DUMPSARENA

# ACP Cloud Security Professional

## Alibaba Cloud ACP-Sec1

**Version Demo**

**Total Demo Questions: 11**

**Total Premium Questions: 111**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Security Compliance | 5 |
| Topic 2, Identity and Access Management | 5 |
| Topic 3, Network Security | 26 |
| Topic 4, Host Security | 18 |
| Topic 5, Application Security | 24 |
| Topic 6, Data Security | 8 |
| Topic 7, Security Operations | 23 |
| Topic 8, Mix Questions | 2 |
| Total | 111 |

QUESTION NO: 1

You have helped a customer set up a content filtering solution based on Content Moderation service However, the customer is complaining that certain images are getting incorrectly flagged as pornographic content. What can you do to help fix this?

**A.** Create an "Image Library" from the Content Moderation console and add the images to the Image Library's whitelist

**B.** Ask your customer to use different images on their site

**C.** Modify the images until Content Moderation service starts marking them as pornographic.

**D.** Open a ticket with Alibaba Cloud support, and send them a copy of the images, so that they can tune Content Moderation's detection algorithms

**ANSWER: A**

**Explanation:**

Create an "Image Library" from the Content Moderation console and add the images to the Image Library's whitelist. An image whitelist is intended for known, approved images that may otherwise produce a moderation result inconsistent with the customer's business context. After the customer adds these images to a whitelist image library and associates that library with the applicable image moderation configuration or request, Content Moderation can recognize the approved content and return the whitelist-related result rather than treating it as a normal suspected pornographic image.

This is especially useful for recurring false positives, such as legitimate product photographs, artwork, marketing assets, or images with visual characteristics that resemble sensitive content to a general-purpose detection model. The customer should add the exact approved images, keep the library under appropriate governance, and use it only for content that has been manually reviewed and authorized. Whitelisting provides a targeted business-policy control without requiring changes to the underlying detection model. Alibaba Cloud documents image libraries as a mechanism for managing custom blacklists and whitelists in Content Moderation; see the Content Moderation overview and the Alibaba Cloud Content Moderation product page.

**QUESTION NO: 2**

Alibaba Cloud CloudMonitor is a service that monitors Alibaba Cloud resources and

Internet applications Which of the following functions are currently provided by

CloudMonitor? (Number of correct answers: 4)

**A.** Custom firewall

**B.** Alerting

**C.** Site monitoring

**D.** Cloud service monitoring

**E.** Custom monitoring

**ANSWER: B C D E**

**Explanation:**

CloudMonitor provides alerting, site monitoring, cloud service monitoring, and custom monitoring. Alerting enables users to create alarm rules for monitored metrics and to receive notifications through configured alert contacts or notification methods when rule conditions are met. Cloud service monitoring supplies predefined monitoring metrics for Alibaba Cloud services and resources, helping users observe resource health, utilization, and operational status. Custom monitoring lets applications publish custom metrics to CloudMonitor, so business-specific indicators can be visualized and used in alarm rules. Site monitoring performs availability and performance checks from monitoring points for Internet-facing sites and services, including checks such as HTTP, HTTPS, TCP, ICMP, and DNS where supported. Together, these capabilities cover infrastructure metrics, application-defined metrics, external availability checks, and actionable alarm notifications.

Alibaba Cloud documents these features in its CloudMonitor overview and describes how alarm rules evaluate metric conditions and issue alerts. See the CloudMonitor overview and the alarm rule documentation.

## QUESTION NO: 3

A website is built using open-source software To prevent hacker attacks and fix vulnerabilities in a timely manner, the administrator of the website wants to use the patch management feature in Security Center. Which of the following statements about patch management is FALSE.

**A.** Before patches for most common Web vulnerabilities are released, the Alibaba Cloud Security O&M team will have fixed the vulnerabilities using self-developed patches

**B.** Rollback of Web vulnerabilities means to restore the original files, while rollback of Windows vulnerabilities means to uninstall the patch upgrade

**C.** Patch management can operate machines in batches in the cloud. For large-scale vulnerabilities, it supports one-key patch upgrade, which is easy and convenient

**D.** Vulnerabilities are automatically fixed Once a self-developed paten is released, it automatically fixes vulnerabilities for all customers who have enabled patch management.

## ANSWER: D

**Explanation:**

“Vulnerabilities are automatically fixed Once a self-developed paten is released, it automatically fixes vulnerabilities for all customers who have enabled patch management.” is the false statement. Enabling Security Center patch management does not by itself authorize an unconditional, platform-wide repair of every detected vulnerability on every customer server. Vulnerability remediation is performed against the affected assets and is governed by the repair method, vulnerability type, applicable operating system or software, and the customer’s selected remediation or automatic-fixing configuration. For example, fixing may require the administrator to initiate a repair task, select servers, or configure automatic fixing for eligible vulnerabilities. A patch can also require a restart, depend on a particular software version, or be unavailable for an asset because the vulnerability is not patchable by the supported method. Security Center’s self-developed hot patches are intended to provide protection or remediation for supported web vulnerabilities, but their release does not mean that all customers who merely enabled patch management are automatically fixed without applicable configuration and scope. Alibaba Cloud documents vulnerability remediation as an asset-oriented operation and provides settings for automatic vulnerability fixing rather than describing it as a universal automatic action for all customers. See the Security Center vulnerability-fixing documentation and vulnerability fix settings documentation.

## QUESTION NO: 4

Alibaba Cloud ECS instances are common targets of hacker attacks. There are many types of attacks against ECS instances. Which of the following attacks specifically target the operating system of an ECS instance? (Number of correct answers: 3)

**A.** SQL injection

**B.** Trojan or Webshell installation

**C.** Brute force RDP password cracking

**D.** Brute force SSH password cracking

## ANSWER: B C D

**Explanation:**

“Trojan or Webshell installation,” “Brute force RDP password cracking,” and “Brute force SSH password cracking” are attacks directed at the host operating system and its administrative access surface. A Trojan is malicious software executed on the instance, while a Webshell provides an attacker with persistent remote command execution on the server after it is

placed and run. Both can lead to host takeover, privilege escalation, persistence, or theft of data stored or processed by the ECS instance.

RDP and SSH are remote-management protocols exposed by Windows and Linux ECS instances, respectively. Repeated password-guessing attempts against these services target the operating system's authentication mechanism. If successful, the attacker can sign in as a system user and operate within that user's permissions, making strong credentials, key-based SSH authentication, multi-factor protections where applicable, and restrictive security-group rules essential controls. Alibaba Cloud recommends limiting remote access sources and strengthening account security for ECS instances. Security Center can also identify threats and suspicious behavior affecting cloud hosts. See ECS security best practices and the Alibaba Cloud Security Center overview.

## QUESTION NO: 5

Anti-DDoS is one of the major products of Alibaba Cloud Security service Many websites have suffered DDoS attacks of different types. Therefore, accurate understanding of DDoS attacks is critical to the website security protection. Which of the following statements about

DDoS attacks is the MOST accurate?

**A.** The main purpose of a DDoS attack is to prevent the target server from providing normal services

**B.** A DDoS attack cracks the servers logon password by means of numerous attempts

**C.** The purpose of a DDoS attack is to steal confidential information

**D.** DDoS attacks primarily target a database

## ANSWER: A

**Explanation:**

The main purpose of a DDoS attack is to prevent the target server from providing normal services. A distributed denial-of-service attack attempts to exhaust or overwhelm a target's available resources, such as network bandwidth, connection capacity, processing power, or application-handling capacity. Attackers generate traffic or requests from many distributed sources, often using compromised devices, so that legitimate users cannot reliably reach the website, application, or other online service. The defining security impact is loss of availability: services may become slow, intermittently unreachable, or completely unavailable while the attack continues. This is why DDoS protection focuses on detecting abnormal traffic patterns, absorbing large traffic volumes, filtering malicious requests, and forwarding clean traffic to the protected service. Alibaba Cloud describes Anti-DDoS services as protections designed to mitigate DDoS attacks and help maintain service availability during volumetric or resource-exhaustion events. Understanding availability as the primary objective is essential when selecting protections, setting mitigation capacity, and preparing incident-response procedures for internet-facing workloads. See the Alibaba Cloud Anti-DDoS Basic overview and the CISA DDoS guidance.

## QUESTION NO: 6

When submitting requests to the Content Moderation service API, which HTTP method should you use?

**A.** HEAD

**B.** PUT

**C.** GET

**D.** POST

## ANSWER: D

**Explanation:**

The correct method is **POST**. Alibaba Cloud Content Moderation API operations are invoked by sending request parameters in a POST request to the relevant service endpoint. This suits moderation workloads because a request commonly contains

structured input, such as text to inspect, an image URL, an OSS object reference, or callback and moderation configuration. POST permits these parameters to be included in the request body, avoiding practical URL-length limitations and allowing the API to receive the complete payload required to create a moderation task or perform synchronous moderation.

For example, Content Moderation API documentation describes submitting API requests with POST and provides request examples that use a POST method together with the required common parameters, action name, version, and service-specific parameters. The API request format also requires signing the request under Alibaba Cloud's RPC-style API conventions, with the request sent to the Content Moderation endpoint. Using POST ensures the request follows the protocol expected by the service and that submitted content is processed correctly. See the Content Moderation API overview and the Alibaba Cloud API calling guidance.

## QUESTION NO: 7

There is a limit on the number of Customer Master Keys (CMKs) that users can create

using Key Management Service (KMS), but users can raise this limit by submitting a support ticket to Alibaba Cloud.

**A.** True

**B.** False

## ANSWER: A

**Explanation:**

**True** is correct. Alibaba Cloud Key Management Service applies quotas to customer-managed keys, historically referred to as Customer Master Keys (CMKs), to ensure that KMS resources are managed predictably within an Alibaba Cloud account and region. The number of keys that can be created is therefore not unlimited. When an organization's legitimate operational requirements exceed the default key quota—for example, because it separates encryption keys by application, environment, tenant, or data classification—it can request a quota increase through Alibaba Cloud support. The request can be evaluated and processed by Alibaba Cloud based on the account and service requirements. This approach lets customers retain the benefits of isolated key management designs without treating the initial service quota as a fixed, permanent ceiling. Teams should monitor their KMS key usage and plan quota requests before onboarding workloads that require substantial numbers of independently managed keys. Alibaba Cloud documents KMS usage limits and quota-related information in its KMS limits documentation. The general process for requesting adjustments to applicable cloud-service quotas is also described in the Alibaba Cloud quota management documentation.

## QUESTION NO: 8

Products like ECS and Server Load Balancer it will be automatically protected by Anti-

DDoS Basic service

**A.** True

**B.** False

## ANSWER: A

**Explanation:**

**True** is correct. Anti-DDoS Basic is Alibaba Cloud's foundational, no-additional-charge DDoS mitigation service and is automatically provided for eligible Alibaba Cloud assets, including Elastic Compute Service instances and Server Load Balancer instances. This automatic coverage is intended to provide baseline protection for public-facing cloud resources without requiring the customer to separately purchase or manually deploy a protection instance first.

The service monitors traffic to supported asset IP addresses and, when an attack is identified, applies Alibaba Cloud's basic scrubbing and mitigation capabilities to help preserve service availability. Protection is associated with the relevant cloud resource and its public IP configuration, so customers should still ensure that their internet-facing services are correctly configured and remain within the service's supported protection scope and capacity. For workloads that require stronger

defenses, more extensive mitigation capacity, or advanced operational controls, Alibaba Cloud offers higher-tier Anti-DDoS services; however, that does not change the automatic baseline coverage supplied by Anti-DDoS Basic for supported ECS and Server Load Balancer resources.

Alibaba Cloud documents the service and its automatically protected asset types in its Anti-DDoS Basic overview and provides further operational guidance in the Anti-DDoS Basic documentation.

## QUESTION NO: 9

Which of the following measures can help protect an Alibaba Cloud account from credential compromise? (Number of correct answers: 3)

**A.** Enable MFA for the Alibaba Cloud account

**B.** Use RAM users or RAM roles for daily operations

**C.** Review and disable unnecessary AccessKey pairs

**D.** Share the Alibaba Cloud account password among administrators

**E.** Store AccessKey pairs in public source code repositories

## ANSWER: A B C

**Explanation:**

**Enabling MFA for the Alibaba Cloud account**, **using RAM users or RAM roles for daily operations**, and **regularly reviewing and disabling unnecessary AccessKey pairs** are correct. MFA reduces the likelihood that a stolen password alone can be used to sign on. Daily work should use identities with only the required permissions instead of the highly privileged Alibaba Cloud account.

AccessKey pairs are long-term credentials that must be protected and reviewed. Unused or exposed keys should be disabled or deleted promptly. Sharing account credentials or embedding AccessKeys in public code repositories can lead directly to unauthorized use of cloud resources. For more information, see the RAM security best practices.

## QUESTION NO: 10

Alibaba Cloud WAF identifies attacks using human/robot detection, Big Data analysis, model analysis, and other related techniques. Which of the following CC attack defense modes does WAF provide to meet the protection requirements of users? (Number of correct answers 2)

**A.** Threat

**B.** Exception

**C.** Attack emergency

**D.** Normal

## ANSWER: C D

**Explanation:**

Alibaba Cloud WAF provides the **Normal** and **Attack emergency** CC attack-defense modes to accommodate different traffic-risk conditions and protection requirements. Normal mode is intended for routine website operation, applying CC protection with a balanced policy that helps identify and mitigate malicious high-frequency requests while reducing the likelihood of affecting legitimate visitors. It is suitable when traffic patterns are generally stable and the service requires standard, continuous protection.

Attack emergency mode is intended for circumstances in which a website is experiencing, or is at immediate risk of, a substantial CC attack. This mode uses more forceful protective controls to rapidly limit suspicious automated or high-

frequency access and preserve the availability of protected web services. The ability to select an emergency-oriented mode is important because CC attacks can quickly exhaust application resources even when they do not resemble traditional network-layer denial-of-service attacks. Together, these modes allow an organization to use an appropriate protection posture during normal operations and escalate defenses when attack pressure rises. Alibaba Cloud documents CC protection as part of WAF's basic web-attack protection capabilities; see Configure the basic protection rule and the Web Application Firewall documentation.

## QUESTION NO: 11

When importing key material into Key Management Service (KMS), you will be given an import token and public encryption key valid for 24 hours. The public key KMS provides must be used to encrypt your key material before upload KMS allows you to choose different public key encryption algorithms Which ones are supported? (Number of correct answers; 3)

**A.** RSAES_OAEP_SHA_1

**B.** RSAES_ECDHE_V1 _5

**C.** RSAES_OAEP_SHA_256

**D.** RSAES PKCS1 V1 5

## ANSWER: A C D

**Explanation:**

Alibaba Cloud KMS supports the three RSA encryption schemes named **RSAES_OAEP_SHA_1**, **RSAES_OAEP_SHA_256**, and **RSAES PKCS1 V1 5** for protecting externally generated key material before it is imported. KMS returns an import token together with a wrapping public key through the import-parameter workflow. The customer uses that public key and one of the supported RSA schemes to encrypt the plaintext key material locally, then submits the encrypted result and import token to KMS. This design ensures that the plaintext key material is not exposed during transmission to the service.

The selected scheme must match the encryption operation performed locally. RSAES_OAEP_SHA_1 uses OAEP padding with SHA-1, RSAES_OAEP_SHA_256 uses OAEP padding with SHA-256, and RSAES PKCS1 V1 5 uses PKCS#1 v1.5 encryption padding. The KMS import-parameter API documents the public key and import token used in this process, while the KMS key-material import documentation describes the supported wrapping algorithms and import workflow. See GetParametersForImport API reference and Import key material.