sollen sensible Systeme intern bleiben?
Sollen lokale Systeme mit Cloud verbunden werden?
Sollen mehrere Anbieter genutzt werden?
Gibt es Datenschutz- oder Compliance-Anforderungen?
Wie wichtig sind Kontrolle,
Kosten,
Skalierung
und Verfügbarkeit?

Merksatz:

Das passende Cloud-Modell hängt von Technik,
Sicherheit,
Kosten
und Anforderungen ab.

Public Cloud

Public Cloud bedeutet:

Ein Cloud-Anbieter stellt Ressourcen für viele Kunden bereit.

Die Kunden nutzen dieselbe Anbieterplattform, sind aber logisch voneinander getrennt.

Typische Ressourcen:

virtuelle Maschinen
Speicher
Datenbanken
Webdienste
Containerdienste
KI-Dienste
Identitätsdienste
Monitoring
Backup
SaaS-Anwendungen

Merksatz:

Public Cloud ist Cloud beim öffentlichen Anbieter für viele Kunden.

Public Cloud einfach erklärt

Beispiel:

Ein Unternehmen mietet virtuelle Server bei einem Cloud-Anbieter.

Die Server laufen nicht im eigenen Serverraum, sondern im Rechenzentrum des Anbieters.

Das Unternehmen verwaltet seine Ressourcen über:

Webportal
API
Kommandozeile
Automatisierung
Infrastructure as Code

Merksatz:

Public Cloud wird über Anbieterplattformen bereitgestellt und verwaltet.

Typische Public-Cloud-Eigenschaften

Typische Eigenschaften:

schnelle Bereitstellung
hohe Skalierbarkeit
nutzungsabhängige Abrechnung
große Auswahl an Diensten
weltweite Regionen
standardisierte Plattform
Self-Service
API-Steuerung
viele Automatisierungsmöglichkeiten

Merksatz:

Public Cloud ist schnell,
flexibel
und dienstorientiert.

Public Cloud: Vorteile

Vorteile:

- keine eigene Hardwarebeschaffung
- schnelle Bereitstellung
- flexible Skalierung
- viele fertige Dienste
- weltweite Verfügbarkeit
- nutzungsabhängige Kosten
- moderne Sicherheitsfunktionen
- Automatisierung gut möglich
- geeignet für wechselnde Last

Merksatz:

Public Cloud bietet Flexibilität und schnelle Bereitstellung.

Public Cloud: Nachteile

Nachteile:

- Abhängigkeit vom Anbieter
- laufende Kosten können unübersichtlich werden
- Datenschutz und Datenstandort prüfen
- Internetabhängigkeit
- weniger Kontrolle über physische Infrastruktur
- Fehlkonfigurationen möglich
- Anbieteränderungen können Auswirkungen haben
- Know-how für sichere Nutzung nötig

Merksatz:

Public Cloud braucht Kostenkontrolle,
Sicherheitskonzept
und klare Verantwortlichkeiten.

Public Cloud und Mandantentrennung

In der Public Cloud nutzen viele Kunden dieselbe Plattform.

Damit Kunden getrennt bleiben, gibt es Mandantentrennung.

Mandantentrennung bedeutet:

Ressourcen eines Kunden sind logisch von anderen Kunden getrennt.

Beispiele:

eigene Benutzerverwaltung
eigene virtuelle Netzwerke
eigene Speicherbereiche
eigene Zugriffsrechte
eigene Abrechnung

Merksatz:

Public Cloud ist gemeinsam genutzt,
aber logisch getrennt.

Private Cloud

Private Cloud bedeutet:

Cloud-Prinzipien werden für eine einzelne Organisation bereitgestellt.

Sie kann betrieben werden:

im eigenen Rechenzentrum
bei einem Dienstleister
in einer dedizierten Umgebung

Wichtig:

Die Plattform wird nicht allgemein von vielen unabhängigen Kunden geteilt,
sondern ist für eine Organisation bestimmt.

Merksatz:

Private Cloud ist Cloud für eine Organisation.

Private Cloud einfach erklärt

Beispiel:

Ein Unternehmen betreibt im eigenen Rechenzentrum eine virtualisierte Plattform.

Fachbereiche können dort selbst Ressourcen anfordern:

virtuelle Maschinen

Speicher

Netzwerke

Datenbanken

Testumgebungen

Die Bereitstellung erfolgt automatisiert und zentral verwaltet.

Merksatz:

Private Cloud nutzt Cloud-Prinzipien,
aber in kontrollierter Umgebung.

Typische Private-Cloud-Eigenschaften

Typische Eigenschaften:

mehr Kontrolle

dedizierte Umgebung

interne Sicherheitsvorgaben

eigene Netzstruktur

eigene Compliance-Vorgaben

Automatisierung

Self-Service

Ressourcenpools

interne Verrechnung möglich

Merksatz:

Private Cloud verbindet Cloud-Funktionen mit stärkerer Kontrolle.

Private Cloud: Vorteile

Vorteile:

- hohe Kontrolle über Umgebung
- besser an interne Vorgaben anpassbar
- Daten können im eigenen Betrieb bleiben
- eigene Sicherheitsarchitektur möglich
- geeignet für sensible Systeme
- Integration in bestehende Infrastruktur
- weniger Abhängigkeit von Public-Cloud-Anbieter

Merksatz:

Private Cloud ist interessant,
wenn Kontrolle und Anpassung wichtig sind.

Private Cloud: Nachteile

Nachteile:

- eigene Hardware oder Dienstleister nötig
- höhere Betriebsverantwortung
- Skalierung begrenzter als Public Cloud
- Investitionskosten möglich
- eigenes Fachwissen nötig
- Wartung bleibt stärker beim Unternehmen
- Verfügbarkeit muss selbst geplant werden

Merksatz:

Private Cloud gibt Kontrolle,
aber auch mehr Betriebsaufwand.

Private Cloud ist nicht automatisch Cloud

Nur weil Server virtualisiert sind, ist es noch nicht automatisch eine Private Cloud.

Cloud-typische Merkmale sind zum Beispiel:

Self-Service
Automatisierung
Ressourcenpooling
schnelle Bereitstellung
messbare Nutzung
standardisierte Dienste
zentrale Verwaltung

Merksatz:

Virtualisierung allein ist noch keine vollständige Private Cloud.

Public Cloud und Private Cloud vergleichen

Merkmal	Public Cloud	Private Cloud
Betreiber	öffentlicher Anbieter	Unternehmen oder Dienstleister
Nutzerkreis	viele Kunden	eine Organisation
Kontrolle	geringer über physische Basis	höher
Skalierung	sehr hoch	abhängig von eigener Kapazität
Kostenmodell	oft nutzungsabhängig	oft Investition plus Betrieb
Anpassbarkeit	begrenzt durch Anbieter	höher
Datenstandort	Anbieterregion wählen	stärker selbst bestimmbar

Merksatz:

Public Cloud ist flexibler skalierbar.
Private Cloud ist stärker kontrollierbar.

Hybrid Cloud

Hybrid Cloud bedeutet:

Lokale IT oder Private Cloud wird mit Public Cloud kombiniert.

Beispiele:

internes Rechenzentrum
plus
Public-Cloud-Dienste

Oder:

Private Cloud
plus
Public Cloud

Merksatz:

Hybrid Cloud kombiniert lokale oder private IT mit Public Cloud.

Hybrid Cloud einfach erklärt

Beispiel:

Kundendatenbank läuft lokal.

Webfrontend läuft in der Public Cloud.

Backup wird zusätzlich in der Cloud gespeichert.

Verbindung erfolgt über VPN oder dedizierte Leitung.

So nutzt das Unternehmen lokale Kontrolle und Cloud-Flexibilität gleichzeitig.

Merksatz:

Hybrid Cloud verbindet zwei Welten.

Typische Hybrid-Cloud-Szenarien

Typische Szenarien:

- lokales Active Directory mit Cloud-Diensten verbinden
- lokale Server mit Cloud-Backup sichern
- Cloud-Webanwendung greift auf lokale Datenbank zu
- lokale Anwendung nutzt Cloud-Speicher
- Cloud als Ausweichstandort
- schrittweise Migration in die Cloud
- Lastspitzen in Cloud auslagern
- sensible Daten lokal,
- skalierbare Dienste in Cloud

Merksatz:

Hybrid Cloud wird oft für schrittweise Migration und flexible Erweiterung genutzt.

Hybrid Cloud: Vorteile

Vorteile:

- Kombination aus Kontrolle und Skalierung
- schrittweise Migration möglich
- sensible Systeme können lokal bleiben
- Cloud-Dienste ergänzen lokale IT
- Backup und Notfallkonzepte möglich
- flexible Lastverteilung
- bestehende Investitionen weiter nutzbar

Merksatz:

Hybrid Cloud ermöglicht Übergang und Kombination.

Hybrid Cloud: Nachteile

Nachteile:

- höhere Komplexität
- Netzwerkanbindung muss stabil sein
- VPN oder Direktverbindung nötig

Identitätsmanagement muss zusammenpassen
Monitoring über mehrere Umgebungen nötig
Sicherheitsregeln müssen abgestimmt werden
Datenflüsse müssen dokumentiert werden
Fehlersuche wird komplexer

Merksatz:

Hybrid Cloud ist flexibel,
aber technisch anspruchsvoller.

Hybrid Cloud und Netzwerk

Hybrid Cloud braucht eine sichere Verbindung zwischen Umgebungen.

Möglichkeiten:

Site-to-Site-VPN
dedizierte Leitung
Cloud-VPN
SD-WAN
private Verbindung zum Anbieter

Wichtig:

Routing
DNS
Firewall-Regeln
Latenz
Bandbreite
Verschlüsselung
Redundanz

Merksatz:

Hybrid Cloud steht und fällt mit sauberer Netzwerkanbindung.

Hybrid Cloud und Identitäten

Benutzer sollen oft sowohl lokale als auch Cloud-Dienste nutzen.

Dafür braucht man ein Identitätskonzept.

Beispiele:

- lokale Benutzerverwaltung
- Cloud-Verzeichnisdienst
- Synchronisierung
- Single Sign-On
- MFA
- Rollen
- Conditional Access

Merksatz:

Hybrid Cloud braucht einheitliche Identitäten und Zugriffskonzepte.

Hybrid Cloud und Datenflüsse

Bei Hybrid Cloud muss klar sein:

- Welche Daten liegen lokal?
- Welche Daten liegen in der Cloud?
- Welche Daten werden übertragen?
- Wer darf zugreifen?
- Wo werden Backups gespeichert?
- Welche Systeme kommunizieren miteinander?
- Welche Schnittstellen gibt es?

Merksatz:

Hybrid Cloud braucht dokumentierte Datenflüsse.

Multi Cloud

Multi Cloud bedeutet:

Ein Unternehmen nutzt mehrere Cloud-Anbieter gleichzeitig.

Beispiel:

Anbieter A für virtuelle Server

Anbieter B für E-Mail und Office

Anbieter C für Backup

Anbieter D für KI- oder Datenanalyse

Merksatz:

Multi Cloud bedeutet mehrere Cloud-Anbieter parallel.

Multi Cloud ist nicht dasselbe wie Hybrid Cloud

Hybrid Cloud:

Kombination aus lokaler IT und Cloud

Multi Cloud:

Nutzung mehrerer Cloud-Anbieter

Beispiel:

Nur Anbieter A und Anbieter B,
ohne lokale Systeme:
Multi Cloud,
aber nicht zwingend Hybrid Cloud.

Merksatz:

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

Multi Cloud: Vorteile

Vorteile:

weniger Abhängigkeit von einem Anbieter
passende Dienste je Anbieter nutzbar
bessere Verhandlungsposition möglich
Ausweichmöglichkeiten
regulatorische oder regionale Anforderungen leichter erfüllbar
Spezialdienste verschiedener Anbieter nutzbar

Merksatz:

Multi Cloud kann Anbieterabhängigkeit verringern.

Multi Cloud: Nachteile

Nachteile:

höhere Komplexität
unterschiedliche Bedienkonzepte
unterschiedliche Sicherheitsmodelle
mehrere IAM-Systeme
schwierigeres Monitoring
höhere Anforderungen an Know-how
Kostenkontrolle komplizierter
Datenübertragung zwischen Anbietern kann teuer sein

Merksatz:

Multi Cloud reduziert Abhängigkeit,
erhöht aber Komplexität.

Multi Cloud und Vendor Lock-in

Vendor Lock-in bedeutet:

Ein Unternehmen wird stark abhängig von einem Anbieter.

Ursachen:

proprietäre Dienste
spezielle APIs
spezielle Datenformate
komplexe Migration
hohe Ausstiegskosten
Mitarbeitende kennen nur eine Plattform

Multi Cloud kann Vendor Lock-in verringern, aber nicht automatisch verhindern.

Merksatz:

Vendor Lock-in bedeutet starke Anbieterabhängigkeit.

Multi Cloud und Portabilität

Portabilität bedeutet:

Anwendungen oder Daten können leichter zwischen Umgebungen verschoben werden.

Möglichkeiten:

Container
offene Standards
standardisierte APIs
Infrastructure as Code
portable Datenformate
automatisierte Deployments

Aber:

vollständig einfache Portabilität ist selten.

Merksatz:

Portabilität muss geplant werden.

Community Cloud

Community Cloud bedeutet:

Eine Cloud wird von mehreren Organisationen mit ähnlichen Anforderungen genutzt.

Beispiele:

Behörden
Forschung
Bildung
Gesundheitswesen
bestimmte Branchen
Verbände

Gemeinsam sind oft:

Sicherheitsanforderungen
Datenschutzvorgaben
Compliance-Regeln
fachliche Anforderungen

Merksatz:

Community Cloud ist Cloud für eine bestimmte Gemeinschaft.

Community Cloud: Vorteile

Vorteile:

gemeinsame Anforderungen können besser berücksichtigt werden
branchenspezifische Vorgaben möglich
Kosten können geteilt werden
gemeinsame Standards
spezielle Sicherheits- und Compliance-Anforderungen

Merksatz:

Community Cloud bündelt ähnliche Anforderungen mehrerer Organisationen.

Community Cloud: Nachteile

Nachteile:

weniger flexibel als Public Cloud
begrenzter Nutzerkreis
Abstimmung zwischen Organisationen nötig
Governance komplexer
Angebot möglicherweise kleiner
Verantwortlichkeiten müssen klar geregelt sein

Merksatz:

Community Cloud braucht klare gemeinsame Regeln.

Cloud-Modelle im Vergleich

Modell	Kerngedanke
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:

Jedes Modell löst andere Anforderungen.

Typische Entscheidungskriterien

Wichtige Kriterien:

Datenschutz
Datenstandort
Kosten
Skalierbarkeit
Kontrolle
Verfügbarkeit
Compliance
Latenz
vorhandene Systeme
Know-how
Sicherheitsanforderungen
Anbieterabhängigkeit
Integrationsaufwand

Merksatz:

Cloud-Modell nach Anforderungen auswählen,
nicht nach Modewort.

Datenstandort

Datenstandort bedeutet:

Wo werden Daten gespeichert und verarbeitet?

Wichtig für:

Datenschutz
rechtliche Anforderungen
Kundenanforderungen
Latenz

Compliance
Vertragsbedingungen

Beispiel:

Daten müssen innerhalb der EU gespeichert werden.

Merksatz:

Datenstandort ist bei Cloud-Auswahl entscheidend.

Compliance

Compliance bedeutet:

Einhaltung von Regeln,
Gesetzen,
Standards
und internen Vorgaben.

Bei Cloud relevant:

Datenschutz
Informationssicherheit
Branchenvorgaben
Auditierbarkeit
Aufbewahrungsfristen
Löschkonzepte
Zugriffsnachweise
Vertragsanforderungen

Merksatz:

Cloud muss zu rechtlichen und organisatorischen Vorgaben passen.

Cloud und Latenz

Latenz ist die Verzögerung bei der Datenübertragung.

Sie ist wichtig bei:

- Echtzeitanwendungen
- Datenbankzugriffen
- Remote Desktop
- VoIP
- Produktionssystemen
- verteilten Anwendungen

Ein weit entfernter Cloud-Standort kann höhere Latenz verursachen.

Merksatz:

Cloud-Region beeinflusst Latenz.

Cloud und Bandbreite

Cloud-Dienste brauchen passende Bandbreite.

Relevant bei:

- Backups
- Dateiübertragung
- Videodaten
- Datenbankreplikation
- Migration
- Synchronisation
- Hybrid-Cloud-Anbindung

Merksatz:

Cloud-Nutzung kann viel Netzwerkverkehr erzeugen.

Cloud und Datenübertragungskosten

Bei Cloud können Datenübertragungen Kosten verursachen.

Besonders wichtig:

- ausgehender Datenverkehr aus der Cloud
- Daten zwischen Regionen
- Daten zwischen Anbietern
- große Backups
- Replikation
- Downloads durch Benutzer

Merksatz:

Cloud-Traffic kann Kosten verursachen.

Cloud und Verfügbarkeit

Cloud-Anbieter stellen viele Möglichkeiten für Verfügbarkeit bereit.

Aber:

Der Kunde muss sie nutzen und konfigurieren.

Beispiele:

- mehrere Zonen
- mehrere Regionen
- Load Balancer
- Replikation
- Backup
- Auto Scaling
- Monitoring

Merksatz:

Cloud bietet Möglichkeiten für Hochverfügbarkeit,
aber nicht automatisch fertige Hochverfügbarkeit.

Cloud und Ausfallsicherheit

Ausfallsicherheit bedeutet:

Ein Dienst bleibt trotz Störung nutzbar
oder kann schnell wiederhergestellt werden.

Wichtige Konzepte:

Redundanz
Backup
Wiederherstellung
Notfallplan
mehrere Zonen
mehrere Regionen
regelmäßige Tests

Merksatz:

Ausfallsicherheit muss geplant,
umgesetzt
und getestet werden.

Cloud und Verantwortung

Auch beim Bereitstellungsmodell gilt:

Verantwortung verschwindet nicht.

Der Kunde muss prüfen:

Wer betreibt was?
Wer sichert was?
Wer patcht was?
Wer darf zugreifen?
Wer überwacht?
Wer reagiert bei Störung?
Wer ist Ansprechpartner?
Was steht im Vertrag?

Merksatz:

Cloud-Verantwortung muss klar geregelt sein.

Cloud und Verträge

Cloud-Nutzung braucht klare vertragliche Regelungen.

Wichtige Punkte:

Leistungsumfang
Verfügbarkeit
Supportzeiten
Datenschutz
Datenstandort
Auftragsverarbeitung
Kündigung
Datenexport
Wiederherstellung
Sicherheitsmaßnahmen
Haftung

Merksatz:

Cloud ist auch ein organisatorisches und vertragliches Thema.

Service Level Agreement

Service Level Agreement wird abgekürzt:

SLA

Ein SLA beschreibt zugesicherte Serviceleistungen.

Beispiele:

Verfügbarkeit
Reaktionszeit

Wiederherstellungszeit

Supportzeit

Leistungswerte

Wichtig:

SLA genau lesen.

Hohe Prozentwerte bedeuten trotzdem mögliche Ausfallzeit.

Merksatz:

SLA beschreibt zugesicherte Servicequalität.

SLA und Verfügbarkeit

Verfügbarkeit wird oft in Prozent angegeben.

Beispiele:

Verfügbarkeit	grobe Bedeutung
99 %	deutlich mehr mögliche Ausfallzeit als 99,9 %
99,9 %	höher verfügbar
99,99 %	sehr hohe Verfügbarkeit
99,999 %	extrem hohe Verfügbarkeit

Wichtig:

Je höher die Verfügbarkeit,
desto aufwendiger und teurer ist sie meist.

Merksatz:

Mehr Neunen bedeuten weniger erlaubte Ausfallzeit,
aber meist mehr Aufwand.

Cloud und Exit-Strategie

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

Fragen:

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

Merksatz:

Cloud-Einstieg braucht auch Cloud-Ausstiegsplan.

Cloud und Datenportabilität

Datenportabilität bedeutet:

Daten können in ein anderes System oder zu einem anderen Anbieter übertragen werden.

Wichtig:

offene Formate
Exportfunktionen
dokumentierte Schnittstellen
keine unnötigen proprietären Abhängigkeiten
regelmäßige Exporttests

Merksatz:

Daten sollten nicht in einem Dienst gefangen sein.

Cloud und Schatten-IT

Schatten-IT bedeutet:

Fachbereiche nutzen IT-Dienste ohne Wissen oder Freigabe der IT-Abteilung.

Beispiele:

- private Cloud-Speicher
- nicht freigegebene SaaS-Tools
- eigene KI-Dienste
- externe Projektplattformen
- private Messenger

Risiken:

- Datenschutzprobleme
- Datenabfluss
- fehlende Backups
- keine Rechtekontrolle
- keine Löschung bei Austritt
- keine Vertragsprüfung

Merksatz:

Schatten-IT entsteht oft,
wenn offizielle Lösungen fehlen oder zu unpraktisch sind.

Cloud Governance

Cloud Governance beschreibt Regeln und Steuerung für Cloud-Nutzung.

Dazu gehören:

- wer darf Cloud-Ressourcen erstellen?
- welche Dienste sind erlaubt?
- welche Regionen sind erlaubt?
- welche Sicherheitsstandards gelten?
- wie werden Kosten überwacht?
- wie werden Daten klassifiziert?
- wie werden Zugriffe geprüft?
- wie werden Änderungen dokumentiert?

Merksatz:

Cloud Governance sorgt für kontrollierte Cloud-Nutzung.

Tagging

Tagging bedeutet:

Cloud-Ressourcen werden mit Schlagworten oder Metadaten markiert.

Beispiele:

Projekt
Kostenstelle
Verantwortlicher
Umgebung
Kritikalität
Ablaufdatum
Datenschutzklasse

Vorteile:

Kosten zuordnen
Ressourcen finden
Verantwortliche erkennen
Aufräumen erleichtern
Automatisierung ermöglichen

Merksatz:

Tags machen Cloud-Ressourcen verwaltbar.

Cloud-Kostenkontrolle

Kostenkontrolle ist wichtig, weil Cloud-Ressourcen schnell erstellt werden können.

Maßnahmen:

Budgets
Alarme
Tags
Kostenstellen
Rechtebegrenzung
Abschalten ungenutzter Ressourcen
passende Größen wählen
Reservierungen prüfen
Datenverkehr beobachten

Merksatz:

Cloud-Flexibilität braucht Kostenkontrolle.

Typische Cloud-Fehlentscheidungen

Häufige Fehler:

Cloud-Modell ohne Anforderungen auswählen
Datenschutz nicht prüfen
Kosten nicht überwachen
keine Exit-Strategie planen
kein Backup-Konzept erstellen
keine Rollen definieren
Ressourcen öffentlich freigeben
Multi Cloud ohne Know-how einführen
Hybrid Cloud ohne Netzplanung starten
SLA falsch verstehen

Merksatz:

Cloud muss geplant werden,
nicht nur gebucht.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist Public Cloud?
- Was ist Private Cloud?
- Was ist Hybrid Cloud?
- Was ist Multi Cloud?
- Was ist Community Cloud?
- Was ist der Unterschied zwischen Hybrid Cloud und Multi Cloud?
- Welche Vorteile hat Public Cloud?
- Welche Vorteile hat Private Cloud?
- Warum ist Hybrid Cloud komplexer?
- Was bedeutet Vendor Lock-in?
- Was bedeutet Datenstandort?
- Was ist ein SLA?
- Warum braucht Cloud eine Exit-Strategie?
- Was ist Cloud Governance?
- Warum ist Tagging sinnvoll?
- Warum ist Cloud-Kostenkontrolle wichtig?

Typische Prüfungsfallen

Public Cloud ist nicht automatisch unsicher.

Private Cloud ist nicht automatisch günstiger.

Hybrid Cloud ist nicht einfach nur irgendeine Cloud.

Multi Cloud ist nicht dasselbe wie Hybrid Cloud.

Community Cloud ist für bestimmte Organisationengruppen.

Virtualisierung allein ist noch keine Private Cloud.

Cloud ist nicht automatisch hochverfügbar.

Cloud ist nicht automatisch günstiger.

Datenstandort prüfen.

SLA genau lesen.

Hohe Verfügbarkeit muss konfiguriert werden.

Multi Cloud erhöht Komplexität.

Hybrid Cloud braucht gute Netzplanung.

Vendor Lock-in früh beachten.

Exit-Strategie vor dem Wechsel planen.

Schatten-IT ist ein Sicherheitsrisiko.

Governance verhindert unkontrollierte Cloud-Nutzung.

Tagging hilft bei Kosten und Verwaltung.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Public Cloud	Cloud-Plattform 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
Mandantentrennung	logische Trennung verschiedener Kunden
Vendor Lock-in	starke Anbieterabhängigkeit
Portabilität	Übertragbarkeit von Daten oder Anwendungen
Datenstandort	Ort der Speicherung und Verarbeitung
Compliance	Einhaltung von Regeln und Vorgaben
SLA	Service Level Agreement
Exit-Strategie	Plan zum Verlassen eines Dienstes
Datenportabilität	Daten in anderes System übertragen können
Schatten-IT	nicht offiziell freigegebene IT-Nutzung
Cloud Governance	Regeln für Cloud-Nutzung
Tagging	Metadaten für Ressourcen

Begriff	Kurze Erklärung
Kostenkontrolle	Überwachung und Steuerung von Cloud-Kosten
Verfügbarkeit	Dienst ist nutzbar
Ausfallsicherheit	Dienst bleibt trotz Störung verfügbar oder wird wiederhergestellt

IHK-sichere Kurzformulierung

Public Cloud bezeichnet Cloud-Dienste eines öffentlichen Anbieters, die von vielen Kunden genutzt werden, wobei die Kunden logisch voneinander getrennt sind. Private Cloud stellt Cloud-Funktionen für eine einzelne Organisation bereit und bietet mehr Kontrolle, aber auch mehr Betriebsverantwortung. Hybrid Cloud kombiniert lokale oder private IT mit Public Cloud, während Multi Cloud die Nutzung mehrerer Cloud-Anbieter beschreibt. Community Cloud wird von Organisationen mit gemeinsamen Anforderungen genutzt. Bei der Auswahl eines Cloud-Modells müssen Datenschutz, Datenstandort, Compliance, Kosten, Skalierbarkeit, Kontrolle, Verfügbarkeit, Latenz, Anbieterabhängigkeit und Exit-Strategie berücksichtigt werden.

Merksätze

Bereitstellungsmodell beschreibt,
wo und für wen Cloud läuft.

Public Cloud = Anbieterplattform für viele Kunden.

Private Cloud = Cloud für eine Organisation.

Hybrid Cloud = lokal oder privat plus Public Cloud.

Multi Cloud = mehrere Anbieter.

Community Cloud = gemeinsame Anforderungen.

Public Cloud ist flexibel.

Private Cloud gibt mehr Kontrolle.

Hybrid Cloud kombiniert Welten.

Multi Cloud reduziert Anbieterabhängigkeit,
erhöht aber Komplexität.

Hybrid ist nicht automatisch Multi Cloud.

Multi Cloud ist nicht automatisch Hybrid.

Virtualisierung allein ist keine Private Cloud.

Mandantentrennung trennt Kunden logisch.

Vendor Lock-in früh beachten.

Portabilität planen.

Datenstandort prüfen.

Compliance beachten.

Cloud-Region beeinflusst Latenz.

Cloud-Traffic kann Kosten verursachen.

Cloud ist nicht automatisch hochverfügbar.

Hochverfügbarkeit muss geplant werden.

SLA genau lesen.

Exit-Strategie vor Nutzung bedenken.

Datenportabilität ist wichtig.

Schatten-IT vermeiden.

Cloud Governance schafft Regeln.

Tagging hilft bei Verwaltung und Kosten.

Cloud-Kosten aktiv überwachen.

Cloud muss geplant werden,

nicht nur gebucht.
