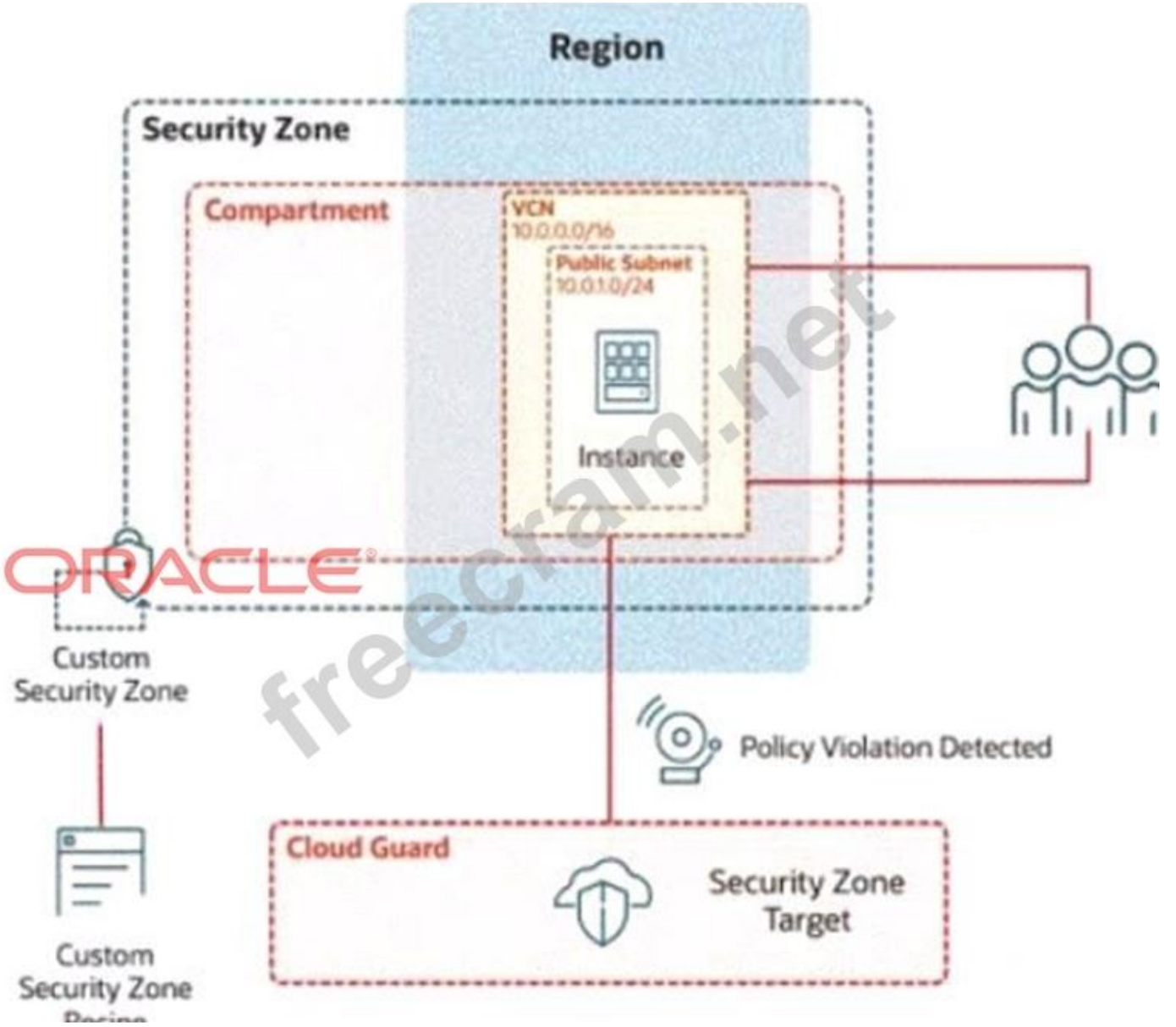
Oracle.1z0-1104-25.v2026-01-24.q16

Exam Code:	1z0-1104-25
Exam Name:	Oracle Cloud Infrastructure 2025 Security Professional
Certification Provider:	Oracle
Free Question Number:	16
Version:	v2026-01-24
# of views:	106
# of Questions views:	225
https://www.freecram.net/torrent/Oracle.1z0-1104-25.v2026-01-24.q16.html	

NEW QUESTION: 1
Challenge 2 -Task 1
In deploying a new application, a cloud customer needs to reflect different security postures. If a security zone is enabled with the Maximum Security Zone recipe, the customer will be unable to create or update a resource in the security zone if the action violates the attached Maximum Security Zone policy.
As an application requirement, the customer requires a compute instance in the public subnet. You therefore, need to configure Custom Security Zones that allow the creation of compute instances in the public subnet.
Review the architecture diagram, which outlines the resoures you'll need to address the requirement:



Preconfigured

To complete this requirement, you are provided with the following:

Access to an OCI tenancy, an assigned compartment, and OCI credentials

Required IAM policies

Task3: Create and configure a Virtual Cloud Network and Private Subnet

Createand configure virtual cloud Network (VCN) named IAD SP-PBT-VCN-01, with an internet Gateway and configure appropriate route rules to allow external connectivity.

Enter the OCID of the created VCN in the text box below.

Answer:

See the solution below in Explanation.

Explanation:

To create and configure a Virtual Cloud Network (VCN) named IAD-SP-PBT-VCN-01 with an Internet Gateway and appropriate route rules for external connectivity, follow these steps based on the Oracle Cloud Infrastructure (OCI) Networking documentation.

Step-by-Step Solution for Task 3: Create and Configure a VCN and Private Subnet

* Log in to the OCI Console:
* Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.
com).
* Ensure you have access to the assigned compartment.
* Navigate to Virtual Cloud Networks:
* From the OCI Console, click the navigation menu (hamburger icon) on the top left.
* UnderNetworking, selectVirtual Cloud Networks.
* Create a New VCN:
* ClickStart VCN Wizardand selectCreate VCN with Internet Connectivity.
* VCN Name:Enter IAD-SP-PBT-VCN-01.
* Compartment:Select the assigned compartment.
* VCN CIDR Block:Enter 10.0.0.0/16 (matches the diagram's VCN CIDR).
* Public Subnet CIDR Block:Enter 10.0.10.0/24 (matches the diagram's public subnet).
* Accept the default settingsfor the public subnet and Internet Gateway creation.
* ClickCreateto provision the VCN, Internet Gateway, and public subnet.
* Verify the Internet Gateway:
* After creation, go to the VCN details page for IAD-SP-PBT-VCN-01.
* UnderResources, selectInternet Gateways.
* Ensure the Internet Gateway is attached and enabled.
* Configure Route Rules:
* In the VCN details page, underResources, selectRoute Tables.
* Select the default route table associated with the public subnet (10.0.10.0/24).
* ClickAdd Route Rules.
* Target Type:SelectInternet Gateway.
* Destination CIDR Block:Enter 0.0.0.0/0.
* Target Internet Gateway:Select the Internet Gateway created with the VCN.
* ClickAdd Route Ruleto save.
* Update Security List (if needed):
* UnderResources, selectSecurity Lists.
* Edit the default security list for the public subnet.
* Add an ingress rule:
* Source CIDR:0.0.0.0/0
* IP Protocol:TCP
* Source Port Range:All
* Destination Port Range:22 (for SSH) or as required by your application.
* Add an egress rule:
* Destination CIDR:0.0.0.0/0
* IP Protocol:All
* Save the changes.
* Note the VCN OCID:

* Return to the VCN details page for IAD-SP-PBT-VCN-01.
* Copy theOCIDdisplayed (e.g., ocid1.vcn.oc1..<unique_string>).
OCID of the Created VCN
* Enter the OCID of the created VCN (IAD-SP-PBT-VCN-01) into the text box. The exact OCID will be available after Step 3 (e.g., ocid1.vcn.oc1..<unique_string>).

NEW QUESTION: 2
"A programmer is developing a Node.js application which will run on a Linux server on their on-premises data center. This application will access various Oracle Cloud Infrastructure (OCI) services using OCI SDKs.
What is the secure way to access OCI services with OCI Identity and Access Management (IAM)?
A. Create a new OCI IAM user associated with a dynamic group and a policy that grants the desired permissions to OCI services. Add the on-premises Linux server in the dynamic group.
B. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, generate the keypair used for signing API requests and upload the public key to the IAM user.
C. Create an OCI IAM policy with appropriate permissions to access the required OCI services and assign the policy to the on-premises Linux server."
D. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, add the user name and password to a file used by Node.js authentication.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Task 2: Create a Compute Instance and Install the Web Server
Create a compute instance, where:
Name: PBT-CERT-VM-01
Image: Oracle Linux 8
Shape: VM.Standard.A1.Flex
Subnet: Compute-Subnet-PBT-CERT
Install and configure Apache web server:
a.
Install Apache
sudo yum -y install httpd
b.
Enable and start Apache
sudo systemctl enable httpd
sudo systemctl restart httpd
2. Install and configure Apache web server:
a. Install Apache

sudo yum -y install httpd
b. Enable and start Apache
sudo systemctl enable httpd
sudo systemctl restart httpd
c. Configure firewall to allow HTTP traffic (port 80)
sudo firewall-cmd --permanent --add-port=80/tcp
sudo firewall-cmd --reload
d. Create an index.html file
sudo bash -c 'echo You are visiting Web Server 1 >> /var/www/html/index.html' Enter the OCID of the created compute instance PBT-CERT-VM-01 in the text box below.

Answer:

See the solution below in Explanation.

Explanation:

Task 2: Create a Compute Instance and Install the Web Server

Step 1: Create the Compute Instance

* Log in to the OCI Console.
* Navigate toCompute>Instances.
* ClickCreate Instance.
* Enter the following details:
* Name: PBT-CERT-VM-01
* Compartment: Select your assigned compartment.
* Placement: Leave as default or select an availability domain (e.g., Availability Domain 1).
* Image: ClickChange Image, selectOracle Linux 8, and confirm.
* Shape: ClickChange Shape, selectVM.Standard.A1.Flex, and configure:
* OCPUs: 1 (or adjust as needed)
* Memory: 6 GB (or adjust as needed)
* Networking:
* Virtual Cloud Network: Select PBT-CERT-VCN-01.
* Subnet: Select Compute-Subnet-PBT-CERT.
* Leave public IP assignment enabled for internet access.
* SSH Key: Provide your public SSH key (upload or paste) for secure access.
* ClickCreateand wait for the instance to be provisioned.

Step 2: Connect to the Compute Instance

* Once the instance is created, note thePublic IP Addressfrom the instance details page.
* Use an SSH client to connect:
* Command: ssh -i <private-key-file> opc@<public-ip-address>
* Replace <private-key-file> with your private key path and <public-ip-address> with the instance's public IP.

Step 3: Install and Configure Apache Web Server

* Install Apache:
* Run: sudo yum -y install httpd

* Enable and Start Apache:
* Run: sudo systemctl enable httpd
* Run: sudo systemctl restart httpd
* Configure Firewall to Allow HTTP Traffic (Port 80):
* Run: sudo firewall-cmd --permanent --add-port=80/tcp
* Run: sudo firewall-cmd --reload
* Create an index.html File:
* Run: sudo bash -c 'echo "You are visiting Web Server 1" >> /var/www/html/index.html' Step 4: Verify the Configuration
* Open
a web browser and enter http://
<public-ip-address> to ensure the page displays "You are visiting Web Server 1".
* If needed, troubleshoot by checking Apache status: sudo systemctl status httpd.
Step 5: Retrieve and Enter the OCID
* Go to the instance details page for PBT-CERT-VM-01 underCompute>Instances.
* Copy theOCID(a long string starting with ocid1.instance., unique to your tenancy).
* Enter the copied OCID exactly as it appears into the text box provided.
Notes
* These steps are based on OCI Compute documentation and Oracle Linux 8 setup guides.
* Ensure the security list PBT-CERT-CS-SL-01 allows inbound traffic on port 22 (SSH) and port 80 (HTTP) if not already configured.
* The OCID will be unique to your instance; obtain it from the OCI Console after creation

NEW QUESTION: 4
"Your company is in the process of migrating its sensitive data to Oracle Cloud Infrastructure (OCI) and is prioritizing the strongest possible security measures. Encryption is a key part of this strategy, but you are particularly concerned about the physical security of the hardware where your encryption keys will be stored.
Which characteristic of OCI Key Management Service (KMS) helps ensure the physical security of your encryption keys?
A. Granular customer control over key access permissions
B. Centralized key management for simplified administration
C. Utilization of FIPS 140-2 validated Hardware Security Modules (HSMs)"
D. Seamless integration with other OCI services for streamlined workflows
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Your organization needs to implement strong password policies for users in OCI.
Which of the following statements is TRUE about password policies in OCI IAM?
A. Simple password policies are suitable for production environments.
B. Custom password policies allow for granular control over password complexity.

C. Only one password policy can be applied to all users in a domain.
D. The default password policy cannot be modified.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Task 5: Create a Certificate
Create a certificate, where:
Certificate name: PBT-CERT-01-<username>
For example, if your username is 99008677-lab.user01, then the certificate name should be PBT-CERT-
01990086771abuser01
Ensure you eliminate special characters from the user name.
Common name: PBT-CERT-OCICERT-01
Certificate Authority: PBT-CERT-CA-01 (created in the previous task)
Answer:
See the solution below in Explanation.
Explanation:
Since I can't create resources or retrieve OCIDs directly in your OCI environment, I'll provide a step-by-step solution based on verified OCI documentation and best practices as of 02:30 PM BST on Thursday, June 12,
2025. Follow these instructions precisely in the OCI Console or CLI, using the preconfigured PBI_Vault_SP vault and the PBT-CERT-CA-01<username> Certificate Authority created in the previous task. Replace
<username> with your actual username (e.g., 99008677-lab.user01), ensuring special characters are removed.
Task 5: Create a Certificate
Step 1: Access the OCI Vault
* Log in to the OCI Console.
* Navigate toIdentity & Security>Vault.
* Select the root compartment.
* Locate and click on the vault named PBI_Vault_SP.
Step 2: Create the Certificate
* In the PBI_Vault_SP vault details page, underResources, clickCertificates.
* ClickCreate Certificate.
* Enter the following details:
* Name: Replace <username> with your username (e.g., if your username is 99008677-lab.user01, remove special characters like - and . to get 99008677labuser01, then use PBT-CERT-
0199008677labuser01).
* Common Name: Enter PBT-CERT-OCICERT-01.

* Certificate Authority: Select the PBT-CERT-CA-01<username> CA created in Task 4 (e.g., PBT-CERT-CA-0199008677labuser01).
* Subject: Leave as default or adjust (e.g., Organization, Country) if required.
* Validity Period: Set as needed (e.g., 1 year), or use the default.
* Compartment: Ensure it's set to the root compartment.
* ClickCreate Certificateand wait for the certificate to be issued.
Step 3: Verify the Certificate
* After creation, go to theCertificatessection under PBI_Vault_SP.
* Confirm the certificate PBT-CERT-01<username> (e.g., PBT-CERT-0199008677labuser01) is listed and its status is active.

NEW QUESTION: 7
According to the Oracle Cloud Infrastructure (OCI) Shared Responsibility Model, which statement accurately reflects OCI's responsibility for security?
A. OCI is responsible for securing the underlying infrastructure but not customer data.
B. Customers are responsible for securing both infrastructure and data.
C. OCI provides security only for free-tier services; customers secure everything else.
D. OCI has no security responsibilities; customers need to secure their resources.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Task 4: Create a Certificate Authority (CA)
Create a certificate authority, where:
CA name: PBT-CERT-CA-01-<username>
For example, if your username is 99008677-lab.user01, then the certificate authority name should be PBT- CERT-CA-01990086771abuser01 Ensure you eliminate special characters from the user name.
Common name: PBT-CERT-OCICA-01
Master Encryption Key: PBT-CERT-MEK-01 (created in the previous task)
Answer:
See the solution below in Explanation.
Task 4: Create a Certificate Authority (CA)
Step 1: Access the OCI Vault
* Log in to the OCI Console.
* Navigate toIdentity & Security>Vault.
* Select the root compartment.
* Locate and click on the vault named PBI_Vault_SP.
Step 2: Create the Certificate Authority
* In the PBI_Vault_SP vault details page, underResources, clickCertificate Authorities.
* ClickCreate Certificate Authority.
* Enter the following details:

* Name: Replace <username> with your username (e.g., if your username is 99008677-lab.user01, remove special characters like - and . to get 99008677labuser01, then use PBT-CERT-CA-0199008677labuser01).
* Common Name: Enter PBT-CERT-OCICA-01.
* Master Encryption Key: Select the PBT-CERT-MEK-01<username> key created in Task 3 (e.g., PBT-CERT-MEK-0199008677labuser01).
* Subject: Leave as default or adjust (e.g., Organization, Country) if required by your setup.
* Validity Period: Set as needed (e.g., 10 years), or use the default.
* Compartment: Ensure it's set to the root compartment.
* ClickCreate Certificate Authorityand wait for the CA to be provisioned.
Step 3: Verify the Certificate Authority
* After creation, go to theCertificate Authoritiessection under PBI_Vault_SP.
* Confirm the CA PBT-CERT-CA-01<username> (e.g., PBT-CERT-CA-0199008677labuser01) is listed and its status is active.

NEW QUESTION: 9
When trying to encrypt plaintext using Command Line Interface (CLI), the developer gets a Service Error.
This is the command the developer tried to run:

```
oci kms crypto encrypt --key-id ocid1.key.oc1.iad.bbptfrr5aaeuk.abuwcljt32arg6e6xlswgluvc52lnrtk62jq7jenfejfxlhb46nkav3zhsta --plaintext foobar --endpoint https://bbptfrr5aaeuk-management.kms.us-ashburn-1.oraclecloud.com
```

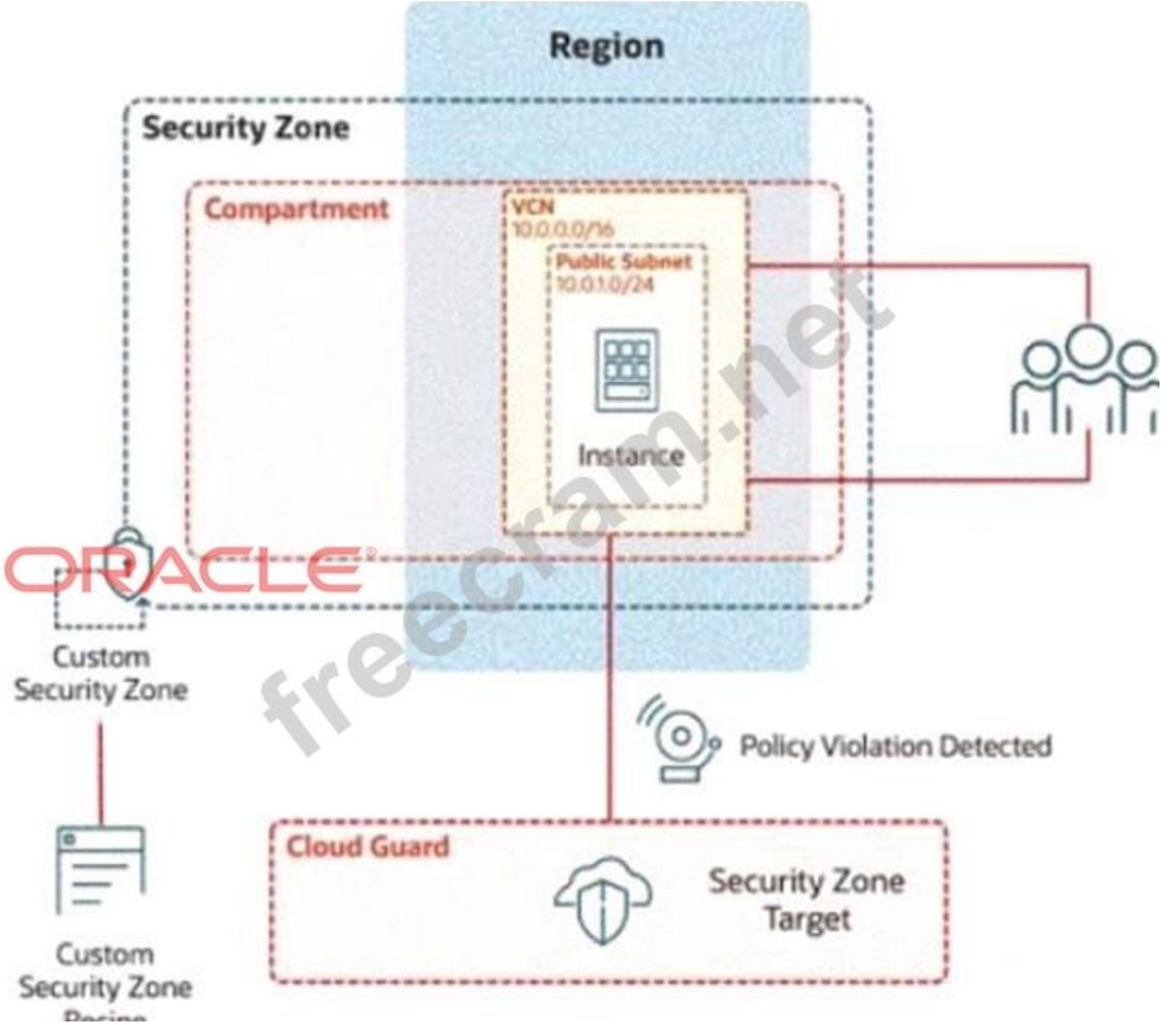
What is the reason for this error?
A. The developer has the wrong endpoint.
B. The user should pass the key version OCID instead of the key OCID.
C. The plaintext needs to be in JSON form.
D. The developer forgot to specify the region.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A. OCI Security Zones
B. OCI Threat Intelligence
C. OCI Web Application Firewall
D. OCI Incidence Responder
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which Oracle Data Safe feature enables the Internal test, development, and analytics teams to operate effectively while minimizing their exposure to sensitive data?
A. Data auditing
B. Sensitive data discovery
C. Data encryption

D. Security assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Challenge 2
In deploying a new application, a cloud customer needs to reflect different security postures. If a security zone is enabled with the Maximum Security Zone recipe, the customer will be unable to create or update a resource in the security zone if the action violates the attached Maximum Security Zone policy.
As an application requirement, the customer requires a compute instance in the public subnet. You therefore, need to configure Custom Security Zones that allow the creation of compute instances in the public subnet.
Review the architecture diagram, which outlines the resoures you'll need to address the requirement:



Preconfigured

To complete this requirement, you are provided with the following:
Access to an OCI tenancy, an assigned compartment, and OCI credentials
Required IAM policies
Task 5: Provision a Compute Instance
Provision a compute instance in the IAD-SP-PBT-PUBSNET-01 public subnet, where:
Name IAD-SP-PBT-1-VM-01
image: Oracle Linux 8
Shape VM: Standard, A1, Flex
Enter the OCID of the created compute instance in the text box below.
Answer:
See the solution below in Explanation.
Explanation:
To provision a compute instance named IAD-SP-PBT-1-VM-01 in the IAD-SP-PBT-PUBSNET-01 public subnet with the specified configuration (Oracle Linux 8 image, VM Standard A1 Flex shape), follow these steps based on the Oracle Cloud Infrastructure (OCI) Compute documentation.
Step-by-Step Solution for Task 5: Provision a Compute Instance
* Log in to the OCI Console:
* Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.
com).
* Ensure you have access to the assigned compartment.
* Navigate to Compute Instances:
* From the OCI Console, click the navigation menu (hamburger icon) on the top left.
* UnderCompute, selectInstances.
* Create a New Compute Instance:
* Click theCreate Instancebutton.
* Configure the Instance Details:
* Name:Enter IAD-SP-PBT-1-VM-01.
* Compartment:Select the assigned compartment.
* Placement:Choose the availability domain (e.g., AD-1) based on your region's availability.
* Select the Image:
* UnderImage and Shape, clickChange Image.
* SelectOracle Linux 8from the platform images list.
* ClickSelect Image.
* Choose the Shape:
* ClickChange Shape.
* SelectVM Standardcategory.
* ChooseA1 Flexfrom the shape options.
* Configure the OCPUs (e.g., 1 OCPU) and memory (e.g., 6 GB) as needed for A1 Flex, then click Select Shape.

* Configure Networking:
* UnderNetworking, ensure theVirtual Cloud Networkis set to IAD-SP-PBT-VCN-01.
* Set theSubnetto IAD-SP-PBT-PUBSNET-01 (public subnet with CIDR 10.0.1.0/24).
* EnableAssign a public IPv4 addressto allow external connectivity.
* Leave the default security list or assign a custom one if configured previously.
* Set Up SSH Access:
* UnderAdd SSH Keys, either:
* Upload your public SSH key file, or
* Paste your public SSH key manually.
* This ensures you can access the instance via SSH.
* Launch the Instance:
* ClickCreateto provision the compute instance.
* Wait for the instance to reach theRunningstate (this may take a few minutes).
* Note the Instance OCID:
* Once the instance is running, go to the instance details page for IAD-SP-PBT-1-VM-01.
* Copy theOCIDdisplayed (e.g., ocid1.instance.oc1..<unique_string>).
OCID of the Created Compute Instance
* Enter the OCID of the created compute instance (IAD-SP-PBT-1-VM-01) into the text box. The exact OCID will be available after Step 9 (e.g., ocid1.instance.oc1..<unique_string>).
Notes
* Ensure the security zone IAD_SAP-PBT-CSZ-01 and its associated recipe IAD-SP-PBT-CSP-01 allow compute instance creation in the public subnet (10.0.1.0/24).
* Verify network connectivity by testing SSH access using the public IP assigned to the instance.

NEW QUESTION: 13
During your investigation of a load balancer issue, you discovered that all back-end servers associated with one of the affected listeners were reported as unhealthy. However, when you checked the back-end servers, they seemed to be working just fine.
What might be causing this issue?
A. Incorrect DNS configuration
B. Misconfigured security rule
C. Overloaded back-end servers
D. Misconfigured health check
E. Incorrect subnet configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 14
An OCI administrator notices that a compute instance running in the production compartment is unable to create Object Storage buckets using the OCI CLI command:
oci os bucket create --name mybucket --compartment-id <compartment_OCID> --auth instance_principal The error message returned states:

"NotAuthorizedOrNotFound: You are not authorized to perform this action." The administrator verifies that the instance has Internet access and can reach OCI endpoints.
What then could be causing the issue?
A. The instance is not part of any Dynamic Group or the matching rule is incorrect.
B. The bucket name is already in use, causing a conflict.
C. The instance is using the wrong OCI CLI authentication method.
D. The policy is written at the root compartment instead of the production compartment.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
A company has deployed OCI Zero Trust Packet Routing (ZPR) to secure its network. They have two compute instances, VM1-01 and VM-02, in a public subnet. VM-01 is tagged with the security attribute app:
vm01, and VM-02 is tagged with app:vm02. The VCN is labeled with network:vcn01, The ZPR policy states:

```
IN ZPR:network:vcn01 VCN ALLOW ZPR:app:vm01 TO CONNECT ZPR:app:vm02 ON PORT 22
```

"What is the expected outcome of this policy?
A. VM-01 can SSH into VM-02, but VM-02 cannot SSH into VM-01.
B. Neither VM-01 nor VM-02 can SSH into each other."
C. Both VM-01 and VM-02 can SSH into each other.
D. VM-02 can SSH into VM-01, but VM-01 cannot SSH into VM-02.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
In Oracle Cloud Infrastructure (OCI), bare metal instances provide customers with direct access to the underlying hardware. To mitigate security risks when a customer terminates a bare metal instance, OCI utilizes Root-of-Trust hardware.
What is the primary function of the Root-of-Trust hardware in this context?
A. It eliminates the need for hypervisors, reducing the potential attack surface.
B. It automatically encrypts data at rest on the bare metal instance.
C. It ensures all non-volatile memory on the terminated instance is securely wiped before reuse.
D. It guarantees complete isolation between customer workloads on different instances.
Answer: (SHOW ANSWER)

Valid 1z0-1104-25 Dumps shared by ExamDiscuss.com for Helping Passing 1z0-1104-25 Exam! ExamDiscuss.com now offer the **newest 1z0-1104-25 exam dumps**, the ExamDiscuss.com 1z0-1104-25 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 1z0-1104-25 dumps with Test Engine here: https://www.examdiscuss.com/Oracle/exam/1z0-1104-25/premium/ (**39** Q&As Dumps, **35%OFF Special Discount Code: freecram**)