



1Z0-1104-22^{Q&As}

Oracle Cloud Infrastructure 2022 Security Professional

Pass Oracle 1Z0-1104-22 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/1z0-1104-22.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What must be configured for a load balancer to accept incoming traffic?

- A. Service Gateway
- B. SSL certificate
- C. Listener
- D. Route table entry pointing to the listener IP address

Correct Answer: C

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP.

<https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/loadbalancing.htm> To create a listener:

On your Load Balancer Details page, click Listeners.

Click Create Listener.

Enter the following:

Click Create.

QUESTION 2

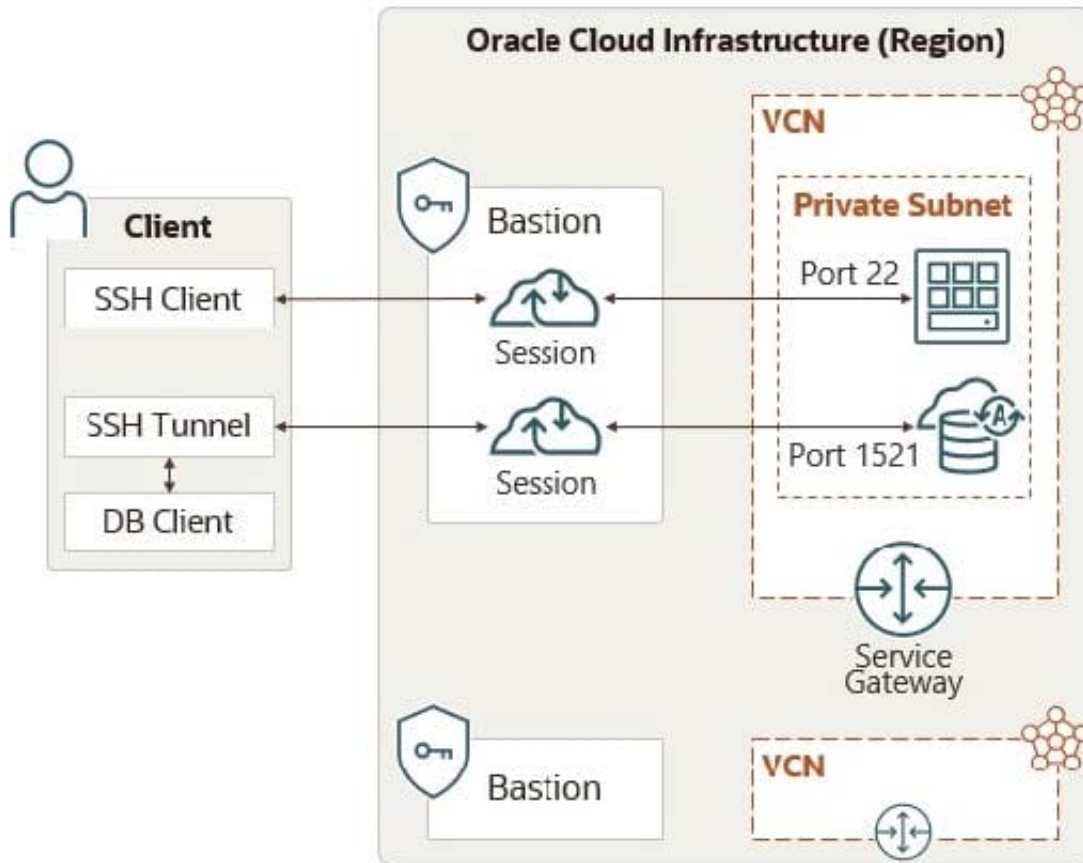
Which Oracle Cloud Service provides restricted access to target resources?

- A. Bastion
- B. Internet Gateway
- C. Load balancer
- D. SSL certificate

Correct Answer: A

Bastion

Oracle Cloud Infrastructure Bastion provides restricted and time-limited access to target resources that don't have public endpoints.



https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_features.htm

QUESTION 3

As a lead Security Architect, you have tasked to restrict access to and from the worker nodes in pods running in Oracle Container Engine for Kubernetes?

- A. Cloud Guard
- B. Vulnerability Scanning
- C. Security Lists
- D. Identity and Access Management

Correct Answer: C



Node Pool Security Lists

Network administrators can define security list rules on node pool subnets to restrict access to and from worker nodes. Defining security list rules allows administrators to enforce network restrictions that cannot be overridden on the hosts in your cluster.

Because all pod-to-pod communication occurs in a VXLAN overlay network on the worker nodes, you are cannot use security list rules to restrict pod-to-pod communication. However, you can use security lists to restrict access to and from your worker nodes.

Important: There is a minimum set of security list rules that must exist on node pool subnets to ensure that the cluster can function. See [Example Network Resource Configurations](#) for information on the minimum set of security list rules before making any changes to your security list rules.

QUESTION 4

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 ?

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

Correct Answer: B

QUESTION 5

Where are logs stored?

- A. OCI Object Storage
- B. OCI File Storage
- C. OCI Block Storage
- D. Cloud Agent

Correct Answer: A

You can collect log data continuously from Oracle CloudInfrastructure (OCI) Object Storage. To enable the log



collection, create ObjectCollectionRule resource using REST API or CLI. After the successful creation of this resource and having the required IAM policies, the log collection will be initiated.

<https://docs.oracle.com/en-us/iaas/logging-analytics/doc/collect-logs-your-oci-object-storage-bucket.html>

[1Z0-1104-22 VCE Dumps](#)

[1Z0-1104-22 Practice Test](#)

[1Z0-1104-22 Study Guide](#)