

[Q98-Q122 Verified 1z0-1104-23 dumps Q&As - Pass Guarantee or Full Refund [Feb-2024]



Verified 1z0-1104-23 dumps Q&As - Pass Guarantee or Full Refund [Feb-2024]

1z0-1104-23 PDF Dumps | Feb 13, 2024 Recently Updated Questions

Oracle 1z0-1104-23 Exam Syllabus Topics:

TopicDetailsTopic 1- Create and configure Web Application Firewall- Implement security monitoring and alertingTopic 2- Describe key capabilities provided by Data Safe- Describe the use case for auditing and review OCI Audit LogsTopic 3- Configure and secure load balancers to ensure high availability- Design a scalable authorization model with users, groups, and policiesTopic 4- Implement conditional and advanced policies- Configure Dynamic Groups, Network Sources, and Tag-Based Access ControlTopic 5- Configure, deploy and maintain OCI Certificates- Implement Network, Platform, and Infrastructure SecurityTopic 6- Use threat intelligence to identify rogue users- Configure security for OCI storage services

NO.98 Which type of software do you use to centrally distributeand monitor the patch level of systems throughout the enterprise?

- * Network Monitor software
- * Web Application Firewall
- * Patch Management software

* Recovery Manager software

https://docs.oracle.com/cd/E11857_01/em.111/e18710/T531901T535649.htm

NO.99 Which three Oracle Cloud Infrastructure (OCI) services are covered by Cloud Guard? (Choose three.)

- * Oracle Integration Osud (OIC)
- * Blockchain
- * Object Storage
- * Database Cloud Service
- * Identity and Access Management (IAM)

NO.100 Challenge 4 – Task 3 of 6

Configure Web Application Firewall to Protect Web Server Against XSS Attack Scenario You have to protect web applications hosted on OCI from cross-site scripting (XSS) attacks. You can use the OCI Web Application Firewall (WAF) capabilities to create rules that compare against incoming requests to determine if the request contains an XSS attack payload. If a request is determined to be an attack, WAF should return the HTTP Service Unavailable (503) error.

To ensure that the configured WAF blocks the XSS attack, run the following script: [http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”](http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”>) To complete this deployment, you have to perform the following tasks in the environment provisioned for you:

Configure a Virtual Cloud Network (VCN)

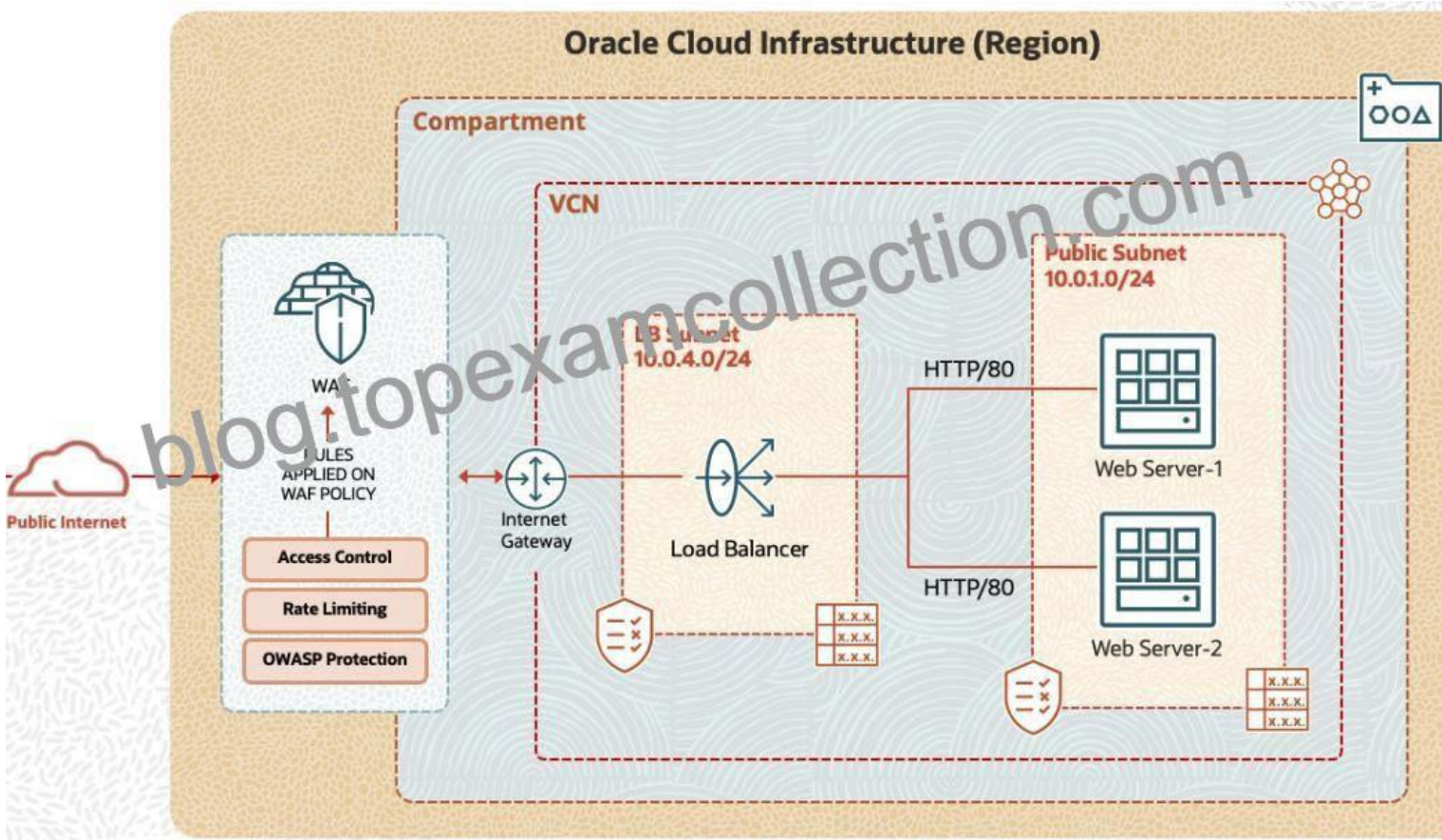
Create a Compute Instance and install the Web Server

Create a Load Balancer and update Security List

Create a WAF policy

Configure Protection Rules against XSS attacks

Verify the created environment against XSS attacks



Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99233424-C01 and Region us-ashburn-1.

Complete the following task in the provisioned OCI environment:

Go to the VCN IAD-WAF-PBT-VCN-01.

Create a Security List with the name IAD-SP-PBT-LB-SL-01.

Create a Public subnet named LB-Subnet-IAD-SP-PBT-SNET-02 and attach the above-created security list.

Create a Load Balancer with the name IAD-SP-PBT-LB-01.

Create a Listener Name with the name IAD_SP_PBT_LB_LISN_01.

Add appropriate Ingress and Egress rules to IAD-SP-PBT-LB-SL-01, to allow http traffic to the Load Balancer subnet.
See the solution below in Explanation

Explanation:

SOLUTION:

From the navigation menu, select Networking and then click Virtual Cloud Network.

In the left navigation pane, under List Scope, select <your assigned compartment> from the drop-down menu.

Click IAD-WAF-PBT-VCN-01 from the list of VCNs.

In the left navigation pane, under Resources, click Security Lists.

Click Create Security List.

In the Create Security List dialogue box, enter the following: a) Name: IAD-SP-PBT-LB-SL-01 b) Do not add any ingress or egress rules. c) Click Create Security List.

In the left navigation pane, under Resources, click Subnets.

Click Create Subnet.

In the Create Subnet dialogue box, enter the following: a) Name: LB-Subnet-IAD-SP-PBT-SNET-02 b) Create in Compartment: <your working compartment name> c) Subnet Type: Regional d) IPv4 CIDR Block: 10.0.4.0/24 e) Security List: From the drop-down menu, select the Security List you had created earlier, IAD-SP-PBT-LB-SL-01.

Click Create Subnet.

You now see that the subnet has been created successfully.

Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99233424-C01 and Region us-ashburn-1.

NO.101 Which OCI service can index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor data?

- * Data Guard
- * Data Safe
- * WAF
- * Logging Analytics

About Logging Analytics

Oracle Cloud Logging Analytics is a cloud solution in Oracle Cloud Infrastructure that lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor all log data from your applications and system infrastructure on cloud or on-premises.

NO.102 A number of malicious requests for a web application is coming from a set of IP addresses originating from Antarctica.

Which of the following statement will help to reduce these types of unauthorized requests ?

- * Delete NAT Gateway from Virtual Cloud Network
- * Use WAF policy using Access Control Rules
- * List specific set of IP addresses then deny rules in Virtual Cloud Network Security Lists
- * Change your home region in which your resources are currently deployed

Explanation

A Web Application Firewall (WAF) policy can help protect your web application from malicious requests³. Access Control Rules in a WAF policy can be used to allow, block, or count requests from specific IP addresses or CIDR blocks³. This can be particularly

useful when you're seeing a number of malicious requests coming from a specific set of IP addresses. By setting up appropriate Access Control Rules, you can effectively reduce these types of unauthorized requests.

NO.103 Which type of firewalls are designed to protect against web application attacks, such as SQL injection and cross-site scripting?

- * Stateful inspection firewall
- * Web Application Firewall
- * Incident firewall
- * Packet filtering firewall

Explanation

SQL injections. Cross-site scripting. Distributed denial of service(DDoS) attacks. Botnets. These are just some of the cyber-weapons increasingly being used by malicious actors to target web applications, cause data breaches, and expose sensitive business information.

Oracle WAF uses a multilayered approach to protect web applications from a host of cyberthreats including malicious bots, application layer (L7) DDoS attacks, cross-site scripting, SQL injection, and vulnerabilities defined by the Open Web Application Security Project (OWASP). When a threat is identified, Oracle WAF automatically blocks it and alerts security operations teams so they can investigate further.

<https://www.oracle.com/a/ocom/docs/security/oci-web-application-firewall.pdf>

NO.104 Which Oracle Data Safe feature enables the internal test, development, and analytics teams to operate effectively while minimizing their exposure to sensitive data? (Choose the best Answer.)

- * Data encryption
- * Data Auditing
- * Data masking
- * Data discovery
- * Security assessment

NO.105 You want to make API calls against other OCI services from your instance without configuring user credentials. How would you achieve this?

- * Create a dynamic group and add a policy.
- * Create a dynamic group and add your instance.
- * Create a group and add a policy.
- * No configuration is required for making API calls.

DYNAMIC GROUP

Dynamic groups allow you to group Oracle Cloud Infrastructure instances as principal actors, similar to user groups. You can then create policies to permit instances in these groups to make API calls against Oracle Cloud Infrastructure services. Membership in the group is determined by a set of criteria you define, called matching

rules. <https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/calling-services-from-instances.htm>

NO.106 What is the minimum active storage duration for logs used by Logging Analytics to be archived?

- * 60 days
- * 10 days
- * 30 days
- * 15 days

[https://docs.oracle.com/en-us/iaas/logging-analytics/doc/manage-storage.html#:~:text=The%20minimum%20Active Storage Duration \(Days\) for logs before they can be archived is 30 days.](https://docs.oracle.com/en-us/iaas/logging-analytics/doc/manage-storage.html#:~:text=The%20minimum%20Active Storage Duration (Days) for logs before they can be archived is 30 days.)


NO.107 Bot Management in OCI provides which of the features? Select TWO correct answers.

- * Bad Bot Denylist
- * CAPTCHA Challenge
- * IP Prefix Steering
- * Good Bot Allowlist

Bot Management

Bot Management enables you to mitigate undesired bot traffic from your site using CAPTCHA and JavaScript detection tools while enabling known published bot providers to bypass these controls.

Non-human traffic makes up most of the traffic to sites. Bot Manager is designed to detect and block, or otherwise direct, non-human traffic that can interfere with site operations. The Bot Manager features mitigate bots that conduct content and price scraping, vulnerability scanning, comment spam, brute force attacks, and application layer DDoS attacks. You can also manage the good bot whitelist.

 Caution

When you enable Bot Management, you incur a higher rate on requests to the WAF.

See these topics for more information about Bot Management:

- [JavaScript Challenge](#)
- [Human Interaction Challenge](#)
- [Device Fingerprint Challenge](#)
- [CAPTCHA Challenge](#)
- [Good Bot Allowlist](#)

NO.108 You want software that can automatically collect and aggregate log data generated throughout your organization's infrastructure, analyze it, and send alerts if it detects a deviation from the norm.

Which software must you use?

- * Security Information Management (SIM)
- * SecurityEvent Management (SEM)
- * Security Integration Management (SIM)
- * Security Information and Event Management (SIEM)

Explanation

SIEM software can automatically collect and aggregate log data generated throughout your organization's infrastructure, analyze it, and send alerts if it detects a deviation from the norm.

NO.109 Challenge 4 & Task 5 of 6

Configure Web Application Firewall to Protect Web Server Against XSS Attack Scenario You have to protect web applications hosted on OCI from cross-site scripting (XSS) attacks. You can use the OCI Web Application Firewall (WAF) capabilities to create rules that compare against incoming requests to determine if the request contains an XSS attack payload. If a request is determined to be an attack, WAF should return the HTTP Service Unavailable (503) error.

To ensure that the configured WAF blocks the XSS attack, run the following script: [http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”](http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”>) To complete this deployment, you have to perform the following tasks in the environment provisioned for you:

Configure a Virtual Cloud Network (VCN)

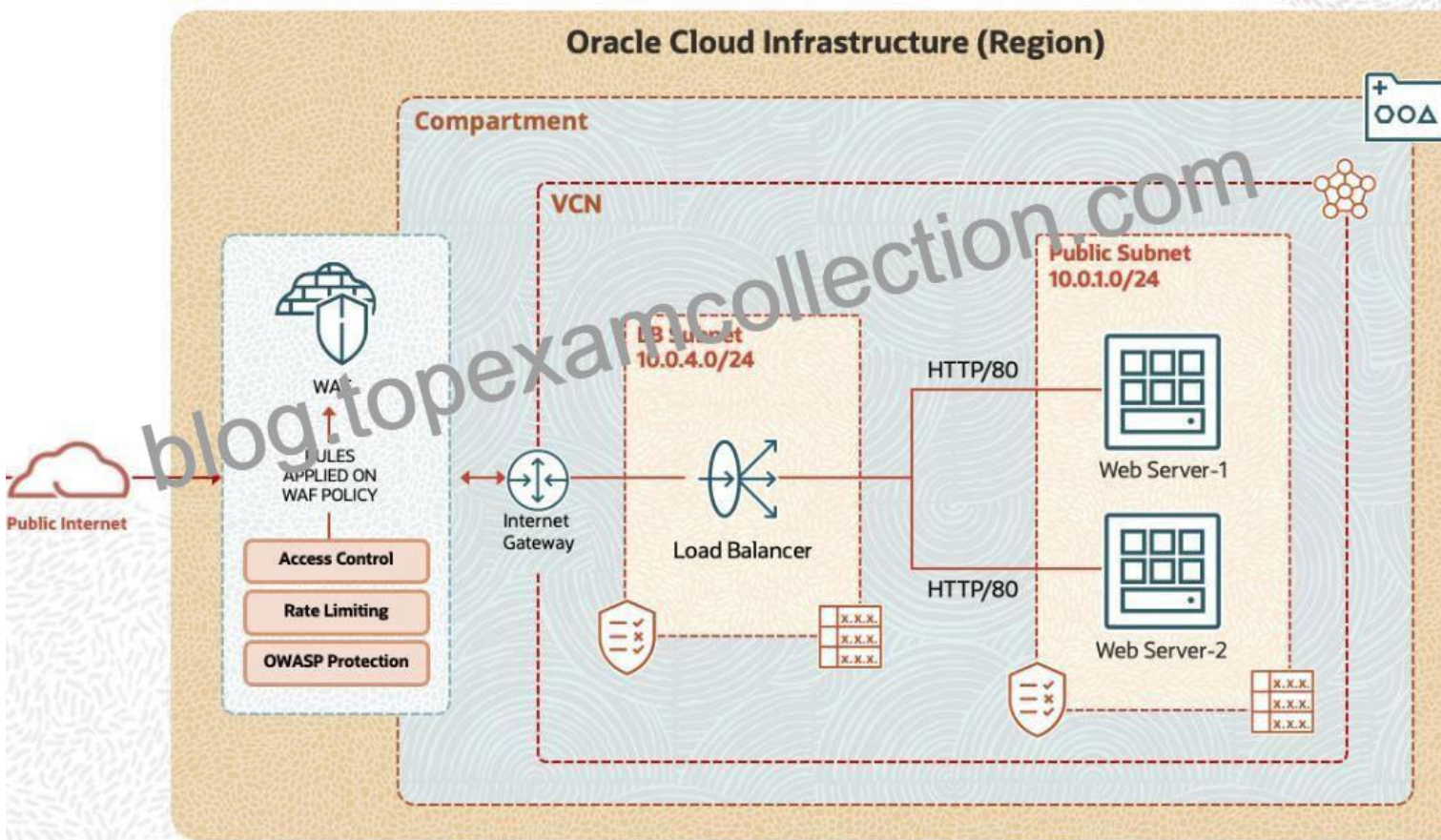
Create a Compute Instance and install the Web Server

Create a Load Balancer and update Security List

Create a WAF policy

Configure Protection Rules against XSS attacks

Verify the created environment against XSS attacks



Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99233424-C01 and Region us-ashburn-1.

Complete the following task in the provisioned OCI environment:

1. Create a Protection Rule with name WAF-PBT-XSS-Protection against XSS attack. for protecting web server

2. Create a New Rule Action with name WAF-PBT-XSS-Action where http response code will be 503 (Service Unavailable).
See the solution below in Explanation

Explanation:

SOLUTION:

From the navigation menu, select Identity & Security. Navigate to Web Application Firewall and click Policies under it.

In the left navigation pane, under List Scope, select the working compartment from the drop-down menu.

Click the IAD-SP-PBT-WAF-01_99233424-lab.user01 WAF policy to add a protection rule.

On the policy details page, click Protections under Policy.

In the Protection section on the console, click Manage request protection rules.

Click Add Request Protection Rule.

In the Add protection rule dialog box, enter the following details:

- a) Name: WAF-PBT-XSS-Protection
- b) Conditions: Do not add any condition.
- c) Under Rule action – Action name: Select Create New Action from the drop-down menu.

In the Add Action dialog box, enter the following details:

- a) Name: WAF-PBT-XSS-Action
- b) Type: Return HTTP Response
- c) Response code: Select “503 Service unavailable” from the drop-down menu.
- d) Response page body: Type “Service Unavailable: Web Server is secured against XSS attacks.” e) Click Add action.

Under Protection Capabilities, click Choose protection capabilities.

In the Choose protection capabilities dialog box, complete the following:

- a) Filter by tags: Type “xss” and press Enter.
- b) Filter by version: Latest
- c) Protection list: Check all protections. Select the check box in the header to add all.
- d) Click Choose protection capabilities.

e) Review and click Add request protection rule.

f) Click Save Changes in the Manage Request Protection Rules dialog box.

The rule you created appears in the list. The WAF policy will update and get back to Active state.

NO.110 Which IAM policy should be created to give XYZ the ability to list contents of a resource excluding the fneeds to authenticate in prod compartment ? Principle of least privilege should be used.

- * Allow group XYZ to manage all resources in compartment != prod
- * Allow group XYZ to use all resources in compartment != prod
- * Allow group XYZ to inspect all resources in tenancy where target.compartment.name != prod
- * Allow group XYZ to read all resources in tenancy where target.compartment.name != prod

Explanation

Graphical user interface, text, application Description automatically generated

Verbs

You use *verbs* in policy definitions to set the permission levels that given user groups have for given resource-types. For example, you would use the `read` verb to allow read-only access.

Here are the verbs have been defined for the set of Oracle Digital Assistant resource-types

Verb	Description
inspect	Generally covers operations that list contents of a resource. This is the verb that provides the most limited access.
read	In user interface terms, this generally means read-only access. In API terms, it generally applies to GET operations.
use	When applied to resources in the service's user interface, this generally allows developing, testing, and deploying of these resources. At the API level, it generally allows GET, PUT, POST, PATCH, and DELETE operations, with the exception of more high-impact operations (such as creating instances and purging data).
manage	Generally allows the user to perform the whole set of a resource type's operations, including high-impact operations such as creating instances and purging data.

NO.111 Which VCNconfiguration is CORRECT with regard to VCN peering within a same region ?

- * 12.0.0.0/16 and 194.168.0.0/16
- * 12.0.0.0/16 and 12.0.0.0/16C 194.168.0.0/24 and 194.168.0.0/24
- * 194.168.0.0/24 and 194.168.0.0/16

When setting up VCN peering within the same region, the VCNs must have non-overlapping CIDRs. In this case, the CIDR blocks 12.0.0.0/16 and 194.168.0.0/16 are different and do not overlap, making them suitable for VCN peering

NO.112 Challenge 4 – Task 4 of 6

Configure Web Application Firewall to Protect Web Server Against XSS Attack Scenario You have to protect web applications hosted on OCI from cross-site scripting (XSS) attacks. You can use the OCI Web Application Firewall (WAF) capabilities to create rules that compare against incoming requests to determine if the request contains an XSS attack payload. If a request is determined to be an attack, WAF should return the HTTP Service Unavailable (503) error.

To ensure that the configured WAF blocks the XSS attack, run the following script: [http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”](http://<public-ip-enforcement-point>/index.html?<p style=”background:url(javascript:alert(1))”>) To complete this deployment, you have to perform the following tasks in the environment provisioned for you:

Configure a Virtual Cloud Network (VCN)

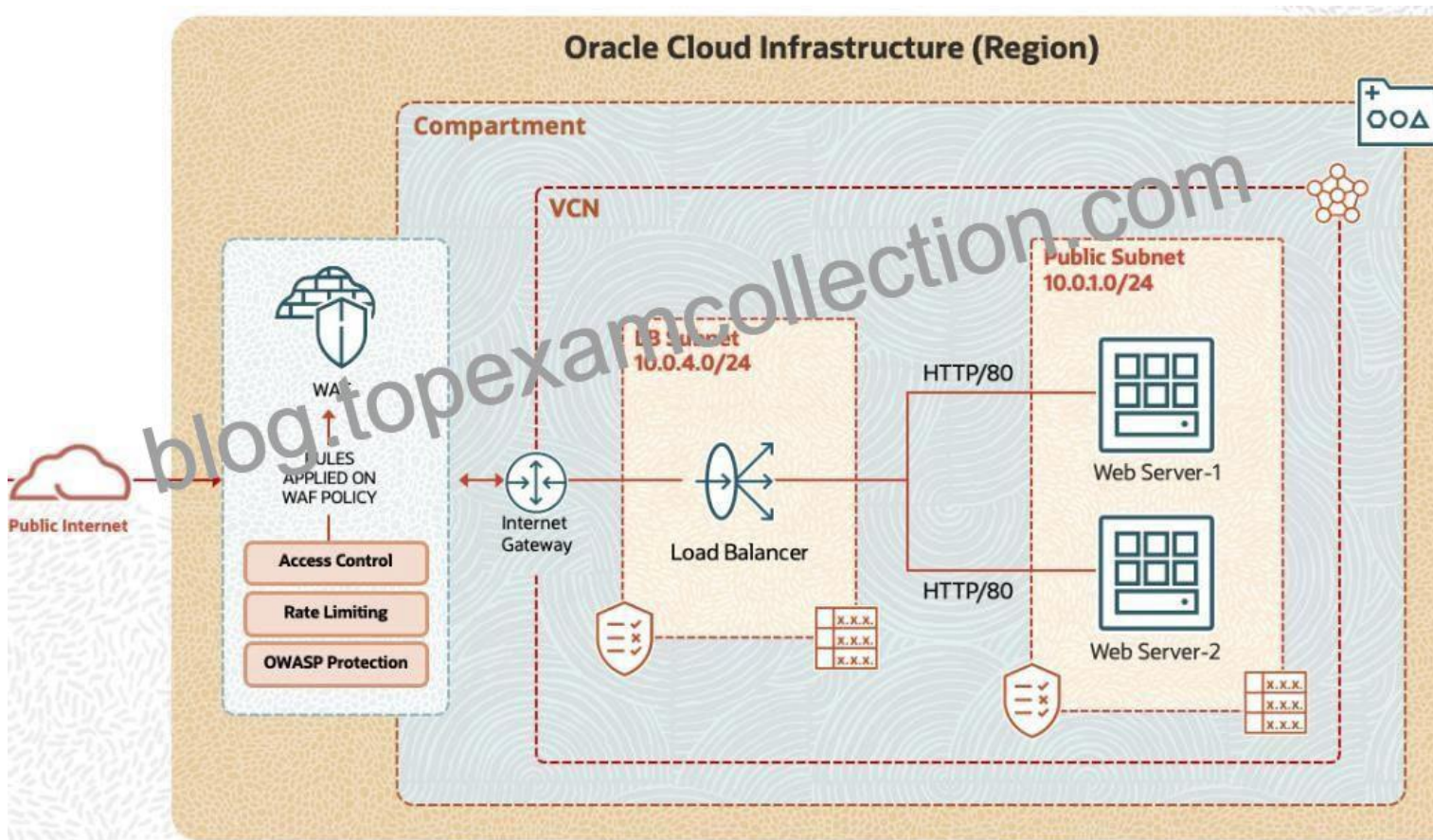
Create a Compute Instance and install the Web Server

Create a Load Balancer and update Security List

Create a WAF policy

Configure Protection Rules against XSS attacks

Verify the created environment against XSS attacks



Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99233424-C01 and Region us-ashburn-1.

Complete the following task in the provisioned OCI environment:

Create a WAF policy with the name IAD-SP-PBT-WAF-01_99233424-lab.user01 Eg: IAD-SP-PBT-WAF-01_99232403-lab.user02
See the solution below in Explanation

Explanation:

SOLUTION:

From the navigation menu, select Identity & Security. Navigate to Web Application Firewall and click Policies under it.

From the left navigation pane, under List Scope, select <your working compartment> from the drop-down menu.

Click Create WAF Policy.

The Create WAF Policy dialogue box appears. Creating a WAF policy consists of the following sections accessible from the left-side navigation:

- a) Basic information
- b) Access control
- c) Rate limiting
- d) Protections
- e) Select enforcement point
- f) Review and create.

In the Basic Information section:

- a) Name: IAD-SP-PBT-WAF-01_99233424-lab.user01
- b) WAF Policy Compartment: Select your working compartment
- c) Action: Keep the default preconfigured actions; do not edit.
- d) Click the Select enforcement point section accessible from the left-side navigation.

Note: You will configure the other section later in this practice. You will directly configure the Enforcement point.

In the Select enforcement point section: a) Add Firewalls: Select a load balancer IAD-SP-PBT-LB-01 in your current compartment from the list. b) Click Next for Review and Create.

Under the Review and Create Section: a) Verify the enforcement point added in the previous step.

Click Create WAF Policy.

The Create WAF Policy dialogue box closes, and you are returned to the WAF Policy page. The WAF policy you created is listed.

NO.113 What would you use to make Oracle Cloud Infrastructure Identity and Access Management govern resources in a tenancy?

- * Policies
- * Users
- * Dynamic groups
- * Groups

POLICY

A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see [Example Scenario and How Policies Work](#). The word `policy` is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named `policy` document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources.

<https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm>

NO.114 When creating an OCI Vault, which factors may lead to select the Virtual Private Vault? Select TWO correct answers

- * Need for more than 9211 key versions
- * Greater degree of isolation
- * To mask PII data for non-production environment
- * Ability to back up the vault

Explanation

Graphical user interface, text, application Description automatically generated



NO.115 VCN Flow log record details about the traffic that has been denied or approved is based on which of the following statements?

- * Configuration of route table
- * Security Lists or Network Security Group Rules
- * Web Application Firewall (WAF)
- * Auth tokens

Explanation

Graphical user interface, application, Teams Description automatically generated

What are VCN Flow Logs?

Each instance in an Oracle Cloud Infrastructure (OCI) Virtual Cloud Network (VCN) has one or more Virtual Network Interface Cards (VNICs) for communication within and outside of the VCN. OCI Networking uses security lists to determine what traffic is allowed in and out of a given VNIC. A VNIC is subject to all the rules in all the security lists and network security groups associated with the VNIC's subnet.

You can enable logging to capture this information. Network logs record details about the traffic that has been accepted or rejected based on the security list rules and network security group rules.

A flow log record is a pipe-delimited string that has the following format:

```
<time_stamp> <src_ip> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start_time> <end_time> <action> <status>
```

For example:

```
2 172.16.2.139 172.16.1.107 73 89 11 102 349 1557424442 1557424510 ALLOW OK
2 172.16.2.145 172.16.2.179 82 64 13 112 441 1557424462 1557424486 REJECT OK
```

NO.116 You are using a custom application with third-party APIs to manage application and data hosted in an Oracle Cloud Infrastructure(OCI) tenancy. Although your third-party APIs don't support OCI's signature-based authentication, you want them to communicate with OCI resources. Which authentication option must you use to ensure this?

- * OCI username and Password
- * API Signing Key
- * SSH Key Pair with 2048-bit algorithm
- * Auth Token

Explanation

An auth token in OCI is an Oracle-generated token that you can use to authenticate with third-party APIs. This can be useful when the third-party APIs do not support OCI's signature-based authentication.

NO.117 Which are the two responsibilities of Oracle when you move your IT infrastructure to Oracle Cloud Infrastructure (OCI)?

- * Strong Identity Access Management (IAM) framework
- * Storage isolation
- * Maintaining customer data
- * Account access management
- * Providing strong security lists

NO.118 You have created several Oracle Cloud Infrastructure Groups with the prefix of 'Test' in your tenancy. For example TestECommerce, TestCatalog, and TestAdministration. You want to create another group called TestGroupsAdmin to manage all the groups that start with 'Test' except for the group TestAdministration. (Choose the best Answer.)

- * allow group TestGroupsAdmin to manage groups in tenancy where any {target.group.name = /Test*/ ,target.group.name != TestAdministration }
- * allow group TestGroupsAdmin to manage groups in tenancy where target.group.name%Test*/ && !(target.group.name = `Test*;1 TestAdministration`)
- * allow group TestGroupsAdmin to manage groups in tenancy where target.group.name = /Test*/ and = TestAdministration
- * allow group TestGroupsAdmin to manage groups in tenancy where all {target.group.name = /Test*/ ,target.group.name != TestAdministration }

NO.119 As a cloud network administrator, you have been tasked with defining ingress and egress access rules for microservices deployed as functions in Oracle Functions. In addition to defining some general access rules in the subnet's security list, you define more fine-grained rules for different functions using Oracle Cloud Infrastructure (OCI) Network Security Groups (NSGs). Once the NSGs are created, where should they be attached in order to apply to a specific deployed function? (Choose the best

Answer.)

- * The function itself
- * The function's docker container
- * The application hosting the function
- * The pod hosting the application

NO.120 Which Oracle Data Safe feature minimizes the amount of personal data and allows internal test, development, and analytics teams to operate with reduced risk?

- * data auditing
- * data encryption
- * security assessment
- * data masking
- * data discovery

Data masking in Oracle Data Safe minimizes the amount of personal data and allows internal test, development, and analytics teams to operate with reduced risk. It replaces sensitive or confidential information in non-production databases with realistic and fully functional data with similar characteristics as the original data.

NO.121 What is the configuration to avoid publishing messages during the specified time range known as?

- * Trigger rule
- * Statistic
- * Resource group
- * Suppression

Graphical user interface, text, application, email Description automatically generated

suppression

A configuration to avoid publishing messages during the specified time range. Useful for suspending alarm notifications during system maintenance. Each suppression applies to a single alarm. In the Console, you can apply one definition of a suppression to multiple alarms. The result is an individual suppression for each alarm. For instructions on suppressing alarms, see [To suppress alarms](#).

NO.122 You have configured Management Agent on an Oracle Cloud Infrastructure (OCI) Linux instance for log Ingestion purposes. OR When using Management Agent to collect logs continuously. Which is required configuration for OCI Logging Analytics service to collect data from multiple logs of this Instance? (Choose the best Answer.)

- * Entity Log Association
- * Log-Log Group Association
- * Source-Entity Association
- * Log Group-Source Association

1z0-1104-23 Exam Questions & Valid 1z0-1104-23 Dumps Pdf:

<https://www.topexamcollection.com/1z0-1104-23-vce-collection.html>