1Z0-997Q&As

Oracle Cloud Infrastructure 2019 Architect Professional

Pass Oracle 1Z0-997 Exam with 100% Guarantee

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

https://www.pass2lead.com/1z0-997.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are working with a social media company as a solution architect. The media company wants to collect and analyze large amounts of data being generated from their websites and social media feeds to gain insights and continuously improve the user experience. In order to meet this requirement, you have developed a microservices application hosted on Oracle Container Engine for Kubernetes. The application will process the data and store the result to an Autonomous Data Warehouse (ADW) instance. Which Oracle Cloud Infrastructure (OCI) service can you use to collect and process a large volume of unstructured data in real time?

A. OCI Events

B. OCI Streaming

C. OCI Resource Manager

D. OCI Notifications

Correct Answer: B

QUESTION 2

You are running a legacy application In a compute Instance on Oracle Cloud Infrastructure (OCI). To provide enough space for it to store internal data, a block volume is attached to the instance in paravirtualized mode. Your application is not resilient to crash-consistent backup. What should you do to securely backup the block volume?

A. Create a volume group, add the block volume and boot volume and then run the volume group backup.

B. Before creating a backup, save your application data and detach the block volume.

C. Create a backup, detach the block volume and save your application data.

D. Use the block volume clone feature to save cost and speed up the backup process.

Correct Answer: D

QUESTION 3

A digital marketing company is planning to host a website on Oracle Cloud Infrastructure (OCI) and leverage OCI Container Engine for Kubernetes (OKE). The web server will make API calls to access OCI Object Storage to store all images uploaded by users. For security purposes, your manager instructed you to ensure that the credentials used by the web server to allow access not stored locally on the compute instance. What solution results in an Implementation with the least effort for this scenario?

A. Configure the credentials using Instance Principal to allow the web server to make API calls to OCl Object Storage

B. Configure the credentials using OCI Registry (OC1R) which will automatically connect with OKE allowing the web server to make API calls to OCI Object Storage.

C. Configure the credentials to use Transparent Data Encryption (TDE) which will automatically allow the web server to make API calls to OCl Object Storage.

D. Configure the credentials using OCI Key Management to allow an instance to make API calls and grant access to OCl Object Storage.

Correct Answer: C

INSTANCE PRINCIPALS The IAM service feature that enables instances to be authorized actors (or principals) to perform actions on service resources. Each compute instance has its own identity, and it authenticates using the certificates that are added to it. These certificates are automatically created, assigned to instances and rotated, preventing the need for you to distribute credentials to your hosts and rotate them. Dynamic groups A special type of group that contains resources (such as compute instances) that match rules that you define (thus the membership can change dynamically as matching resources are created or deleted). These instances act as "principal" actors and can make API calls to services according to policies that you write for the dynamic group. The following steps summarize the process flow for setting up and using instances as principals. The subsequent sections provide more details. 1 Create a dynamic group. In the dynamic group definition, you provide the matching rules to specify which instances you want to allow to make API calls against services. 2 Create a policy granting permissions to the dynamic group to access services in your tenancy (or compartment). 3 A developer in your organization configures the application built using the Oracle Cloud Infrastructure SDK to authenticate using the instance principals provider. The developer deploys the application and the SDK to all the instances that belong to the dynamic group. 4 The deployed SDK makes calls to Oracle Cloud Infrastructure APIs as allowed by the policy (without needing to configure API credentials). 5 For each API call made by an instance, the Audit service logs the event, recording the OCID of the instance as the value of principalId in the event log.

QUESTION 4

You are working as a solution architect for an online retail store to create a portal to allow the users to pay for their groceries using credit cards. Since the application is not fully compliant with the Payment Card Industry Data Security Standard (PCI DSS), your company is looking to use a third party payment service to process credit card payments. The third party service allows a maximum of Spelunk IP addresses 5 public IP addresses at a time However, your website is using Oracle Cloud Infrastructure (OCI) Instance Pool Auto Scaling policy to create up to create up to 15 Instances during peak traffic demand, which are launched In VCN private in VCN private subnets and attached to an OCI public Load Balancer. Upon user payment, the portal connects to the payment service over the Interne! to complete the transaction What solution can you implement to make sure that all compute Instances can connect to the third party system to process the payments aw peak traffic demand?

A. Route credit card payment request from the compute instances through the NAT Gateway. On the third-party services, whitest the public IP associated with the NAT Gateway.

B. Whitelist the Internet Gateway Public IP on the third party service and route all payment requests through the Internet Gateway.

C. Create an OCI Command Line Interface (CLI) script to automatically reserve public IP address for the compute instances. On the third services, whitelist the Reserved public IP.

D. Route payment request from the compute instances through the OCI Load Balancer, which will then be routed to the third party service.

Correct Answer: D

You can OCI Load Balancer for this solution which can you the Public IPs of Load balancer to Traffic to third party services which allows a maximum of Spelunk IP addresses 5 public IP addresses at a time However, your website is using Oracle Cloud Infrastructure (OCI) Instance Pool Auto Scaling policy to create up to 15 Instances during peak traffic demand

QUESTION 5

An organization has its IT infrastructure in a hybrid setup with an on-premises environment and an Oracle Cloud Infrastructure (OCI) Virtual Cloud Network (VCN) in the us-phonix-1 region. The on- premise applications communications with compute instances inside the VPN over a hardware VPN connection. They are looking to implement an Intrusion detected and Prevention (IDS/IPS) system for their OCI environment. This platform should have the ability to scale to thousands of compute of instances running inside the VCN. How should they architect their solution on OCI to achieve this goal?

A. Set up an OCI Private Load Balance! and configure IDS/IPS related health checks at TCP and/or HTTP level to inspect traffic

B. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform to inspection

C. There Is no need to implement an IPS/IDS system as traffic coming over IPSec VPN tunnels Is already encrypt

D. Configure autoscaling on a compute Instance pool and set vNIC to promiscuous mode to called traffic across the vcn and send it IDS/IPS platform for inspection.

Correct Answer: B

in Transit routing through a private IP in the VCN you set up an instance in the VCN to act as a firewall or intrusion detection system to filter or inspect the traffic between the on-premises network and Oracle Services Network. The Networking service lets you implement network security functions such as intrusion detection, application-level firewalls In fact, the IDS model can be host-based IDS (HIDS) or network-based IDS (NIDS). HIDS is installed at a host to periodically monitor specific system logs for patterns of intrusions. In contrast, an NIDS sniffs the traffic to analyze suspicious behaviors. A signature-based NIDS (SNIDS) examines the traffic for patterns of known intrusions. SNIDS can quickly and reliably diagnose the attacking techniques and security holes without generating an over-whelming number of false alarms because SNIDS relies on known signatures. However, anomaly-based NIDS (ANIDS) detects unusual behaviors based on statistical methods. ANIDS could detect symptoms of attacks without specific knowledge of details. However, if the training data of the normal traffic are inadequate, ANIDS may generate a large number of false alarms.

QUESTION 6

You have an Oracle database system in a virtual cloud network (VCN) that needs to be accessible on port

1521 from your on-premises network CIDR 172.17.0.0/24.

You have the following configuration currently.

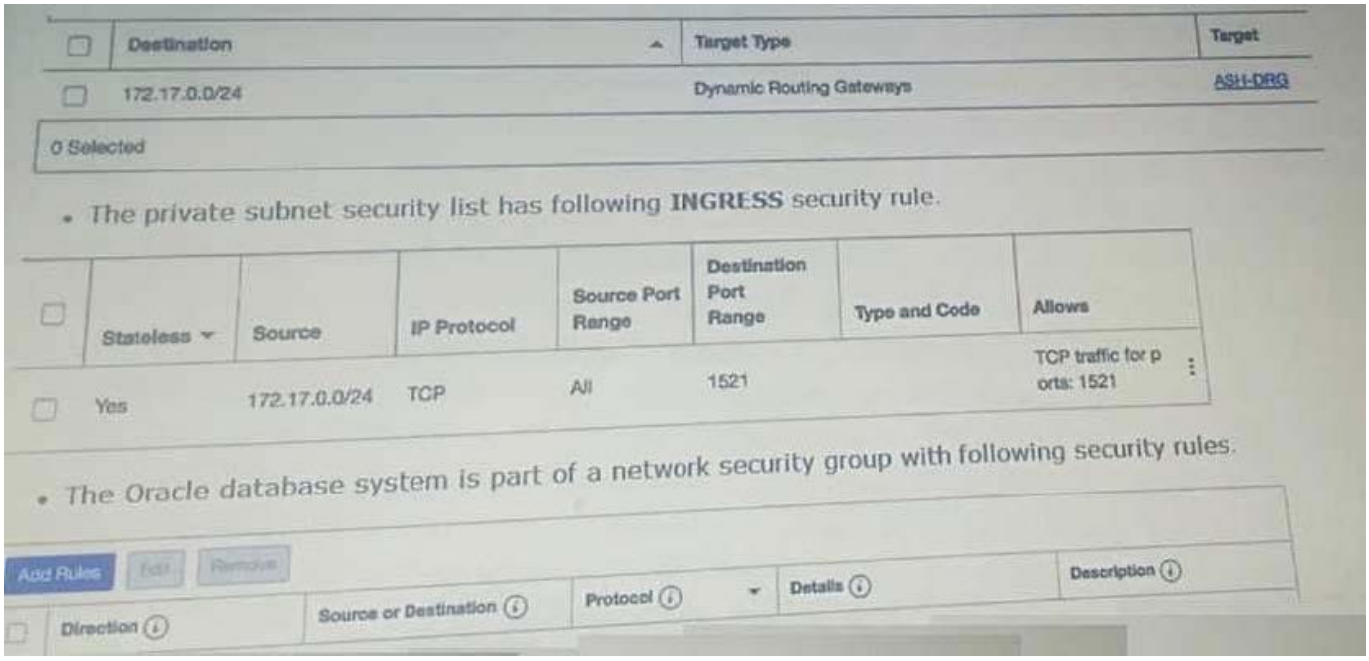
Virtual cloud network (VCD) is associated with a Dynamic Routing Gateway (DRG), and DRG has an

active IPSec connection with your on-premises data center.

Oracle database system is hosted in a private subnet

The private subnet route table has the following configuration The private subnet route table has following

configuration.

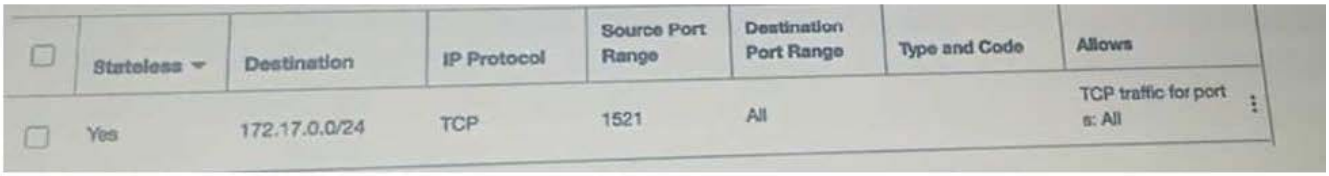


However, you are still unable to connect to the Oracle Database system. Which action will resolve this issue?

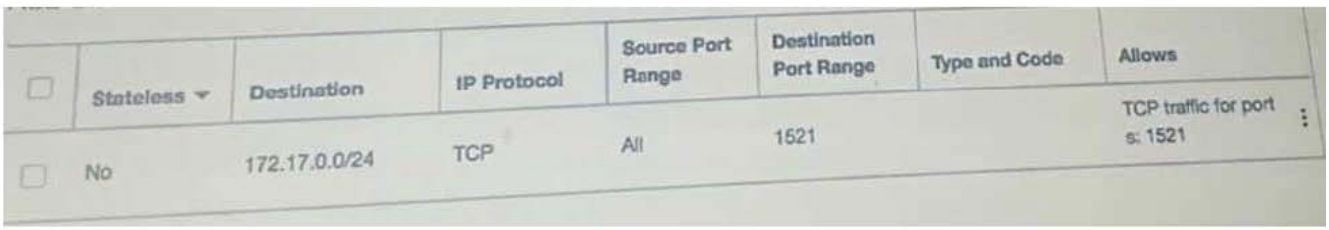
A. Add an EGRESS rule in network security group as following.

B. Add a route rule in the private subnet route table as following.
Questions & Answers PDF P-6

C. Add an EGRESS rule in private subnet scurity list as following.



D. Add an EGRESS rule in private subnet security list as following.



A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 7

An OCI Architect is working on a solution consisting of analysis of data from clinical trials of a pharmaceutical company. The data is being stored in OCI Autonomous Data Warehouse (ADW) having 8 CPU Cores and 70 TB of storage. The architect is planning to setup autoscaling to respond to dynamic changes in the workload. Which of the following needs to be considered while configuring auto scaling? Choose two

A. Enabling auto scaling does not change the concurrency and parallelism settings

B. Auto scaling also scales IO throughput linearly along with CPU

C. The database memory SGA and PGA will not get affected by the changes in the number of CPUs during auto scaling

D. The maximum CPU cores that will be automatically allocated for this database is 16 CPUs

Correct Answer: AB

Auto scaling is enabled by default when you create an Autonomous Database instance or you can use Scale Up/Down on the Oracle Cloud Infrastructure console to enable or disable auto scaling. With auto scaling enabled the database can use up to three times more CPU and IO resources than specified by the number of OCPUs currently shown in the Scale Up/Down dialog. When auto scaling is enabled, if your workload requires additional CPU and IO resources the database automatically uses the resources without any manual intervention required. Enabling auto scaling does not change the concurrency and parallelism settings for the predefined services IO throughput depends on the number of CPUs you provision and scales linearly with the number of CPUs.

QUESTION 8

Your company will soon start moving critical systems Into Oracle Cloud Infrastructure (OCI) platform.

These systems will reside in the us-phoenix-1and us-ashburn 1 regions. As part of the migration planning,

you are reviewing the company\\'s existing security policies and written guidelines for the OCI platform

usage within the company. you have to work with the company managed key.

Which two options ensure compliance with this policy?

A. When you create a new compute instance through OCI console, you use the default options for "configure boot volume" to speed up the process to create this compute instance.

B. When you create a new block volume through OCI console, select Encrypt using Key Management checkbox and use encryption keys generated and stored in OCI Key Management Service.

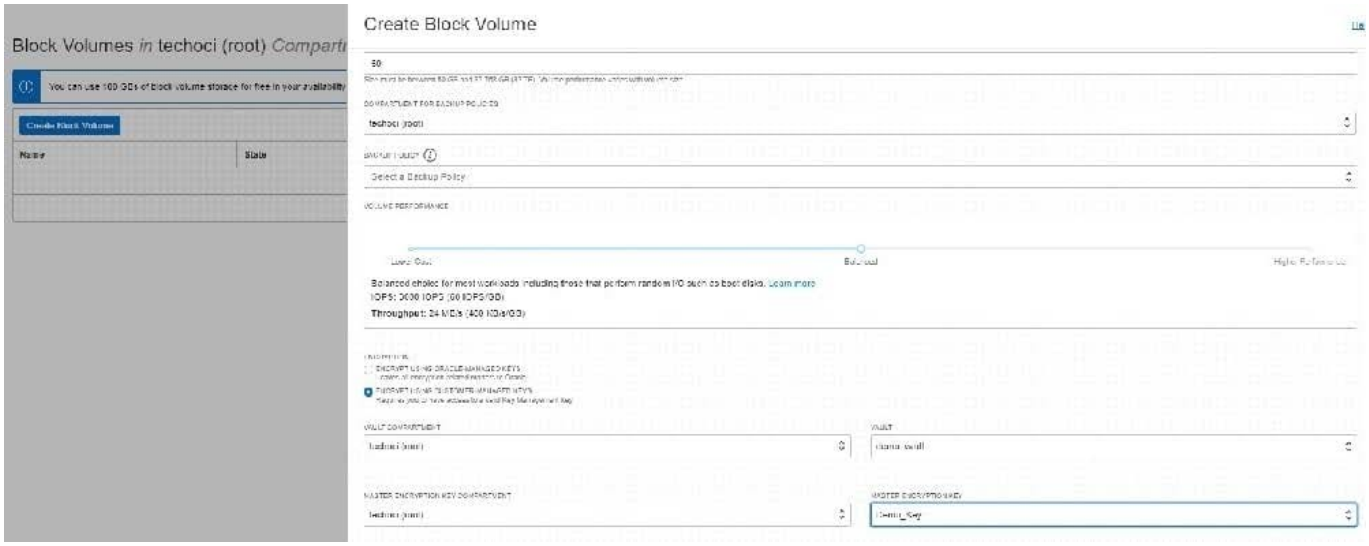
C. When you create a new compute instance through OCI console, you use the default shape to speed up the process to create this compute instance.

D. When you create a new OCI Object Storage bucket through OCI console, you need to choose "ENCRYPT USING CUSTOMER-MANAGED KEYS" option.

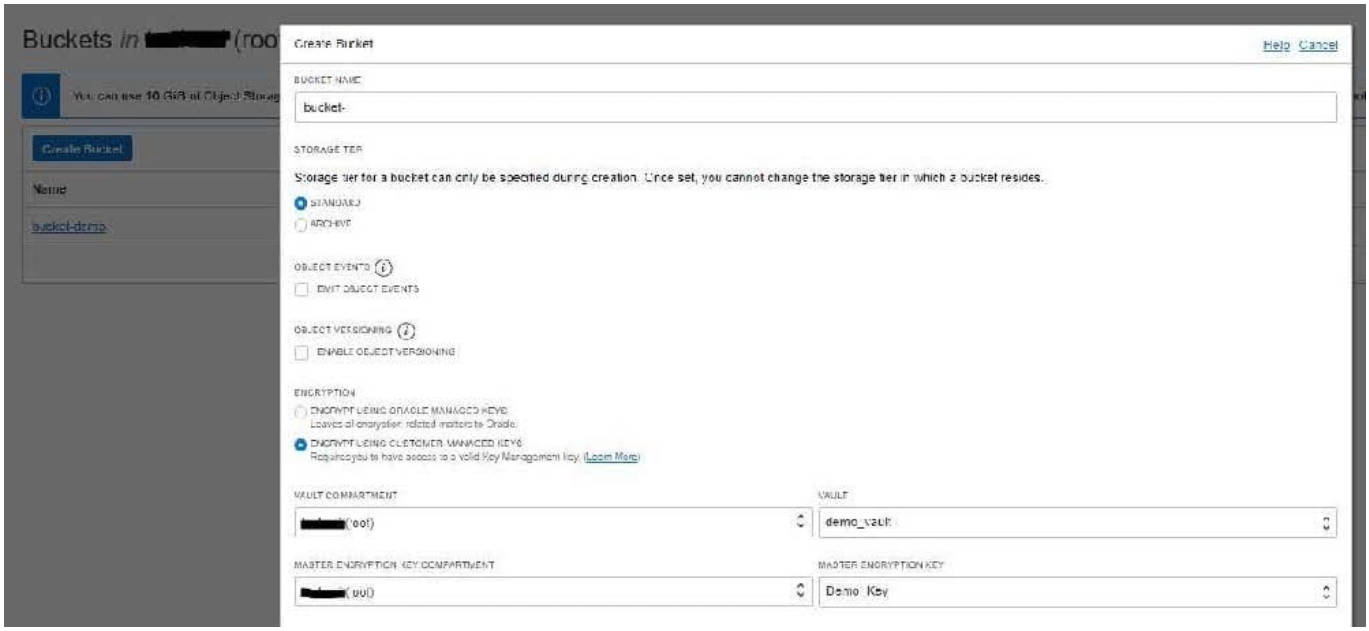
E. You do not need to perform any additional actions because the OCI Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption.

Correct Answer: BD

Block Volume Encryption By default all volumes and their backups are encrypted using the Oracle-provided encryption keys. Each time a volume is cloned or restored from a backup the volume is assigned a new unique encryption key. You have the option to encrypt all of your volumes and their backups using the keys that you own and manage using the Vault service.If you do not configure a volume to use the Vault service or you later unassign a key from the volume, the Block Volume service uses the Oracle-provided encryption key instead.

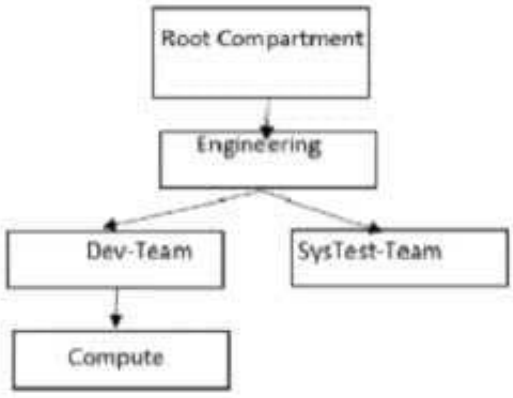


This applies to both encryption at-rest and in-transit encryption. Object Storage Encryption Object Storage employs 256-bit Advanced Encryption Standard (AES-256) to encrypt object data on the server. Each object is encrypted with its own data encryption key. Data encryption keys are always encrypted with a master encryption key that is assigned to the bucket. Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key. However, you can optionally configure a bucket so that it\\'s assigned an Oracle Cloud Infrastructure Vault master encryption key that you control and rotate on your own schedule. Encryption: Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own Vault encryption key. To use Vault for your encryption needs, select Encrypt Using Customer-Managed Keys. Then, select the Vault Compartment and Vault that contain the master encryption key you want to use. Also select the Master Encryption Key Compartment and Master Encryption Key.



QUESTION 9

Give this compartment structure:



You want to move a compute instance that is in \\'Compute\\' compartment to \\'SysTes-Team\\'. You login to your Oracle Cloud Infrastructure (OCI)account and use the \\'Move Resource\\' option. What will happen when you attempt moving the compute resource?

A. The move will be successful though Compute Instance and its Public and Private IP address will stay the same. The Compute instance VNIC will need to be moved separately. The Compute instance will still be associated with the original VCN.

B. The move will fail and you will be prompted to move the VCN first. Once VCN is moved to the target compartment, the Compute instance can be moved.

C. The move will be successful though Compute Instance Public and Private IP address changed, and it will be associated to the VCN in target compartment.

D. The move will be successful though Compute Instance and its Public and Private IP address will stay the same. The Compute instance VNIC will still be associated with the original VCN.

Correct Answer: D

Moving Resources to a Different Compartment Most resources can be moved after they are created. There are a few resources that you can\\'t move from one compartment to another. Some resources have attached resource dependencies and some don\\'t. Not all attached dependencies behave the same way when the parent resource moves. For some resources, the attached dependencies move with the parent resource to the new The parent resource moves immediately, but in some cases attached dependencies move asynchronously and are not visible in the new compartment until the move is complete. For other resources, the attached resource dependencies do not move to the new compartment. You can move these attached resources independently. You can move Compute resources such as instances, instance pools, and custom images from one compartment to another. When you move a Compute resource to a new compartment, associated resources such as boot volumes and VNICs are not moved. You can move a VCN from one compartment to another. When you move a VCN, its associated VNICs, private IPs, and ephemeral IPs move with it to the new compartment.

QUESTION 10

You are part of a project team working in the development environment created in OCI. You have realized that the CIDR block specified for one of the subnet in a VCN is not correct and want to delete the subnet. While deleting you are getting an error indicating that there are still resources that you must delete first. The error includes the OCID of the VNIC that is in the subnet. Which of the following action you will take to troubleshoot this issue?

A. Use OCI CLI to call "GetVnic" operation to find out the parent resource of the VNIC

B. Copy and Paste OCID of the VNIC in the search box of the OCI Console to find out the parent resource of the VNIC

C. Use OCI CLI to delete the VNIC first and then delete the subnet

D. Use OCI CLI to delete the subnet using --force option

Correct Answer: A

VCN, it must first be empty and have no related resources or attached gateways To delete a VCN\\'s subnets, they must first be empty. Note: When you create one of the preceding resources, you specify a VCN and subnet for it. The relevant service creates at least one VNIC in the subnet and attaches the VNIC to the resource. The service manages the VNICs on your behalf, so they are not readily apparent to you in the Console. The VNIC enables the resource to communicate with other resources over the network.

Although this documentation commonly talks about the resource itself being in the subnet, it\\'s actually the resource\\'s attached VNIC. If the subnet is not empty, you instead get an error indicating that there are still resources that you must delete first. The error includes the OCID of a VNIC that is in the subnet (there could be more, but the error returns only a single VNIC\\'s OCID). You can use the Oracle Cloud Infrastructure command line interface (CLI) or another SDK or client to call the GetVnic operation with the VNIC OCID. The response includes the VNIC\\'s display name. Depending on the type of parent resource, the display name can indicate which parent resource the VNIC belongs to. You can then delete that parent resource, or you can contact your administrator to determine who owns the resource. When the VNIC\\'s parent resource is deleted, the attached VNIC is also deleted from the subnet. If there are remaining VNICs in the subnet, repeat the process of determining and deleting each parent resource until the subnet is empty. Then you can delete the subnet. For example, if you\\'re using the CLI, use this command to get information about the VNIC. oci network vnic get --vnic-id