

## AWS Certified Cloud Practitioner (CLF-C01) Prüfungsleitfaden

### Einführung

Die Prüfung „AWS Certified Cloud Practitioner (CLF-C01)“ richtet sich an Personen, die unabhängig von einer bestimmten Jobrolle effektiv ein umfassendes Wissen über die AWS Cloud nachweisen können.

Die Prüfung bestätigt die Fähigkeit eines Kandidaten, die folgenden Aufgaben zu erledigen:

- Erklären des Mehrwerts der AWS Cloud
- Verstehen und Erklären des AWS-Modells der geteilten Verantwortlichkeit
- Verstehen von bewährten Methoden im Bereich Sicherheit
- Verstehen der Kosten, Wirtschaftlichkeit und Abrechnungsmethoden der AWS Cloud
- Beschreiben und Positionieren der wichtigsten AWS-Services, einschließlich Datenverarbeitung, Netzwerk, Datenbanken und Speicher
- Identifizieren von AWS-Services für häufige Anwendungsfälle

### Beschreibung der Zielkandidaten

Der Zielkandidat sollte 6 Monate oder das Äquivalent an aktiver Interaktion mit der AWS Cloud haben, wobei der Schwerpunkt auf dem AWS Cloud-Design, der Implementierung und/oder dem Betrieb liegen sollte. Die Kandidaten zeigen ein Verständnis für gut gestaltete AWS Cloud-Lösungen.

#### Empfohlenes AWS-Wissen

Der Zielkandidat sollte folgende Kenntnisse haben:

- AWS Cloud-Konzepte
- Sicherheit und Compliance innerhalb der AWS Cloud
- Verständnis der wichtigsten AWS-Services
- Verständnis der Wirtschaftlichkeit der AWS Cloud

#### Was gilt als nicht relevant für den Zielkandidaten?

Es folgt eine nicht vollständige Liste der Jobaufgaben, die der Zielkandidat nicht ausführen muss. Diese Punkte kommen in der Prüfung nicht vor:

- Codierung
- Entwurf von Cloud-Architekturen
- Problembehandlung
- Implementierung
- Migration
- Last- und Leistungstests
- Geschäftsanwendungen (z. B. Amazon Alexa, Amazon Chime, Amazon WorkMail)

Eine detaillierte Liste spezifischer Tools und Technologien, die möglicherweise in der Prüfung behandelt werden, sowie Listen der relevanten AWS-Services finden Sie im Anhang.

# Inhalt der Prüfung

## Antwortarten

Es gibt zwei Arten von Fragen bei der Prüfung:

- **Multiple Choice:** beinhaltet eine richtige und drei falsche Antworten (Distraktoren)
- **Mehrfache Antwort:** beinhaltet zwei oder mehr korrekte Antworten aus fünf oder mehr Antwortoptionen

Wählen Sie eine oder mehrere Antworten aus, die die Aussage am besten beschreiben oder die Frage beantworten. Distraktoren oder falsche Antworten sind Antwortoptionen, für die sich ein Kandidat mit unvollständigem Wissen oder fehlenden Fähigkeiten entscheiden könnte. Distraktoren sind im Allgemeinen plausible Antworten, die zum Inhaltsbereich passen.

Unbeantwortete Fragen werden als falsch gewertet. Für Raten gibt es keine Strafe. Die Prüfung umfasst 50 Fragen, die sich auf Ihre Punktzahl auswirken.

## Nicht gewerteter Inhalt

Die Prüfung umfasst 15 nicht gewertete Fragen, die sich nicht auf Ihre Punktzahl auswirken. AWS sammelt mit diesen nicht gewerteten Fragen Informationen zur Bewerberleistung, um diese in Zukunft als bewertete Fragen zu verwenden. Diese nicht gewerteten Fragen werden in der Prüfung nicht identifiziert.

## Prüfungsergebnisse

Die AWS Certified Cloud Practitioner-Prüfung ist eine sogenannte Pass/Fail-Prüfung. Die Prüfung wird nach einem Mindeststandard bewertet, der von AWS-Experten festgelegt wurde, die die bewährten Methoden und Richtlinien der Zertifizierungsbranche befolgen.

Ihre Ergebnisse für die Prüfung werden als skalierte Punktzahl von 100 bis 1.000 angezeigt. Die minimale Punktzahl beträgt 700. Ihre Punktzahl zeigt, wie Sie die Prüfung insgesamt durchgeführt haben und ob Sie bestanden haben oder nicht. Skalierte Bewertungsmodelle helfen dabei, Ergebnisse mehrerer Prüfungsformen gleichzusetzen, die möglicherweise leicht unterschiedliche Schwierigkeitsgrade haben.

Ihr Bewertungsbericht kann eine Tabelle mit Klassifizierungen Ihrer Leistung auf jeder Abschnittsebene enthalten. Diese Informationen sollen allgemeines Feedback zu Ihrer Prüfungsleistung geben. Für die Prüfung wird ein kompensatorisches Bewertungsmodell verwendet, was bedeutet, dass Sie nicht in jedem Abschnitt die notwendige Punktzahl erreichen müssen. Sie müssen nur die Gesamtprüfung bestehen.

Jeder Abschnitt der Prüfung hat eine bestimmte Gewichtung, daher enthalten einige Abschnitte mehr Fragen als andere. Die Tabelle enthält allgemeine Informationen, die Ihre Stärken und Schwächen hervorheben. Bewerten Sie das Feedback auf Abschnittsebene mit Umsicht.

## Inhaltsgliederung

Dieser Prüfungsleitfaden enthält Gewichtungen, Testbereiche und Ziele für die Prüfung. Es handelt sich nicht um eine umfassende Auflistung der Prüfungsinhalte. Für jedes der Ziele steht jedoch zusätzlicher Kontext zur Verfügung, der Ihnen bei der Vorbereitung auf die Prüfung hilft. In der folgenden Tabelle sind die wichtigsten Inhaltsbereiche und ihre Gewichtung aufgeführt. Die Tabelle geht einer vollständigen Übersicht über den Prüfungsinhalt voraus, die den zusätzlichen Kontext enthält. Der Prozentsatz in jedem Bereich spiegelt nur die gewerteten Inhalte wider.

| Bereich                              | % der Prüfung |
|--------------------------------------|---------------|
| Bereich 1: Cloud-Konzepte            | 26 %          |
| Bereich 2: Sicherheit und Compliance | 25 %          |
| Bereich 3: Technologie               | 33 %          |
| Bereich 4: Abrechnung und Preise     | 16 %          |
| <b>GESAMT</b>                        | <b>100 %</b>  |

## Bereich 1: Cloud-Konzepte

### 1.1 Definieren der AWS Cloud und ihres Leistungsversprechens

- Definieren der Vorteile der AWS Cloud, einschließlich
  - Sicherheit
  - Zuverlässigkeit
  - Hochverfügbarkeit
  - Elastizität
  - Agilität
  - Preise auf Umlagebasis
  - Skalierbarkeit
  - Globale Reichweite
  - Degressionsgewinn
- Erläutern, wie die AWS Cloud es Benutzern ermöglicht, sich auf den Unternehmenswert zu konzentrieren
  - Verlagerung technischer Ressourcen auf umsatzgenerierende Aktivitäten im Gegensatz zur Verwaltung der Infrastruktur

### 1.2 Identifizieren der Aspekte der AWS Cloud-Wirtschaftlichkeit

- Definieren der Elemente, die Teil eines Vorschlags für Gesamtbetriebskosten sind
  - Verstehen der Rolle der Betriebskosten (OpEx)
  - Verstehen der Rolle von Kapitalausgaben (CapEx)
  - Verstehen der Arbeitskosten im Zusammenhang mit dem lokalen Betrieb
  - Verstehen der Auswirkungen der Softwarelizenzierungskosten bei der Migration in die Cloud
- Identifizieren, welche Vorgänge die Kosten senken, indem in die Cloud migriert wird
  - Infrastruktur in richtiger Größe
  - Vorteile der Automatisierung
  - Reduzieren des Compliance-Umfangs (z. B. Managed Services (zum Beispiel RDS, ECS, EKS, DynamoDB))

### 1.3 Erläutern der verschiedenen Prinzipien des Cloud-Architekturdesigns

- Erläutern der Designprinzipien
  - Ausfallsicheres Design
  - Entkoppeln von Komponenten im Vergleich zur monolithischen Architektur
  - Implementieren von Elastizität in der Cloud im Vergleich zu lokal
  - Parallel denken

## Bereich 2: Sicherheit und Compliance

### 2.1. Definieren des AWS-Modells übergreifender Verantwortlichkeit

- Erkennen der Elemente des Modells übergreifender Verantwortlichkeit
- Beschreiben der Verantwortlichkeiten des Kunden in AWS
  - Beschreiben, wie sich die Verantwortlichkeiten des Kunden je nach verwendetem Service ändern können (z. B. mit RDS, Lambda oder EC2)
- Beschreiben der AWS-Verantwortlichkeiten

### 2.2 Definieren von Sicherheits- und Compliance-Konzepten der AWS Cloud

- Identifizieren, wo Sie AWS-Compliance-Informationen finden
  - Speicherorte von Listen anerkannter verfügbarer Compliance-Kontrollen (z. B. HIPPA, SOCs)
  - Erkennen, dass die Compliance-Anforderungen zwischen AWS-Services variieren
- Auf hohem Niveau beschreiben, wie Kunden Compliance in AWS erreichen
  - Identifizieren verschiedener Verschlüsselungsoptionen in AWS (z. B. In Transit, im Ruhezustand)
- Beschreiben, wer die Verschlüsselung in AWS für einen bestimmten Service ermöglicht
- Erkennen, dass es Services gibt, die bei der Prüfung und Berichterstattung helfen
  - Erkennen, dass Protokolle für die Überprüfung und Überwachung existieren (Sie müssen die Protokolle nicht verstehen)
  - Definieren von Amazon CloudWatch, AWS Config und AWS CloudTrail
- Erläutern des Konzepts des am wenigsten privilegierten Zugriffs

### 2.3 Identifizieren der AWS Access Management-Funktionen

- Verstehen des Zwecks des Benutzer- und Identitätsmanagements
  - Zugriffsschlüssel und Kennwortrichtlinien (Rotation, Komplexität)
  - Multi-Factor Authentication (MFA)
  - AWS Identity and Access Management (IAM)
    - Gruppen/Benutzer
    - Rollen
    - Richtlinien, verwaltete Richtlinien im Vergleich zu benutzerdefinierten Richtlinien
  - Aufgaben, die die Verwendung von Root-Konten erfordern  
Schutz von Root-Konten

### 2.4 Identifizieren von Ressourcen für die Sicherheitsunterstützung

- Erkennen, dass es verschiedene Netzwerksicherheitsfunktionen gibt
  - Native AWS-Services (z. B. Sicherheitsgruppen, Netzwerk-ACLs, AWS WAF)
  - Sicherheitsprodukte externer Anbieter aus dem AWS Marketplace
- Erkennen, dass es eine Dokumentation gibt und wo sie zu finden ist (zum Beispiel bewährte Methoden, Whitepaper, offizielle Dokumente)
  - AWS Knowledge Center, Security Center, Sicherheitsforum und Sicherheitsblogs
  - Partner-Systemintegratoren
- Wissen, dass Sicherheitsüberprüfungen eine Komponente von AWS Trusted Advisor sind

## Bereich 3: Technologie

### 3.1 Definieren von Methoden zur Bereitstellung und zum Betrieb in der AWS Cloud

- Identifizieren verschiedener Möglichkeiten der Bereitstellung und des Betriebs in der AWS-Cloud auf hohem Niveau
  - Programmatischer Zugriff, APIs, SDKs, AWS Management Console, CLI, Infrastructure as Code
- Identifizieren verschiedener Arten von Cloud-Bereitstellungsmodellen
  - Alles inbegriffen mit Cloud/Cloud-nativ
  - Hybrid
  - Lokal
- Identifizieren von Konnektivitätsoptionen
  - VPN
  - AWS Direct Connect
  - Öffentliches Internet

### 3.2 Definieren der globalen AWS-Infrastruktur

- Beschreiben der Beziehungen zwischen Regionen, Availability Zones und Edge-Standorten
- Beschreiben, wie Hochverfügbarkeit durch die Verwendung mehrerer Availability Zones erreicht wird
  - Abrufen, dass Hochverfügbarkeit durch die Verwendung mehrerer Availability Zones erreicht wird
  - Erkennen, dass Availability Zones keine einzelnen Fehlerpunkte teilen
- Beschreiben, wann die Verwendung mehrerer AWS-Regionen berücksichtigt werden sollte
  - Notfallwiederherstellung/Betriebskontinuität
  - Niedrige Latenz für Endbenutzer
  - Datensouveränität
- Beschreiben der Vorteile von Edge-Standorten auf hohem Niveau
  - Amazon CloudFront
  - AWS Global Accelerator

### 3.3 Identifizieren der wichtigsten AWS-Services

- Beschreiben der Servicekategorien in AWS (Datenverarbeitung, Speicher, Netzwerk, Datenbank)
- Identifizieren von AWS-Datenverarbeitungsservices
  - Erkennen, dass es verschiedene Datenverarbeitungsfamilien gibt
  - Erkennen der verschiedenen Services, die Datenverarbeitung bereitstellen (z. B. AWS Lambda im Vergleich zu Amazon Elastic Container Service (Amazon ECS) oder Amazon EC2 usw.)
  - Erkennen, dass Elastizität durch Auto Scaling erreicht wird
  - Identifizieren des Zweckes von Load Balancern
- Identifizieren der verschiedenen AWS-Speicherservices
  - Beschreiben von Amazon S3
  - Beschreiben von Amazon Elastic Block Store (Amazon EBS)
  - Beschreiben von Amazon S3 Glacier
  - Beschreiben von AWS Snowball
  - Beschreiben von Amazon Elastic File System (Amazon EFS)
  - Beschreiben von AWS Storage Gateway
- Identifizieren von AWS-Netzwerksservices
  - Identifizieren von VPC
  - Identifizieren von Sicherheitsgruppen
  - Identifizieren des Zweckes von Amazon Route 53
  - Identifizieren von VPN, AWS Direct Connect
- Identifizieren der verschiedenen AWS-Datenbankservices

- Installieren von Datenbanken auf Amazon EC2 im Vergleich zu verwalteten Datenbanken von AWS
- Identifizieren von Amazon RDS
- Identifizieren von Amazon DynamoDB
- Identifizieren von Amazon Redshift

### 3.4 Identifizieren von Ressourcen für die Technologieunterstützung

- Erkennen, dass es eine Dokumentation gibt (bewährte Methoden, Whitepaper, AWS Knowledge Center, Foren, Blogs)
- Identifizieren der verschiedenen Ebenen und des Umfangs des AWS-Supports
  - AWS-Missbrauch
  - AWS-Supportfälle
  - Premium Support
  - Technische Kundenbetreuer
- Erkennen, dass es ein Partnernetzwerk (Marktplatz, Drittanbieter) gibt, einschließlich unabhängiger Softwareanbieter und Systemintegratoren
- Identifizieren von Quellen für die technische Unterstützung und Wissen von AWS, einschließlich Professional Services, Lösungsarchitekten, Schulungen und Zertifizierungen und Amazon Partner Network
- Identifizieren der Vorteile der Verwendung von AWS Trusted Advisor

## Bereich 4: Abrechnung und Preise

### 4.1 Vergleichen und Gegenüberstellen der verschiedenen Preismodelle für AWS (z. B. Preise für On-Demand-Instances, Reserved Instances und Spot-Instance)

- Identifizieren von Szenarien/idealen Lösungen für die On-Demand-Instance-Preise
- Identifizieren von Szenarien/idealen Lösungen für die Reserved Instances-Preise
  - Beschreiben der Flexibilität von Reserved Instances
  - Beschreiben des Verhaltens von Reserved Instances in AWS Organizations
- Identifizieren von Szenarien/idealen Lösungen für Spot-Instance-Preise

### 4.2 Erkennen der verschiedenen Kontostrukturen in Bezug auf Abrechnung und Preisgestaltung in AWS

- Erkennen, dass die konsolidierte Abrechnung eine Funktion von AWS Organizations ist
- Identifizieren, wie mehrere Konten bei der Zuweisung von Kosten zwischen Abteilungen helfen

### 4.3 Identifizieren der für die Abrechnung verfügbaren Ressourcen

- Identifizieren von Möglichkeiten, um Rechnungsunterstützung und Informationen zu erhalten
  - Cost Explorer, AWS Kosten- und Nutzungsbericht, Amazon QuickSight, Drittanbieter-Partner und AWS Marketplace-Tools
  - Öffnen eines Falls zur Abrechnung
  - Die Rolle des Concierge für Kunden des AWS Enterprise Support Plans
- Identifizieren, wo Sie Preisinformationen zu AWS-Services finden
  - Einfacher Monatsrechner in AWS
  - Produktseiten von AWS Services
  - API für AWS-Preise
- Erkennen, dass Alarme/Warnungen existieren
- Identifizieren, wie Tags bei der Kostenzuordnung verwendet werden

## Anhang

### Welche Schlüsselinstrumente, Technologien und Konzepte könnten in der Prüfung drankommen?

Es folgt eine nicht vollständige Liste der Tools und Technologien, die in der Prüfung drankommen könnten. Diese Liste kann sich ändern. Sie soll Ihnen helfen, den allgemeinen Umfang der Services, Funktionen oder Technologien der Prüfung zu verstehen. Die allgemeinen Tools und Technologien in dieser Liste erscheinen in keiner bestimmten Reihenfolge. AWS Services sind nach ihren primären Funktionen gruppiert. Während einige dieser Technologien wahrscheinlich mehr als andere in der Prüfung abgedeckt werden, sind deren Reihenfolge und Platzierung in dieser Liste kein Hinweis auf die relative Gewichtung oder die relative Wichtigkeit:

- APIs
- Cost Explorer
- AWS Kosten- und Nutzungsbericht
- AWS-Befehlszeilenschnittstelle (CLI)
- Elastic Load Balancers
- Amazon EC2-Instance-Typen (z. B. Reserved, On-Demand, Spot)
- Globale AWS-Infrastruktur (z. B. AWS-Regionen, Availability Zones)
- Infrastruktur als Code (IaC)
- Amazon Machine Images (AMIs)
- AWS Management Console
- AWS Marketplace
- AWS Professional Services
- AWS Personal Health Dashboard
- Sicherheitsgruppen
- AWS Service Catalog
- AWS Service Health Dashboard
- Service-Kontingente
- AWS Software Development Kits (SDKs)
- AWS Support Center
- AWS Support-Stufen
- Virtuelle private Netzwerke (VPNs)

### AWS-Services und -Funktionen

Analytics:

- Amazon Athena
- Amazon Kinesis
- Amazon QuickSight

Anwendungsintegration:

- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)

Datenverarbeitung und Serverless:

- AWS Batch
- Amazon EC2
- AWS Elastic Beanstalk
- AWS Lambda

- Amazon Lightsail
- Amazon WorkSpaces

Container:

- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Fargate

Datenbank:

- Amazon Aurora
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon RDS
- Amazon Redshift

Entwickler-Tools:

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS CodeStar

Kundenbindung:

- Amazon Connect

Management, Überwachung und Governance:

- AWS Auto Scaling
- AWS Budgets
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Kosten- und Nutzungsbericht
- Amazon EventBridge (Amazon CloudWatch Events)
- AWS License Manager
- AWS Managed Services
- AWS Organizations
- AWS Secrets Manager
- AWS Systems Manager
- AWS Systems Manager Parameter Store
- AWS Trusted Advisor

Netzwerk und Bereitstellung von Inhalten:

- Amazon API Gateway
- Amazon CloudFront
- AWS Direct Connect
- Amazon Route 53
- Amazon VPC

Sicherheit, Identität und Compliance:

- AWS Artifact
- AWS Certificate Manager (ACM)
- AWS CloudHSM



- Amazon Cognito
- Amazon Detective
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS License Manager
- Amazon Macie
- AWS Shield
- AWS WAF

Speicher:

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic File System (Amazon EFS)
- Amazon S3
- Amazon S3 Glacier
- AWS Snowball Edge
- AWS Storage Gateway