Cloud+ Exam Glossary

Find more at BareMetalCyber.com

1. **Capacity Planning**
   Capacity planning is forecasting resource needs (compute, memory, storage, network) so performance targets stay met as usage changes. On the exam it often shows up as "right-sizing vs. scaling": choose whether to add resources, redesign, or set autoscaling based on trends and headroom.

2. **Change Management**
   Change management is the controlled process for requesting, approving, implementing, and documenting changes to reduce risk. Cloud+ scenarios test whether you pick the safest next step (maintenance window, rollback plan, approvals) when a change causes outages or when urgent fixes must still be tracked.

3. **Cloud Bursting**
   Cloud bursting is using cloud resources temporarily when on-premises or primary capacity is exceeded. Exam questions use it to test hybrid design tradeoffs, especially latency, data movement costs, and security controls when workloads span environments.

4. **Cloud Service Model**
   Cloud service models describe what the provider manages vs. what you manage, commonly IaaS, PaaS, and SaaS. On the exam, this drives responsibility decisions: patching, logging, identity controls, backups, and where misconfigurations most likely occur.

5. **Configuration Drift**
   Configuration drift is when systems slowly diverge from the intended configuration over time due to manual changes, inconsistent patches, or unmanaged updates. Cloud+ items often treat drift as the root cause of "it worked yesterday" problems and push you toward automation, version control, and continuous validation.

6. **Continuous Integration and Continuous Delivery (CI/CD)**
   CI/CD is an automated pipeline that builds, tests, and releases changes frequently and consistently. On the exam, it shows up as a way to reduce release risk and improve repeatability, with common traps around poor secrets handling, weak testing gates, or missing rollback paths.

7. **Cost Allocation Tags**
   Cost allocation tags are labels applied to cloud resources so spending can be grouped by team, project, environment, or application. Cloud+ uses this to test governance and financial accountability, especially when a bill spikes and you must attribute costs quickly and accurately.

8. **Data Residency**
   Data residency is the requirement that data be stored and processed in specific geographic locations to meet legal or contractual rules. Exam scenarios use it to test region selection, replication choices, and compliance constraints that can override purely technical preferences.

9. **Disaster Recovery (DR)**
   Disaster recovery is the set of plans and capabilities to restore services after major outages, including site failures or widespread corruption. Cloud+ questions frequently hinge on selecting the right DR approach and proving it meets recovery objectives, not just stating that backups exist.

10. **Domain Name System (DNS)**
    DNS maps names to IP addresses and supports service discovery and routing in many cloud designs. On the exam, DNS is a common hidden dependency: outages may look like “service down” when the real issue is misconfigured records, TTL behavior, or failed name resolution.

11. **Elasticity**
    Elasticity is the ability to automatically add or remove resources to match demand, often in near real time. On the exam, it shows up as selecting autoscaling policies and understanding that elasticity reduces overprovisioning but can introduce warm-up delays and dependency bottlenecks.

12. **Encryption at Rest**
    Encryption at rest protects stored data such as disks, databases, and object storage by making it unreadable without the correct key. Cloud+ questions test when it is required for compliance, how keys are managed, and how encryption choices affect recovery and forensic access.

13. **Encryption in Transit**
    Encryption in transit protects data moving across networks, typically using protocols like TLS. Exam scenarios often ask you to choose controls that prevent interception and tampering between services, especially in hybrid connections and service-to-service traffic.

14. **Federation**
    Federation is linking identities across systems so users can authenticate through a trusted identity provider rather than maintaining separate accounts everywhere. On Cloud+, it commonly appears in enterprise access design and can be a trap if you confuse it with simple account synchronization.

15. **File Storage**
    File storage provides shared directories accessed via file protocols and is usually used for shared content, home directories, or applications expecting a filesystem. The exam uses it to test picking the right storage type and recognizing performance, locking, and throughput constraints.

16. **High Availability (HA)**
    High availability is designing services to stay up despite component failures through redundancy, failover, and health-based routing. Cloud+ items typically test which layer you make redundant and how you avoid single points of failure across compute, storage, and network paths.

17. **Identity and Access Management (IAM)**
    IAM is the framework of identities, roles, policies, and controls that govern who or what can access cloud resources. On the exam, IAM decisions are high-yield because mis-scoped permissions and overprivileged roles are frequent root causes of breaches.

18. **Infrastructure as Code (IaC)**
    IaC is managing infrastructure through declarative templates and version-controlled definitions rather than manual console changes. Cloud+ questions use IaC to test repeatability, drift prevention, and safe change rollout, especially in multi-environment deployments.

19. **Instance Type**
    An instance type is a predefined compute configuration that sets CPU, memory, storage options, and sometimes network performance. On the exam, it shows up in right-sizing decisions where you choose between scaling up, scaling out, or selecting a different resource profile.

20. **Key Management**
    Key management is generating, storing, rotating, revoking, and auditing cryptographic keys used for encryption and signing. Cloud+ scenarios test the operational reality: losing control of keys can mean losing data access, and weak rotation or access controls can undermine encryption entirely.

21. **Latency**
    Latency is the time delay between a request and a response, often felt by users as “slowness” even when systems are not overloaded. On the exam, latency is used to steer architecture choices like region placement, caching, and whether to use synchronous calls between services.

22. **Least Privilege**
    Least privilege means granting only the minimum permissions needed for a user or service to perform its task. Cloud+ questions frequently test permission scoping, role design, and avoiding wildcard access that creates easy escalation paths.

23. **Load Balancer**
    A load balancer distributes traffic across multiple instances or endpoints to improve availability and performance. On the exam, it is commonly tied to health checks, session persistence, TLS termination, and failure isolation, with traps around misconfigured health probes causing “false failovers.”

24. **Logging**
    Logging is recording events and activity for troubleshooting, security monitoring, and compliance evidence. Cloud+ scenarios test whether the right logs exist, whether they are centralized and retained, and how to use them to confirm a hypothesis during incident response.

25. **Metrics**
    Metrics are numerical measurements over time such as CPU utilization, requests per second, error rate, and queue depth. Exam questions often require selecting the most meaningful metric for the symptom and avoiding the trap of chasing a noisy or irrelevant signal.

26. **Microsegmentation**
    Microsegmentation is breaking networks into small, tightly controlled segments to reduce lateral movement and limit blast radius. On Cloud+, it appears in security design questions where you choose network and identity controls to isolate workloads and reduce implicit trust.

27. **Multi-Factor Authentication (MFA)**
    MFA requires two or more factors to authenticate, such as something you know plus something you have. The exam uses MFA as a high-yield security control, especially for admin access, and may test exceptions like service accounts that require different protections.

28. **Multi-Region Deployment**
    Multi-region deployment runs services in more than one region to improve resilience and reduce risk from regional outages. Cloud+ questions use it to test tradeoffs involving data replication, consistency, cost, and complexity of failover and routing.

29. **Network Address Translation (NAT)**
    NAT maps private addresses to public addresses, often enabling outbound internet access without exposing internal systems directly. Exam scenarios test whether NAT is being used for egress control, IP conservation, or segmentation, and how it affects troubleshooting connectivity.

30. **Object Storage**
    Object storage stores data as objects with metadata in a flat namespace and is optimized for durability and scale. Cloud+ items use it for selecting storage for backups, archives, and unstructured data, and for recognizing differences from file and block storage.

31. **Observability**
    Observability is the ability to understand what a system is doing by using logs, metrics, and traces to explain behavior and failures. On the exam, it shows up as choosing what telemetry is missing when troubleshooting is stuck and how to correlate signals across distributed services.

32. **Patch Management**
    Patch management is the process of applying updates to fix vulnerabilities, bugs, or compatibility issues while controlling risk. Cloud+ questions test responsibility boundaries (who patches in different service models) and safe rollout practices that avoid breaking production.

33. **Recovery Point Objective (RPO)**
    RPO is the maximum acceptable amount of data loss measured in time, such as “no more than fifteen minutes of lost transactions.” On the exam, RPO drives backup frequency and replication strategy, and it is often confused with recovery time, so read stems carefully.

34. **Recovery Time Objective (RTO)**
    RTO is the maximum acceptable time to restore a service after an outage, such as “service must be back within one hour.” Cloud+ scenarios use RTO to select between warm standby, active-active, or simpler restore approaches, balancing speed against cost and complexity.

35. **Resilience**
    Resilience is the ability of a system to withstand failures and recover while continuing to provide acceptable service. Exam items use it to test design patterns like redundancy, graceful degradation, and automated recovery rather than relying on manual intervention.

36. **Right-Sizing**
    Right-sizing is adjusting resource allocations to match actual workload needs to improve performance and control cost. On Cloud+, it commonly appears after monitoring data shows consistent underuse or saturation, and the decision is whether to scale up, scale out, or redesign.

37. **Role-Based Access Control (RBAC)**
    RBAC assigns permissions to roles and then assigns roles to users or services, simplifying access management at scale. The exam often tests RBAC as the safer alternative to individual permissions and highlights mis-scoped roles as a frequent security and audit failure.

38. **Service-Level Agreement (SLA)**
    An SLA is a formal commitment about availability, performance, support response, or remediation, usually between provider and customer. Cloud+ questions use SLAs to test expectations and risk decisions, such as whether a design meets uptime requirements given provider guarantees.

39. **Shared Responsibility Model**
    The shared responsibility model defines which security and operational duties belong to the cloud provider and which belong to the customer. On the exam, it is a frequent decision point for controls like patching, identity, logging, data protection, and network configuration.

40. **Snapshot**
    A snapshot is a point-in-time capture of data or a volume state that can be used for restore or cloning. Cloud+ scenarios test whether a snapshot is an appropriate recovery mechanism, how it differs from backups, and how snapshot sprawl can create cost and governance issues.

41. **Storage Tiering**
    Storage tiering is placing data into different storage classes based on access frequency and performance needs, such as hot, warm, and cold tiers. On the exam, tiering decisions show up as cost-performance tradeoffs, especially for logs, backups, and archives.

42. **Tagging Strategy**
    A tagging strategy is a consistent way to label resources for ownership, environment, application, cost tracking, and governance. Cloud+ questions use tagging to test operational control, incident response speed, and cost accountability when resources sprawl.

43. **Telemetry**
    Telemetry is the collection and transmission of monitoring data such as metrics, logs, events, and traces. Exam items often use telemetry gaps to explain why teams cannot confirm root cause, pushing you toward improving data collection and correlation.

44. **Tenancy**
    Tenancy describes whether resources are dedicated to a single customer or shared among multiple customers with logical isolation. Cloud+ questions test risk and compliance decisions where shared tenancy may be acceptable, but certain workloads require stronger isolation.

45. **Throughput**
    Throughput is how much work a system can perform over time, such as requests per second or megabytes per second. On the exam, throughput guides scaling and storage decisions, and it can be confused with latency, so choose the metric that matches the symptom.

46. **Virtual Private Cloud (VPC)**
    A VPC is a logically isolated network environment in the cloud where you define subnets, routing, and network controls. Cloud+ scenarios use VPC design to test segmentation, secure connectivity, and how routing or security rules can break application dependencies.

47. **Vulnerability Management**
    Vulnerability management is identifying, prioritizing, remediating, and verifying security weaknesses across systems and software. On Cloud+, it often appears as choosing the right response to scan results, balancing severity, exposure, and change risk.

48. **Workload**
    A workload is a unit of compute activity, such as an application, service, job, or batch process, along with its resource and dependency needs. Exam questions use "workload" to force you to match characteristics to the right platform choice, scaling pattern, and protection controls.

49. **Zero Trust**
    Zero Trust is a security approach that assumes no implicit trust and requires verification for each access request based on identity, device, and context. On the exam, it shows up as selecting controls that reduce lateral movement, tighten access, and rely on strong identity and policy enforcement.

50. **Zone Redundancy**
    Zone redundancy is deploying resources across multiple availability zones so a single zone failure does not take down the service. Cloud+ uses it in architecture scenarios where you must meet availability requirements while balancing cost, complexity, and data consistency.