

Managing-Cloud-Security Fragenkatalog - Managing-Cloud-Security Deutsche Prüfungsfragen

Managing Cloud Security - C838 - Final Review Questions and Verified Answers

When is the MOST optimal time to determine if data is classified as secure?

The Creation phase is the most optimal time to classify data as secure. When data is created during the create phase, the sensitivity of the data is known.

Discretionary Access Control (DAC)

DAC is when the owner of the document is responsible for defining the limits on a per-document basis.

PII - Direct Identifiers & Indirect Identifiers

Indirect Identifiers - General information, requires more research to id person

Direct Identifiers - Specific. Directly id a person

Block Storage Characteristics

> Files are stored as sectors on a drive

> Format of virtual machine disks

> VMs and servers use this type of storage

> Database will store files on this type of storage

> Storage is in a hierarchical structure

Pass4Test zusammengestellt WGU Pass4Test Managing-Cloud-Security mit Original-Prüfungsfragen und präzise Antworten, wie sie in der eigentlichen Prüfung erscheinen. Eine der Tatsachen Sicherstellung einer hohen Qualität der WGU Managing Cloud Security (JY02)-Prüfung ist die ständig und regelmäßig zu aktualisieren. Pass4Test ernannt nur die besten und kompetentesten Autoren für ihre Produkte und die Prüfung Pass4Test Managing-Cloud-Security zum Zeitpunkt des Kaufs ist absoluter Erfolg.

Wir Pass4Test Team versteht völlig, dass das Vertrauen zwischen die Verkäufer und die Kunden nicht leicht zu erstellen ist. Wir präsentieren Sie die Fachlichkeit und hohe Effizienz mit WGU Managing-Cloud-Security Prüfungssoftware, die von unserer Herzlichkeit erfüllt ist. Wir helfen Ihnen mit umfassenden Prüfungsaufgaben und ausführlichen Analysen, die WGU Managing-Cloud-Security Prüfung zu bestehen. Wir bieten Sie die freundlichsten Kundendienst, um Ihre Vertrauen zu erwerben. Und das Zertifikat der WGU Managing-Cloud-Security, das Sie erwerben, ist die beste Anerkennung für uns.

>> Managing-Cloud-Security Fragenkatalog <<

Managing-Cloud-Security examkiller gültige Ausbildung Dumps & Managing-Cloud-Security Prüfung Überprüfung Torrents

Die WGU Managing-Cloud-Security Zertifizierungsprüfung sind jedem IT-Fachmann sehr wichtig. Solange Sie das Managing-Cloud-Security Zertifikat bekommen, werden Sie im Beruf sicher nicht aussondert. Sie werden befördert und ein höheres Gehalt beziehen. Mit diesem Zertifikat können Sie alle bekommen, was Sie wünschen. Die Fragenpool zur WGU Managing-Cloud-SecurityZertifizierungsprüfung von Pass4Test sind die Ressourcen zum Erfolg. Mit diesen Schulungsmaterialien werden Sie den Schritt zum Erfolg beschleunigen. Sie werden sicher mehr selbstbewusster.

WGU Managing Cloud Security (JY02) Managing-Cloud-Security Prüfungsfragen mit Lösungen (Q62-Q67):

62. Frage

An organization is undergoing an ISO 27001 audit that includes a software as a service (SaaS) solution within scope, and the auditor has requested evidence of controls. What evidence should the organization provide the auditor?

- A. Operating system patch logs
- **B. Provider compliance attestation**
- C. Network firewall rules
- D. Physical diagram of the data center

Antwort: B

Begründung:

When a SaaS solution is included within the scope of an ISO 27001 audit, the organization should provide the cloud provider's compliance attestation as evidence of controls. Managing Cloud guidance explains that in the SaaS model, the provider manages infrastructure, platform, and application-level controls.

Because customers do not manage operating systems, firewalls, or physical data centers in SaaS, they cannot supply direct technical evidence for those controls. Instead, third-party audit reports and attestations demonstrate that the provider has implemented appropriate security controls.

Firewall rules, OS patch logs, and physical diagrams are not accessible to SaaS customers. Therefore, provider compliance attestation is the correct evidence.

63. Frage

Which term refers to taking an accurate account of a system's desired standard state so changes can be quickly detected for approval or remediation?

- A. Deployment
- **B. Baselineing**
- C. Capacity management
- D. Patch management

Antwort: B

Begründung:

Baselineing is the process of establishing a reference point for the standard configuration of systems, networks, or applications. This baseline represents the approved, secure state. By continuously comparing the current environment to the baseline, organizations can detect deviations, unauthorized changes, or misconfigurations.

Patch management involves updating systems, deployment refers to installing new systems, and capacity management focuses on resource planning. While important, these do not establish a standard state for comparison.

Baselineing is essential for change management and security auditing. It supports configuration management databases (CMDBs), intrusion detection, and compliance requirements. When deviations are detected, they can be escalated for remediation or formally approved through change control processes.

64. Frage

Which description accurately characterizes the movement of applications to the cloud?

- A. In a desktop as a service (DaaS) environment, the customer is responsible for securing the underlying infrastructure.
- **B. In a software as a service (SaaS) environment, the CSP is responsible for securing the platform.**
- C. In an infrastructure as a service (IaaS) environment, the CSP is responsible for securing the platform.
- D. In a platform as a service (PaaS) environment, the customer is responsible for securing the underlying infrastructure.

Antwort: B

Begründung:

In a Software as a Service (SaaS) environment, the cloud service provider (CSP) is responsible for securing the platform. Managing Cloud principles explain that SaaS places the majority of security responsibilities on the provider, including infrastructure, operating systems, middleware, and application security.

Customers primarily manage user access, data usage, and configuration settings, while the provider ensures availability, patching, vulnerability management, and platform protection. This division of responsibility simplifies security management for consumers. The other options misrepresent shared responsibility boundaries. In IaaS, customers secure the platform, and in PaaS, providers manage infrastructure. Therefore, option D accurately characterizes application movement to the cloud.

65. Frage

Which action should a customer take to add an extra layer of protection to the data stored in a public cloud environment?

- **A. Use additional encryption for sensitive files and folders**
- B. Use block storage instead of file storage
- C. Use web application firewalls (WAFs)
- D. Use database activity monitoring (DAM)

Antwort: A

Begründung:

While cloud providers typically offer built-in encryption, customers should apply additional encryption for sensitive data to maintain defense-in-depth. Encrypting files and folders before uploading them ensures that even if provider-side protections fail, data remains confidential.

WAFs protect applications from web threats, DAM tools monitor database use, and block storage versus file storage is an architecture choice. None of these directly provide an extra protective layer for stored data.

By maintaining control of their encryption keys, customers ensure compliance with data protection standards such as GDPR, HIPAA, or PCI DSS. This practice also mitigates insider threats within the provider's environment and supports secure multi-cloud strategies. Encryption remains the strongest safeguard for protecting sensitive files in public cloud storage.

66. Frage

Which design principle of secure cloud computing ensures that users have access to a large number of resources that grow based on user demand?

- A. Virtualization
- B. Collaboration
- **C. Rapid elasticity**
- D. Resource pooling

Antwort: C

Begründung:

Rapid elasticity is the design principle that ensures cloud resources can grow or shrink dynamically based on user demand. Managing Cloud principles explain that rapid elasticity allows cloud systems to automatically scale resources such as compute, storage, and bandwidth in near real time.

This capability ensures that users experience consistent performance even during sudden increases in workload. Resources are provisioned when needed and released when demand decreases, enabling efficient utilization and cost control. From a security perspective, elasticity also supports resilience and availability by preventing resource exhaustion.

Resource pooling enables shared infrastructure, virtualization enables abstraction, and collaboration is not a cloud design principle. Therefore, rapid elasticity is the correct answer.

67. Frage

.....

Pass4Test spezialisiert sich auf die Schulungsunterlagen zur WGU Managing-Cloud-Security Zertifizierungsprüfung. Mit Pass4Test brauchen Sie sich keine Sorgen für die WGU Managing-Cloud-Security Zertifizierungsprüfung zu machen. Die Zertifizierungsantworten von Pass4Test sind qualitativ hochwertig. Sobald Sie Pass4Test wählen, können Sie in kurzer Zeit die Prüfung mit einer hohen Note die WGU Managing-Cloud-Security Zertifizierungsprüfung effizient bestehen und bessere Resultate bei weniger Einsatz erzielen.

Managing-Cloud-Security Deutsche Prüfungsfragen: <https://www.pass4test.de/Managing-Cloud-Security.html>

Sie können im Internet teilweise die Fragen und Antworten zur WGU Managing-Cloud-Security Zertifizierungsprüfung kostenlos als

- [illegible]