PassQueen
a.k.a dumpsqueen.com

ACA Cloud Security Associate

Alibaba Cloud ACA-Sec1

Version Demo

Total Demo Questions: 17

Total Premium Questions: 178

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cloud Security Fundamentals	51
Topic 2, Identity and Access Management	12
Topic 3, Network Security	87
Topic 4, Data Security	5
Topic 5, Security Management and Compliance	15
Topic 6, Mix Questions	8
Total	178

QUESTION NO: 1

Which of the following descriptions of the shared responsibilities security model is CORRECT?

A. After beginning to use cloud service, the cloud service provider will become responsible for all ofthe user's security.

B. After beginning to use cloud service, the user and the cloud service provider will be jointlyresponsible for cloud security, with each responsible for different layers of security.

C. After beginning to use cloud service, users must still take care of physical and environmentalsecurity.

D. After beginning to use cloud service, users only need to pay attention to the security of their ownapps and data. All other security will be the responsibility of the cloud service provider.

ANSWER: B

Explanation:

After beginning to use cloud service, the user and the cloud service provider will be jointly responsible for cloud security, with each responsible for different layers of security. This is the central principle of the shared responsibility model: Alibaba Cloud operates and protects the underlying cloud infrastructure, including physical data centers, facilities, hardware, and core cloud-platform components. Customers remain accountable for securing what they deploy and configure in the cloud. Depending on the service type, this includes identity and access management, account credentials, network-access rules, operating-system configuration, application security, data classification, encryption choices, and data access permissions. The exact boundary changes with the service model: managed services shift more operational responsibility to the provider, while IaaS services require customers to manage more of the operating environment. However, using a cloud service never removes the customer's responsibility to configure and use that service securely. Clearly defining these respective responsibilities helps organizations select appropriate controls, maintain compliance, and protect workloads effectively. Alibaba Cloud describes this division as security *of* the cloud being handled by Alibaba Cloud and security *in* the cloud being a customer responsibility. See the Alibaba Cloud Trust Center and Alibaba Cloud security responsibilities documentation.

QUESTION NO: 2

If your company has a lot of employees who would try to simultaneously access ECS server protected by 'Server Guard' using your company's intranet, the 'Sever Guard' may

mistakenly identify those access requests as attacks. Which of the following methods is the best way to solve this problem? Score 2

A. set a highly complexed administrator password

B. change the rule of security group to unblock all company internal ips

C. add those IPs which need to access ECS server into 'Server Guard' logon white list

D. ask employees to access that ECS server not very frequently

ANSWER: C

Explanation:

Adding the company intranet source IP addresses to the Server Guard logon whitelist is the appropriate solution because the alerts are caused by legitimate, high-volume login activity originating from known and trusted corporate networks. A logon whitelist provides a narrowly scoped exception for those trusted sources, allowing employees to continue accessing the ECS instance without their simultaneous login attempts being treated as brute-force attacks. This directly addresses the false-positive detection issue while retaining the security service's protection for login attempts from all other, untrusted IP addresses.

In Alibaba Cloud Security Center, brute-force attack defense is intended to identify abnormal repeated authentication activity. Administrators can configure trusted IP addresses through the relevant whitelist settings when expected operational behavior would otherwise trigger protection or alerts. The whitelist should be limited to stable corporate egress IP ranges and reviewed whenever network routing, VPN gateways, or office locations change. This maintains the intended balance: normal company access is permitted, while suspicious login behavior from non-whitelisted sources remains subject to detection and

response. See Alibaba Cloud's brute-force attack defense configuration documentation and the Security Center documentation for current configuration guidance.

QUESTION NO: 3

Using ECS security group can help you achieve:

A. better CPU usage

B. fine grained access control to you server

C. enlarge your network bandwidth

D. apply QOS to a specific IP

ANSWER: B

Explanation:

"fine grained access control to you server" is correct because an Elastic Compute Service (ECS) security group acts as a stateful virtual firewall for ECS instances. Its inbound and outbound rules let an administrator define which traffic is permitted according to criteria such as protocol, port range, source or destination IP address, and, where applicable, another security group. This enables administrators to expose only the services an instance needs—for example, allowing administrative access from a trusted address range and application traffic only from designated internal resources—while retaining a default-deny posture for traffic that has not been explicitly allowed.

Security groups can be associated with ECS instances and Elastic Network Interfaces, allowing a common, reusable network-access policy to be applied to related workloads. Rules can also be adjusted as an application architecture changes, without requiring configuration of an operating-system firewall on every server. Alibaba Cloud describes security groups as logical groups that provide access-control capabilities for ECS instances, and documents the rule attributes used to control inbound and outbound traffic. For implementation details and rule behavior, see the Alibaba Cloud ECS security groups documentation and the security group rule configuration guide.

QUESTION NO: 4

What is the primary security benefit of using HTTPS rather than HTTP for a public web application?

A. Encrypting data transmitted between the client and server

B. Automatically removing all web application vulnerabilities

C. Preventing all DDoS attacks without additional protection

D. Making a website accessible without DNS resolution

ANSWER: A

Explanation:

Encryption of data in transit is the correct answer. HTTPS uses TLS to protect HTTP communication between a client and server. TLS encrypts the transmitted data and also provides mechanisms for server authentication and integrity protection. This reduces the risk that an attacker monitoring the network can read or modify sensitive information such as credentials, session identifiers, and submitted form data.

HTTPS does not itself remove application vulnerabilities such as SQL injection or authorization flaws. Those issues still require secure coding, patching, and appropriate application-layer protection. For HTTP semantics and TLS usage, see RFC 9110: HTTP Semantics and RFC 8446: The Transport Layer Security Protocol Version 1.3.

QUESTION NO: 5

Which command in RedHat Linux shell can be used to check disk usage?

A. ls

B. df

C. diskUsage

D. diskSpace

ANSWER: B

Explanation:

The `df` command is used to report disk-space usage for mounted file systems in Red Hat Enterprise Linux. It displays information such as the filesystem name, total capacity, space used, space available, utilization percentage, and mount point. For a readable output format, administrators commonly run `df -h`, where the `-h` option presents sizes using units such as MiB and GiB. This makes `df` the appropriate command when the objective is to check overall available and consumed space on disks or mounted filesystems. The command is especially useful during routine operational checks, capacity monitoring, and troubleshooting errors caused by a filesystem reaching full capacity. Red Hat documents filesystem space monitoring with `df`, including use of the human-readable option: Red Hat Enterprise Linux: Managing file systems. The GNU Core Utilities reference also defines `df` as reporting filesystem disk-space usage: GNU Coreutils df invocation.

QUESTION NO: 6

CC attacks can cause serious damages. Which of the following statements about CC attack is

not correct?

Score 2

A. CC attack will simulate real user requests

B. Will consume massive sever side resource

C. CC attack is done on network layer

D. The request generated by CC attack is hard to be distinguished from normal requests

ANSWER: C

Explanation:

“CC attack is done on network layer” is the statement that is not correct. A Challenge Collapsar (CC) attack is an application-layer denial-of-service attack, commonly directed at HTTP or HTTPS services. Attackers generate a high volume of requests for web pages, APIs, dynamic content, or resource-intensive operations. Although the traffic uses network connectivity to reach the target, the attack’s intended exhaustion point is the web application stack and its associated server-side resources, such as web-server workers, CPU, memory, database connections, session capacity, or backend processing capacity.

This application-layer nature is important because CC requests can resemble requests from genuine users. Effective protection therefore commonly uses request-rate controls, behavioral analysis, bot management, verification challenges, and URL- or session-based rules rather than relying only on network-layer traffic filtering. Alibaba Cloud Web Application Firewall provides CC protection specifically to detect and mitigate excessive HTTP(S) request behavior aimed at websites and applications. Alibaba Cloud documents CC protection as a WAF capability for configuring protection rules around request frequency and access behavior: Configure CC protection. See also the Alibaba Cloud Web Application Firewall overview for WAF’s role in protecting web applications at the HTTP/HTTPS layer.

QUESTION NO: 7

In an IP (Internet Protocol) spoofing attack, what field of an IP (Internet Protocol) packet does the

attacker manipulate?

A. The version field

B. The source address field

C. The source port field

D. The destination address field

ANSWER: B

Explanation:

IP spoofing consists of forging the source IP address in an IP packet's header so that the packet appears to have originated from a different host or network. Therefore, **The source address field** is correct. Attackers may use a spoofed source address to conceal the real origin of traffic, impersonate a trusted system in poorly protected trust-based communications, or support reflection and amplification denial-of-service attacks, where replies are directed to a victim whose address was forged as the source.

IPv4 defines a Source Address field in its header, and this field identifies the sender address carried by the datagram. Because the IP layer does not inherently verify that a sender owns the address placed in this field, networks commonly apply ingress and egress filtering, also called source-address validation, to reduce spoofed traffic. Alibaba Cloud security controls such as security groups and network ACLs can help restrict permitted traffic paths, while source-address validation at network boundaries remains a foundational anti-spoofing practice. See the IPv4 specification (RFC 791) and Network Ingress Filtering guidance (BCP 38/RFC 2827).

QUESTION NO: 8

What are the advantages of anti-DDOS pro comparing to anti-DDOS basics service?

(the number of correct answers: 3)

A. stronger defending attacks capability

B. elastic protection bandwidth

C. no upper limit to the attack traffic need to be handled

D. can do anti-fraud protection

E. can protect IDC outside Alibaba Cloud

ANSWER: A B E

Explanation:

Anti-DDoS Pro provides stronger attack-defense capability than the basic service because it is a paid, enhanced DDoS-mitigation offering designed for business workloads that need more comprehensive and resilient protection. It provides substantially greater mitigation capacity and more advanced protection resources than the baseline protection included with Alibaba Cloud services.

Elastic protection bandwidth is also an advantage. Anti-DDoS Pro supports configurable protection plans and the ability to adjust protection capacity as business exposure and attack risks change. This helps an organization match its protection level to its operational requirements rather than relying only on the fixed baseline capability of Anti-DDoS Basic.

Anti-DDoS Pro can protect IDC outside Alibaba Cloud because it supports protection for Internet-facing assets deployed outside Alibaba Cloud, including on-premises data centers and workloads in other cloud environments, through its relevant routing and forwarding deployment models. This makes it suitable for hybrid and multi-cloud architectures that require centralized DDoS protection. Alibaba Cloud describes Anti-DDoS Pro as an enhanced service for defending against large-scale DDoS attacks and documents protection configurations for both Alibaba Cloud and non-Alibaba Cloud resources. See Alibaba Cloud: What is Anti-DDoS Pro? and Alibaba Cloud: Anti-DDoS Pro documentation.

QUESTION NO: 9

Which of the following logs can be accessed through ECS logs provided by Alibaba Cloud?

(the number of correct answers: 2)

A. OS system log

B. Application log

C. Hypervisor log

D. Cloud platform log

ANSWER: A B

Explanation:

“OS system log” and “Application log” are the correct selections. Alibaba Cloud Elastic Compute Service instances generate operating-system-level records, such as Linux syslog, authentication, kernel, and service logs, which are stored within the instance operating system. Applications running on an ECS instance likewise create their own records, including access logs, error logs, transaction logs, and custom business logs. These files can be collected from ECS instances and centrally queried, analyzed, alerted on, or delivered by using Alibaba Cloud Simple Log Service (SLS). In practice, the Logtail collection agent is installed or configured on the ECS instance and reads designated log files or container output, allowing both system and application log data to be sent to a Logstore. This makes ECS-based log collection useful for operational troubleshooting, availability monitoring, audit investigations, and security analysis. Alibaba Cloud documents Logtail as the agent used to collect logs from servers, including ECS instances, and documents the procedures for configuring file-based log collection. See the Logtail overview and collecting text logs from servers documentation.

QUESTION NO: 10

Which of the following statements about cloud security shared responsibilities model are true? (the

number of correct answers: 2)

A. for users who is using IAAS service, they should be responsible for their business system which is on top of cloud infrastructure

B. cloud service provider should guarantee the security of all physical infrastructure

C. the damage caused by attacks leveraging security vulnerability in customers' application server should be charged to cloud service provider

D. cloud user should also take care of some of the hardware maintenance and operation work

ANSWER: A B

Explanation:

In the cloud shared-responsibility model, security duties are divided according to the service layer being consumed. For an infrastructure-as-a-service deployment, the cloud customer remains responsible for the workloads and business systems deployed on the cloud resources. This includes such customer-controlled areas as application security, operating-system configuration and patching, identity and access permissions, workload data, and appropriate network controls. The statement that users of infrastructure-as-a-service offerings are responsible for the business systems on top of cloud infrastructure therefore correctly describes the customer side of the model.

The cloud service provider is responsible for securing the underlying cloud environment, including the physical data centers and the physical infrastructure that delivers the service. This foundation includes facilities, hardware, and the core infrastructure layers operated by the provider. Alibaba Cloud describes its security and compliance commitments through its Trust Center and explains that customers must also apply security controls appropriate to the services and resources they configure. See the Alibaba Cloud Trust Center and Alibaba Cloud ECS security group documentation.

QUESTION NO: 11

Which of following elements are included in a TCP/IP based route table (the number of

correct answers: 3)

A. Network Destination

B. Netmask

C. Mac Address

D. Gateway IP

E. Port

ANSWER: A B D

Explanation:

A TCP/IP route table uses routing information to determine where packets should be forwarded. **Network Destination** identifies the target network or host to which a route applies. It is commonly represented as a destination IP network, such as `192.168.1.0`, and is evaluated together with the netmask or prefix length. **Netmask** specifies which portion of the destination address is the network prefix, thereby defining the range of addresses matched by that route. This enables the routing system to select the most specific applicable route for a packet's destination.

Gateway IP identifies the next-hop router to which traffic is sent when the target network is reached through another device. A route can therefore combine a destination network, a netmask, and a gateway to state: for packets matching this network prefix, forward them to this next-hop IP address. In cloud networking, the same underlying concepts are represented by a destination CIDR block and a next hop in a route entry. Alibaba Cloud VPC route tables similarly define route entries with a destination CIDR block and next-hop information. See Alibaba Cloud VPC route tables documentation and Microsoft route command documentation.

QUESTION NO: 12

Which of the following statements are true to describe a SQL attack commonly used pattern? (the number of correct answers: 3)

A. Adding more search request together with the original one

B. adding an absolute true condition to bypass original request

C. use incorrect SQL function

D. use selfmade variable

E. adding ";" or "--" to change the original request purpose with new request attached

ANSWER: A B E

Explanation:

SQL injection commonly exploits application code that concatenates untrusted input into a database query. "Adding more search request together with the original one" describes appending a query component, commonly through a UNION-based payload, so that the database returns data selected by the injected portion in addition to the intended search results. "adding an absolute true condition to bypass original request" describes a tautology attack, in which an always-true predicate changes the query's filtering or authentication logic. For example, an injected condition that always evaluates to true can cause a WHERE clause to match unintended rows.

"adding ";" or "--" to change the original request purpose with new request attached" also reflects established injection syntax. SQL comment markers such as `--` can cause the database to ignore the remaining intended query text, and statement separators such as `;`, where the database driver and configuration permit them, can be used for stacked-query

injection. These patterns are precisely why applications should use parameterized queries and why web application firewalls inspect requests for SQL-injection signatures and anomalous query syntax. See the OWASP SQL Injection guidance and Alibaba Cloud's WAF protection rules overview.

QUESTION NO: 13

Which of the following 2 security risks are not included in OWASP published 2017 Top 10

Web

Application Security Risks

A. Cross-Site Request Forgery(CSRF)

B. Cross-Site Scripting(XSS)

C. Unvalidated Redirects and Forwards

D. Injection

ANSWER: A C

Explanation:

Cross-Site Request Forgery(CSRF) and Unvalidated Redirects and Forwards are the two risks not included as individual categories in the OWASP Top 10: 2017. Both appeared in the OWASP Top 10: 2013, but OWASP revised the list for the 2017 edition based on its data collection and risk-ranking methodology. The 2017 list included categories such as Injection and Cross-Site Scripting(XSS), but did not retain Cross-Site Request Forgery(CSRF) or Unvalidated Redirects and Forwards as standalone Top 10 entries.

CSRF remains an important application-security concern: an attacker can cause a victim's authenticated browser to submit an unintended request to a trusted application. Likewise, unsafe redirects or forwards can still enable phishing, credential theft, or access-control bypass scenarios when applications accept untrusted destination values. Their omission from the 2017 Top 10 therefore does not mean they are no longer security issues; it means they were not separate risks in that specific OWASP edition. The OWASP 2017 archive lists the ten categories and provides the historical context for this version of the project. See the OWASP Top 10: 2017 archive and OWASP's CSRF attack reference.

QUESTION NO: 14

Which of the IP addresses are private IP addresses? (Correct Answers: 2)

A. 192.169.1.1

B. 172.16.58.14

C. 10.44.10.45

D. 8.8.8.8

ANSWER: B C

Explanation:

`172.16.58.14` and `10.44.10.45` are private IPv4 addresses because each falls within an address block reserved by RFC 1918 for use inside private networks. The RFC 1918 private ranges are `10.0.0.0/8`, covering addresses from `10.0.0.0` through `10.255.255.255`; `172.16.0.0/12`, covering `172.16.0.0` through `172.31.255.255`; and `192.168.0.0/16`. Therefore, `10.44.10.45` belongs to the first range, while `172.16.58.14` belongs to the second range.

Private addresses are intended for internal communication, such as within an Alibaba Cloud VPC, and are not globally routed on the public Internet. A VPC can use private IPv4 CIDR blocks to assign internal addresses to ECS instances and other resources; Internet access generally requires a public IP address, EIP, or network address translation configuration. The authoritative definition of these private-use ranges is RFC 1918, available through the RFC Editor. Alibaba Cloud's VPC documentation also describes VPC private CIDR block planning and use: Create and manage a VPC.

QUESTION NO: 15

Which of the following methods can't be used against CC attack?

A. use WAF

B. change HTTP service to HTTPS service

C. resolve domain name to a disguised IP

D. change the service providing port

ANSWER: B

Explanation:

Changing an HTTP service to an HTTPS service cannot, by itself, defend against a CC (Challenge Collapsar) attack. A CC attack is an application-layer HTTP flood in which the attacker repeatedly requests web pages, URLs, or resource-intensive application functions. The attack traffic can use normal-looking, valid HTTP requests; HTTPS merely carries those same requests over an encrypted TLS connection. Encryption protects confidentiality and integrity while data is in transit, but it does not determine whether a request is legitimate, limit request frequency, distinguish automated clients, or prevent application resources from being exhausted.

In fact, HTTPS endpoints can still be targeted with high volumes of TLS and HTTPS requests. Effective CC mitigation requires application-aware inspection and traffic controls, such as request-rate controls, bot management, challenge or verification mechanisms, IP or session reputation, and custom protection rules. Alibaba Cloud Web Application Firewall provides protection capabilities for HTTP flood and web-application attacks, including rule-based controls that can identify and handle abnormal request behavior. Therefore, converting the transport protocol from HTTP to HTTPS is valuable security hygiene, but it is not a standalone anti-CC measure. See Alibaba Cloud's Web Application Firewall overview and WAF protection documentation.

QUESTION NO: 16

In Windows OS you can turn off a service through: Score 2

A. Control Panel → Administrative Tools → Services, then stop the running service

B. Control Panel->windows update->Stop

C. Create new firewall rule to stop service

D. Delete administrator role and related accounts

ANSWER: A

Explanation:

"Control Panel → Administrative Tools → Services, then stop the running service" is correct because Windows services are managed through the Services management console. This console displays installed services, their current state, startup configuration, and recovery settings. An administrator can select a running service and use the Stop command to terminate that service's active process in a controlled manner. The same interface can be used to prevent a service from automatically restarting after reboot by changing its startup type when that is operationally appropriate.

Access to service management normally requires administrative privileges, which is important on cloud-hosted Windows instances as well as on physical servers. Stopping unnecessary services is a common system-hardening practice because it

reduces the number of active processes and potentially exposed network listeners. Administrators should first confirm that the service is not required by the operating system, applications, monitoring agents, or business workloads before stopping it. Microsoft documents service administration through the Services console and related service-control tools at sc stop and provides an overview of Windows service concepts at About Services.

QUESTION NO: 17

User A rented 2 ECS server and one RDS in Alibaba Cloud to setup his company public

website. After the web site will become available online, the security risks he/she will face

will include: (the number of correct answers: 3)

A. physical cable is cut by someone

B. ECS admin password is hacked

C. website codes has some vulnerability

D. RDS DB got unknown remote logon

E. the disk in ECS is broken

ANSWER: B C D

Explanation:

"ECS admin password is hacked," "website codes has some vulnerability," and "RDS DB got unknown remote logon" are direct security risks for an internet-facing website deployment. Compromise of an ECS administrator credential can give an attacker privileged control of the web server, allowing changes to application files, installation of malicious software, or access to data and credentials stored on the instance. Strong passwords, multi-factor authentication where available, least-privilege RAM access, and monitoring of unusual logon activity help reduce this exposure.

Application-code vulnerabilities are also a primary risk once a site is public. Common weaknesses such as injection flaws, insecure authentication, or unsafe file handling can be exploited through the website itself. Secure development, prompt patching, vulnerability scanning, and web application protections should be part of the operating process.

An unknown remote database logon indicates possible unauthorized access to data. RDS access should be restricted through IP allowlists, tightly scoped accounts and permissions, secure credential management, and encryption in transit. Alibaba Cloud Security Center helps identify threats and vulnerabilities on cloud assets, while ECS security controls can restrict network exposure. See Alibaba Cloud Security Center overview and ECS security group overview.