Cloud+ Certification Test Bank

Welcome to the Bare Metal Cyber Audio Academy, an audio-first learning library built to help you pass certification exams through clear, practical instruction you can use anywhere. Each course is designed for busy learners who want structured coverage of the exam objectives, high-yield recall practice, and scenario-ready decision skills without needing slides, labs, or extra downloads. The handouts that come with each course are meant to reinforce what you hear, giving you quick reference material like question banks, key definitions, and review prompts you can use before a study session or right before exam day. The goal is simple: help you recognize what the exam is asking, select the best answer confidently, and avoid common traps. You can find the full catalog of courses, books, and resources at https://baremetalcyber.com/, where everything is organized to support steady progress from first listen to test-day readiness.

Find more for free at BareMetalCyber.com

Contents

Bank 1

1. A cloud administrator needs to reduce the risk that a compromised workload can move laterally to other workloads in the same environment. Which approach best supports that goal?
   A. Increase throughput by selecting larger instance types
   B. Enable microsegmentation using tight network controls between workloads
   C. Use object storage for application data instead of block storage
   D. Add a load balancer to distribute traffic across instances

2. A team reports that users cannot reach an application by its hostname, but direct access by IP address works. Which dependency is the most likely root cause based on the provided material?
   A. Domain Name System (DNS)
   B. Block storage
   C. Snapshot scheduling
   D. Multi-factor authentication (MFA)

3. A security review finds that several administrators have broad permissions they do not need for their daily tasks. Which principle is the best match to correct this issue?
   A. Elasticity
   B. Baseline
   C. Least privilege
   D. Zone redundancy

4. A company must restore service within one hour after a major outage, and the exam scenario asks which requirement drives the speed of recovery. Which term best fits?
   A. Recovery Time Objective (RTO)
   B. Recovery Point Objective (RPO)
   C. Storage tiering
   D. Authentication

5. A company states it can tolerate losing up to fifteen minutes of recent transactions during a recovery event. Which requirement is being described?
   A. Recovery Time Objective (RTO)
   B. Recovery Point Objective (RPO)
   C. Service-Level Agreement (SLA)
   D. Availability monitoring

6. After a month of manual console changes, two environments that should be identical begin behaving differently. Which concept best explains this problem?
   A. Configuration drift
   B. Federation
   C. Cloud bursting
   D. Tagging strategy

7. A team wants to release a new application version with minimal downtime and a fast rollback option if errors appear after cutover. Which deployment approach best matches?
   A. Patch management
   B. Blue/green deployment
   C. Right-sizing
   D. Storage tiering

8. A cloud engineer needs a shared directory that multiple systems can mount and use like a standard filesystem. Which storage type best matches?
   A. Object storage
   B. Block storage
   C. File storage
   D. Snapshot

9. During architecture review, a team argues that the cloud provider handles everything, including identity permissions and logging decisions. Which concept best corrects this misunderstanding?
   A. Shared responsibility model
   B. Tenancy
   C. Latency
   D. Observability

10. A billing spike occurs and leadership asks which project or environment caused the increase. Which control best supports attribution of spend to teams and workloads?
    A. Change management
    B. Cost allocation tags
    C. Encryption in transit
    D. Throughput

---

1. Correct Answer: B. Enable microsegmentation using tight network controls between workloads

Explanation: Microsegmentation reduces lateral movement by isolating workloads with tightly controlled network paths. This is a common Cloud+ security design decision because it limits blast radius when one workload is compromised.

2. Correct Answer: A. Domain Name System (DNS)
   Explanation: DNS maps names to IP addresses, so hostname failures with working IP access strongly indicate name resolution issues. The provided material describes DNS as a common hidden dependency that can make a service appear down.

3. Correct Answer: C. Least privilege
   Explanation: Least privilege means granting only the minimum permissions needed to perform required tasks. The provided material highlights broad, unnecessary access as a frequent cause of escalation risk and audit failures.

4. Correct Answer: A. Recovery Time Objective (RTO)
   Explanation: RTO is the maximum acceptable time to restore service after an outage. The scenario focuses on recovery speed, which the material ties directly to RTO-driven design choices.

5. Correct Answer: B. Recovery Point Objective (RPO)
   Explanation: RPO is the maximum acceptable data loss measured in time. The scenario's "fifteen minutes of transactions" matches the provided definition and common exam confusion with RTO.

6. Correct Answer: A. Configuration drift
   Explanation: Configuration drift occurs when environments diverge over time due to manual changes and inconsistent updates. The provided material frames drift as a root cause of "it worked yesterday" problems and a driver for repeatability controls.

7. Correct Answer: B. Blue/green deployment
   Explanation: Blue/green deployment uses a parallel environment and shifts traffic when ready, enabling fast rollback. The provided material links this method to reduced downtime and safer recovery from a bad release.

8. Correct Answer: C. File storage
   Explanation: File storage provides shared directories accessed like a filesystem, which matches the requirement for multi-system mounts. The material contrasts file storage with block and object storage based on access patterns and use cases.

9. Correct Answer: A. Shared responsibility model
   Explanation: The shared responsibility model defines what the provider manages versus what the customer must manage. The material emphasizes that identity,

logging, and many security controls remain customer responsibilities depending on the service model.

10. Correct Answer: B. Cost allocation tags
    Explanation: Cost allocation tags label resources so spending can be grouped by project, team, or environment. The material describes tags as a governance and attribution control for quickly explaining and managing cost spikes.

Bank 2

1. A cloud engineer is selecting encryption controls for a database that stores regulated data. The primary goal is to ensure stored records are unreadable without the correct key. Which control best matches?
   A. Encryption in transit
   B. Encryption at rest
   C. Availability monitoring
   D. Blue/green deployment

2. An application's response time increases even though CPU and memory utilization remain normal. The next decision focuses on where requests are being delayed across the network path. Which concept best fits this symptom focus?
   A. Throughput
   B. Tenancy
   C. Latency
   D. Snapshot

3. A company wants users to sign in using a trusted enterprise identity provider rather than maintaining separate cloud-only accounts. Which concept best describes this approach?
   A. Federation
   B. Microsegmentation
   C. Right-sizing
   D. Storage tiering

4. A team needs to understand what a distributed system is doing by correlating logs, metrics, and traces to explain failures. Which capability best matches?
   A. Patch management
   B. Observability
   C. Role-Based Access Control (RBAC)
   D. Zone redundancy

5. A service owner is deciding which measurement is most meaningful for "how much work the system can process per unit time." Which term best matches?
   A. Throughput
   B. Baseline
   C. Authentication
   D. Data residency

6. An organization requires that certain customer data be stored and processed in specific geographic locations due to legal constraints. Which requirement is being described?
   A. Tenancy
   B. Data residency
   C. Cloud bursting
   D. Capacity planning

7. A team wants to create a repeatable, version-controlled way to deploy identical infrastructure across multiple environments and reduce manual changes. Which approach best fits?
   A. Infrastructure as Code (IaC)
   B. Tagging strategy
   C. Load balancer
   D. Backup and restore

8. An administrator wants to simplify permissions by assigning users to roles that carry predefined permissions, rather than granting permissions one by one. Which access model best fits?
   A. Authentication
   B. Role-Based Access Control (RBAC)
   C. Encryption in transit
   D. Network Address Translation (NAT)

9. A cloud environment must survive the failure of an entire availability zone without taking the service offline. Which design choice best supports this requirement?
   A. Zone redundancy
   B. Right-sizing
   C. Block storage
   D. Cost allocation tags

10. A team wants to move infrequently accessed audit logs to cheaper storage while keeping recent logs readily available for investigations. Which practice best matches?
    A. Storage tiering
    B. Cloud bursting
    C. Multi-Factor Authentication (MFA)
    D. Change management

---

1. Correct Answer: B. Encryption at rest
   Explanation: Encryption at rest protects stored data by making it unreadable without the correct key. The provided material frames it as a common compliance and design decision tied to key management.

2. Correct Answer: C. Latency
   Explanation: Latency is the time delay between a request and a response and can cause user-visible slowness even when systems are not overloaded. The provided material uses latency to steer decisions like region placement and dependency path analysis.

3. Correct Answer: A. Federation
   Explanation: Federation links identities across systems so users authenticate through a trusted identity provider instead of separate accounts everywhere. The provided material highlights it as an enterprise access design concept that is easy to confuse with simple account synchronization.

4. Correct Answer: B. Observability
   Explanation: Observability is understanding system behavior by using logs, metrics, and traces to explain failures. The provided material describes observability as a decision point when troubleshooting stalls due to missing signals or poor correlation.

5. Correct Answer: A. Throughput
   Explanation: Throughput measures how much work a system can perform over time, such as requests per second. The material notes throughput is often confused with latency, so selecting the right metric depends on the symptom.

6. Correct Answer: B. Data residency
   Explanation: Data residency requires data be stored and processed in specific geographic locations to satisfy legal or contractual rules. The provided material ties it to region selection and replication constraints that can override pure technical preferences.

7. Correct Answer: A. Infrastructure as Code (IaC)
   Explanation: IaC manages infrastructure through declarative templates and version-controlled definitions rather than manual console changes. The provided material connects IaC to repeatability and reduced configuration drift across environments.

8. Correct Answer: B. Role-Based Access Control (RBAC)
   Explanation: RBAC assigns permissions to roles and then assigns roles to users or

services, simplifying access management. The provided material emphasizes mis-scoped roles as a frequent security and audit failure point.

9. Correct Answer: A. Zone redundancy
   Explanation: Zone redundancy deploys resources across multiple availability zones so a single zone failure does not take down the service. The provided material frames this as an availability design decision balanced against cost and complexity.

10. Correct Answer: A. Storage tiering
    Explanation: Storage tiering places data into different storage classes based on access frequency and performance needs. The provided material uses tiering as a cost-performance tradeoff for items like logs, backups, and archives.

Bank 3

1. A team is migrating a database workload and needs low-latency I/O with a volume the operating system can format and mount. Which storage type best fits?
   A. Object storage
   B. File storage
   C. Block storage
   D. Snapshot

2. A security assessor requires the organization to control the encryption key lifecycle rather than relying on provider-managed keys. Which approach best matches?
   A. Bring Your Own Key (BYOK)
   B. Encryption in transit
   C. Federation
   D. Availability monitoring

3. An incident response effort is stalled because the team cannot confirm what actions occurred across services during the outage window. Which capability is most directly missing?
   A. Elasticity
   B. Tenancy
   C. Cost allocation tags
   D. Logging

4. A development team wants an automated pipeline that consistently builds, tests, and releases changes to reduce release risk and improve repeatability. Which practice best matches?
   A. Patch management
   B. Continuous Integration and Continuous Delivery (CI/CD)
   C. Change management
   D. Tagging strategy

5. Monitoring shows a compute workload is consistently underutilized, and leadership wants to reduce cost without harming performance. Which action best aligns with the provided material?
   A. Right-sizing
   B. Cloud bursting
   C. Zone redundancy
   D. Data residency

6. A business requirement states the service must continue operating even if an entire region becomes unavailable. Which architecture choice best supports that outcome?
   A. Availability monitoring
   B. Storage tiering
   C. Multi-region deployment
   D. Instance type change

7. A private subnet needs outbound internet access for updates while keeping workloads from being directly reachable from the internet. Which network component best supports this?
   A. Load balancer
   B. Virtual Private Cloud (VPC)
   C. Microsegmentation
   D. Network Address Translation (NAT)

8. A cloud engineer needs a rule set that permits or denies traffic based on source, destination, port, and protocol to tightly control flows. Which control best fits?
   A. Zero Trust
   B. Access Control List (ACL)
   C. Role-Based Access Control (RBAC)
   D. Metrics

9. Performance troubleshooting starts by comparing current behavior to a known-good reference for normal conditions. Which concept best matches that reference point?
   A. Throughput
   B. Telemetry
   C. Baseline
   D. Service-Level Agreement (SLA)

10. An application must distribute incoming requests across multiple instances and remove unhealthy targets automatically to improve availability. Which component best fits?
    A. Load balancer
    B. File storage
    C. Encryption at rest
    D. Capacity planning

---

1. Correct Answer: C. Block storage
   Explanation: Block storage provides raw volumes that an operating system can format and mount, which is commonly used for databases and high-performance workloads. The provided material distinguishes block storage from object and file storage based on access patterns and latency needs.

2. Correct Answer: A. Bring Your Own Key (BYOK)
   Explanation: BYOK means using customer-managed encryption keys rather than provider-managed keys. The provided material frames this as a common security and compliance decision tied to control of key lifecycle and auditability.

3. Correct Answer: D. Logging
   Explanation: Logging records events and activity that support troubleshooting, security monitoring, and evidence of what happened. The provided material emphasizes that missing or non-centralized logs can block incident triage and confirmation of root cause.

4. Correct Answer: B. Continuous Integration and Continuous Delivery (CI/CD)
   Explanation: CI/CD is an automated pipeline that builds, tests, and releases changes frequently and consistently. The provided material links CI/CD to improved repeatability and reduced release risk when controls like testing gates and rollback paths are present.

5. Correct Answer: A. Right-sizing
   Explanation: Right-sizing adjusts resource allocations to match actual workload needs to improve performance and control cost. The provided material notes right-sizing commonly follows monitoring data showing consistent underuse or saturation.

6. Correct Answer: C. Multi-region deployment
   Explanation: Multi-region deployment runs services in more than one region to reduce risk from regional outages. The provided material highlights tradeoffs such as replication, consistency, cost, and complexity of failover and routing.

7. Correct Answer: D. Network Address Translation (NAT)
   Explanation: NAT maps private addresses to public addresses and commonly enables outbound internet access without directly exposing internal systems. The provided material connects NAT to egress behavior and troubleshooting connectivity paths.

8. Correct Answer: B. Access Control List (ACL)
   Explanation: An ACL is a rule set that permits or denies traffic based on attributes

like source, destination, port, and protocol. The provided material frames ACL choices as “tightest rule set that still meets the requirement” decisions.

9. Correct Answer: C. Baseline
   Explanation: A baseline is a known-good reference for normal performance, capacity, configuration, or behavior. The provided material uses baselines to support troubleshooting by identifying regressions and abnormal patterns.

10. Correct Answer: A. Load balancer
    Explanation: A load balancer distributes traffic across multiple instances to improve availability and performance. The provided material ties load balancers to health checks and failure isolation decisions that keep services stable during instance failures.

Bank 4

1. A team is deciding what to measure to spot abnormal behavior and quickly confirm whether a performance issue is a real regression or just normal fluctuation. Which item best fits as the reference they compare against?
   A. Baseline
   B. Tenancy
   C. Snapshot
   D. Encryption in transit

2. An auditor asks who is responsible for identity permissions, logging choices, and data protection controls in a cloud deployment, since “the provider handles everything” is not acceptable. Which concept best frames the correct answer?
   A. Observability
   B. Shared responsibility model
   C. Elasticity
   D. Storage tiering

3. A company needs a repeatable method to request, approve, implement, and document changes so risky updates do not repeatedly break production. Which practice best matches?
   A. Change management
   B. Microsegmentation
   C. Cloud bursting
   D. Throughput

4. Users report the application is “slow,” and the team must decide whether the issue is delay per request rather than total work processed per second. Which term best matches the “delay per request” concept?
   A. Throughput
   B. Capacity planning
   C. Latency
   D. Cost allocation tags

5. Security policy requires stronger assurance for administrator access than passwords alone. Which control best satisfies that requirement?
   A. Domain Name System (DNS)
   B. Multi-Factor Authentication (MFA)
   C. Block storage
   D. File storage

6. An organization wants a consistent way to label resources so ownership, environment, and application context are obvious during incidents and audits. Which approach best matches?
   A. Tenancy
   B. Load balancer
   C. Tagging strategy
   D. Zone redundancy

7. A cloud architect needs to ensure the service stays available even if a single facility inside a region fails, while keeping low latency within that region. Which design choice best supports this goal?
   A. Availability Zone (AZ) distribution
   B. Data residency enforcement
   C. Cloud bursting
   D. Patch management

8. A team wants to reduce time-to-recover from a bad release by shifting traffic between two environments with a quick rollback option. Which method best matches?
   A. Backup and restore
   B. Blue/green deployment
   C. Storage tiering
   D. Network Address Translation (NAT)

9. A workload needs resources to grow and shrink automatically with demand to avoid overprovisioning. Which capability best matches?
   A. Federation
   B. Encryption at rest
   C. Elasticity
   D. Snapshot

10. A security reviewer wants network rules that isolate workloads to prevent lateral movement and reduce blast radius after a compromise. Which approach best matches?
    A. Role-Based Access Control (RBAC)
    B. Storage tiering
    C. Microsegmentation
    D. Service-Level Agreement (SLA)

---

1. Correct Answer: A. Baseline
   Explanation: A baseline is a known-good reference for normal performance, configuration, or behavior. The provided material uses baselines to help identify regressions and abnormal patterns during troubleshooting.

2. Correct Answer: B. Shared responsibility model
   Explanation: The shared responsibility model defines which duties belong to the provider versus the customer. The provided material emphasizes that identity, logging, and many security controls remain customer responsibilities depending on the service model.

3. Correct Answer: A. Change management
   Explanation: Change management is the controlled process for requesting, approving, implementing, and documenting changes to reduce risk. The provided material ties it to safer rollouts, rollback planning, and proper tracking even under urgency.

4. Correct Answer: C. Latency
   Explanation: Latency is the time delay between a request and a response and is felt as “slowness” even when utilization is normal. The provided material contrasts latency with throughput to guide the right troubleshooting focus.

5. Correct Answer: B. Multi-Factor Authentication (MFA)
   Explanation: MFA requires two or more factors to authenticate and provides stronger assurance than passwords alone. The provided material highlights MFA as a high-yield control, especially for administrative access.

6. Correct Answer: C. Tagging strategy
   Explanation: A tagging strategy is a consistent way to label resources for ownership, environment, application, and governance context. The provided material connects tagging to operational control and faster response during cost and incident investigations.

7. Correct Answer: A. Availability Zone (AZ) distribution
   Explanation: An availability zone is an isolated location within a region designed to reduce shared-failure risk. The provided material uses AZ distribution for high availability decisions that avoid single-facility outages while staying within a region.

8. Correct Answer: B. Blue/green deployment
   Explanation: Blue/green deployment uses a parallel environment and shifts traffic when ready, enabling fast rollback. The provided material links it to reduced downtime and safer recovery when a release introduces errors.

9. Correct Answer: C. Elasticity
   Explanation: Elasticity is the ability to automatically add or remove resources to match demand. The provided material notes elasticity reduces overprovisioning but may introduce warm-up delays and dependency bottlenecks.

10. Correct Answer: C. Microsegmentation
    Explanation: Microsegmentation breaks networks into small, tightly controlled segments to reduce lateral movement. The provided material frames it as a security design choice that limits blast radius when a workload is compromised.

Bank 5

1. A team wants to keep sensitive data readable only when the correct keys are available, even if the underlying storage media is accessed by an unauthorized party. Which control best matches?
   A. Encryption at rest
   B. Encryption in transit
   C. Availability monitoring
   D. Load balancer

2. A cloud administrator needs a clear record of activity across services for troubleshooting and security investigation. Which capability best supports this need?
   A. Latency
   B. Logging
   C. Instance type
   D. Tenancy

3. A company must be able to explain which team and environment caused a sudden cost spike by grouping spend to specific resources. Which practice best supports this?
   A. Shared responsibility model
   B. Federation
   C. Cost allocation tags
   D. Object storage

4. A cloud architect is choosing a storage option for long-term backups and large unstructured datasets that must scale easily and store metadata. Which storage type best fits?
   A. Object storage
   B. Block storage
   C. File storage
   D. Network Address Translation (NAT)

5. An environment that is supposed to be identical across regions diverges after repeated manual console updates, causing inconsistent behavior. Which concept best describes this issue?
   A. Patch management
   B. Configuration drift

C. Observability
D. Storage tiering

6. A network design requires an isolated cloud network where subnets and routing can be defined to support segmentation and secure connectivity. Which component best matches?
   A. Virtual Private Cloud (VPC)
   B. Service-Level Agreement (SLA)
   C. Recovery Time Objective (RTO)
   D. Baseline

7. A team needs to recover service quickly after a major outage, and the requirement is stated as “service must be restored within one hour.” Which requirement is being described?
   A. Recovery Point Objective (RPO)
   B. Data residency
   C. Recovery Time Objective (RTO)
   D. Throughput

8. A security review finds permissions are granted directly to individuals in inconsistent ways, and the team wants to simplify access management by assigning roles instead. Which model best fits?
   A. Access Control List (ACL)
   B. Role-Based Access Control (RBAC)
   C. Multi-region deployment
   D. Backup and restore

9. A team wants a deployment method that reduces downtime and enables an immediate rollback by switching traffic between two environments. Which approach best fits?
   A. Storage tiering
   B. Change management
   C. Baseline comparison
   D. Blue/green deployment

10. A cloud service must continue operating even if an entire region fails, and the design must account for replication and routing complexity. Which architecture choice best matches?
    A. Cloud bursting
    B. Availability monitoring

C. Multi-region deployment
D. Snapshot

---

1. Correct Answer: A. Encryption at rest
   Explanation: Encryption at rest protects stored data by making it unreadable without the correct key. The provided material ties it to compliance requirements and key management decisions.
2. Correct Answer: B. Logging
   Explanation: Logging records events and activity for troubleshooting and security monitoring. The provided material emphasizes that missing logs can prevent confirming what happened during incidents.
3. Correct Answer: C. Cost allocation tags
   Explanation: Cost allocation tags label resources so spending can be grouped by team, project, or environment. The provided material describes tags as a way to quickly attribute and investigate cost spikes.
4. Correct Answer: A. Object storage
   Explanation: Object storage stores data as objects with metadata in a flat namespace and is optimized for durability and scale. The provided material positions it for backups, archives, and unstructured data rather than block or file use cases.
5. Correct Answer: B. Configuration drift
   Explanation: Configuration drift occurs when environments diverge over time due to manual changes and inconsistent updates. The provided material highlights drift as a common root cause of inconsistent behavior across environments.
6. Correct Answer: A. Virtual Private Cloud (VPC)
   Explanation: A VPC is a logically isolated network environment where you define subnets, routing, and network controls. The provided material uses VPC design to test segmentation and secure connectivity decisions.
7. Correct Answer: C. Recovery Time Objective (RTO)
   Explanation: RTO is the maximum acceptable time to restore service after an outage. The provided material uses RTO to drive choices like failover strategy and recovery design.
8. Correct Answer: B. Role-Based Access Control (RBAC)
   Explanation: RBAC assigns permissions to roles and then assigns roles to users or

services. The provided material notes RBAC simplifies access management and that mis-scoped roles are common exam-relevant pitfalls.

9. Correct Answer: D. Blue/green deployment
   Explanation: Blue/green deployment shifts traffic between parallel environments to reduce downtime and enable fast rollback. The provided material connects it to safer releases and quicker recovery from bad deployments.

10. Correct Answer: C. Multi-region deployment
    Explanation: Multi-region deployment runs services in more than one region to reduce risk from regional outages. The provided material highlights tradeoffs involving replication, consistency, cost, and routing complexity.