

CL100 CompTIA Cloud+

Kurzbeschreibung:

Teilnehmer erhalten eine praxisnahe Einführung in Konzepte und Techniken für sichere Cloud-Umgebungen. Behandelt werden Aufbau und Automatisierung von Cloud-Infrastrukturen sowie Schutz geschäftskritischer Anwendungen und Daten. Der Kurs bereitet auf die internationale CompTIA Cloud+ Zertifizierung vor und vermittelt herstellerunabhängige Kompetenzen.

Zielgruppe:

Der Kurs **CL100 CompTIA Cloud+** ist geeignet für:

- Systems Administrator
- Systems Engineer
- Cloud Engineer
- Network Administrator
- Network Engineer
- Cloud Specialist
- Cloud Project Manager

Voraussetzungen:

Um den Inhalten und dem Lerntempo des Kurses **CL100 CompTIA Cloud+** gut folgen zu können, sind folgende Vorkenntnisse empfehlenswert:

- mindestens 24 Monate Berufserfahrung im Bereich IT-Netzwerke, Netzwerkspeicher oder Rechenzentrumsverwaltung
- Kenntnis der Definitionen der verschiedenen Cloud Service Modelle (IaaS, PaaS, SaaS)
- Kenntnis der gebräuchlichen Definitionen des Cloud-Bereitstellungsmodells (privat, öffentlich, hybrid)
- mit mindestens einer Public Cloud IaaS-Plattform praktische Erfahrungen gesammelt haben

Sonstiges:

Dauer: 5 Tage

Preis: 2490 Euro plus Mwst.

Ziele:

Der **CL100 CompTIA Cloud+** Kurs vermittelt Ihnen die Fähigkeiten, die für die Aufrechterhaltung und Verbesserung von Cloud-Infrastrukturdiensten erforderlich sind. CompTIA Cloud+ bietet einen umfassenden Überblick über die verschiedenen Kenntnisse, Fähigkeiten und Fertigkeiten, die Systemadministratoren benötigen, um Rechenzentrumsaufgaben effizient auszuführen.

Die CompTIA Cloud+ Zertifizierungsprüfung besteht aus maximal 90 Fragen, die in 90 Minuten beantwortet werden müssen. Sie brauchen ein Ergebnis von mindestens 700 Punkten (auf einer Skala von 100-900), um die Prüfung zu bestehen.

Die Prüfung können Sie in einem [Pearson VUE Testzentrum](#) oder [online](#) ablegen.



Inhalte/Agenda:

- ♦ **CloudArchitektur (23 %)**
 - ♦ Analyse von CloudModellen (öffentlich, privat, hybrid, MultiCloud) zur Unterstützung von Geschäftsanforderungen
 - ♦ Virtualisierungsverfahren und deren Bedeutung in CloudUmgebungen
 - ♦ Einrichtung und Verwaltung von CloudNetzwerken (VPN, virtuelle Netzwerke)
 - ♦ Containertechnologien und deren Einsatz in der Cloud
 - ♦ Orchestrierung von Containern mit Tools wie Kubernetes
 - ♦ Grundlagen von Datenbanken und deren Nutzung in CloudUmgebungen
 - ♦ RessourcenOptimierung für Leistung und Kosteneffizienz
 - ♦ Verwaltung der Abrechnung und Kostenkontrolle in der Cloud
- ♦
- ♦ **Bereitstellung (Deployment) (19 %)**
 - ♦ Analyse der Systemanforderungen für die Migration von Workloads
 - ♦ Einsatz von Infrastructure as Code (IaC) zur Automatisierung
 - ♦ Planung und Durchführung von Migrationen in die Cloud
 - ♦ Bereitstellung und Konfiguration von CloudRessourcen
- ♦
- ♦ **Betrieb (Operations) (17 %)**
 - ♦ LifecycleManagement von CloudRessourcen (skalieren, aktualisieren)
 - ♦ Strategien für Backup und Wiederherstellung zur Sicherstellung der Datenintegrität
 - ♦ Observability: Überwachung und Analyse von CloudUmgebungen zur PerformanceOptimierung
- ♦
- ♦ **Sicherheit (19 %)**
 - ♦ Vulnerability Management: Identifizierung und Behebung von Schwachstellen
 - ♦ Identity & Access Management (IAM): Zugriffskontrollen in der Cloud
 - ♦ ContainerSicherheit (Sicherheitsmaßnahmen für containerisierte Anwendungen)
 - ♦ Einhaltung von ComplianceStandards (z. B. PCI DSS, SOC 2, ISO 27001)
 - ♦ Implementierung von Sicherheitskontrollen zum Schutz von CloudUmgebungen
- ♦
- ♦ **DevOpsGrundlagen (10 %)**
 - ♦ Automatisierung von CloudBetriebsprozessen mit Tools wie Ansible, Jenkins, Terraform
 - ♦ Versionsverwaltung: GitWorkflows, BranchStrategien, CodeReviews
 - ♦ CI/CDPipeline: Automatisierte Build, Test und DeploymentProzesse
 - ♦ Systemintegration: Integration verschiedener Systeme für nahtlose Abläufe
 - ♦ Verwendung von DevOpsTools (z. B. Kubernetes, Ansible, Jenkins)
 - ♦ Eventdriven Architekturen
- ♦
- ♦ **Fehlerbehebung (Troubleshooting) (12 %)**
 - ♦ Analyse und Lösung von Problemen bei Bereitstellung, Konnektivität, Sicherheit
 - ♦ NetzwerkTroubleshooting: DNS, DHCP, VPCInterna
 - ♦ Umgang mit Sicherheitsvorfällen: gestohlene Zugangsdaten, Privilegien eskalieren
 - ♦ Behebung von Störungen bei CloudDiensten und Infrastruktur
 - ♦ Identifikation und Korrektur von Fehlkonfigurationen in CloudUmgebungen