Oracle.1Z0-1067-20.v2020-07-20.q22

Exam Code:	1Z0-1067-20
Exam Name:	Oracle Cloud Infrastructure 2020 Cloud Operations Associate
Certification Provider:	Oracle
Free Question Number:	22
Version:	v2020-07-20
# of views:	1721
# of Questions views:	21389
https://www.freecram.com/torrent/Oracle.1Z0-1067-20.v2020-07-20.q22.html	

NEW QUESTION: 1
You are a Cloud Operations administrator who has recently joined a new department. You have created 10 Terraform stacks using Oracle Cloud Infrastructure (OCI) resource manager. Each stack creates a different set of resources In OCI for your development team.
What determines the cost of these Terraform stacks?
A. The cost for each stack will be higher for pay as you go (PAYG) than for monthly flex billing.
B. The length of time It takes to build each resource using these Terraform stacks.
C. Resource manager stacks are free but you are charged for the resources they create.
D. The number of lines of text in your Terraform configuration files.
Answer: C (LEAVE A REPLY)
There are no fees for installing and managing Resource Manager, you only pay for the infrastructure you deploy and use for your applications.
https://www.oracle.com/cloud/systems-management/resource-manager/

NEW QUESTION: 2
Which three statements ate true about Object Storage data security and encryption In Oracle Cloud Infrastructure (OCI)?
A. OCI Key Management is used by default to provide data security.
B. Client-side encryption is managed by the customer.
C. A VPN connection to OCI is required to ensure secure data transfer to an object storage bucket.
D. All traffic to and from Object Storage service is encrypted using TLS.
E. Server side encryption uses per-object keys which are managed by Oracle.
Answer: (SHOW ANSWER)
All data in Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, customers can use client-side

encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option for customers is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java.
Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default. FastConnect public peering allows on-premises access to Object Storage to go over a private network, rather than the public internet.
Oracle Cloud Infrastructure Key Management is a managed service the enables you, the customer, to manage and control AES symmetric keys used to encrypt your data-at-rest. Keys are stored in a FIPS 140-2, Level 3-certified, Hardware Security Module (HSM) that is durable and highly available. The Key Management service is integrated with many Oracle Cloud Infrastructure services, including Block Volumes, File Storage, Oracle Container Engine for Kubernetes, and Object Storage.
Use the Key Management service if you need to store your Master Encryption Keys in an HSM to meet governance and regulatory compliance requirements or when you want more control over the cryptoperiod of the encryption keys used for your data.
When you store your data with Oracle Cloud Infrastructure Block Volumes, File Storage Service, and Object Storage and don't use Key Management, your data is protected using encryption keys that are securely stored and controlled by Oracle.

NEW QUESTION: 3
Your team Implemented a SaaS application that requires a whole system deployment for each new customer. The Infrastructure provisioning is already automated via Terraform, and now you have been asked to develop an Ansible playbook to centralize configuration file management and deployment.
What Is the most effective way to ensure your playbooks are utilizing up-to-date and accurate Inventory?
A. Implement a Command Line Interface script to list all the resources and run it within Ansible to generate a dynamic inventory list.
B. Export an inventory list using Terraform apply command.
C. Export an inventory list from the Oracle Cloud Infrastructure Web console.
D. Download the dynamic inventory script provided by Oracle Cloud Infrastructure and include It in the playbook Invocation command.
Answer: (SHOW ANSWER)
Ansible tracks configuration resources by preserving lists, called inventory lists. These inventory files can be either simple static lists, or they can be dynamic lists that automatically update when inventory resources are added, deleted, or moved.
When using Ansible to work with hosts that you have provisioned in Oracle Cloud Infrastructure, static inventory lists can cause problems because Compute instances are added and deleted over time. They can also be affected by external tools such as Terraform, or by the Oracle Cloud Infrastructure SDKs.

Oracle Cloud Infrastructure provides two tools for working with Ansible inventory: a dynamic inventory plugin (recommended) and a dynamic inventory script.
Using the Dynamic Inventory Script
Having up-to-date and accurate inventory lists is essential for running Ansible playbooks. Oracle Cloud Infrastructure provides you with a script that you can download and run to ensure that your instance inventory list is always up-to-date. The script ensures that you always have the current set of Oracle Cloud Infrastructure compute instances available to your playbooks
https://docs.cloud.oracle.com/en-us/iaas/Content/API/SDKDocs/ansibleinventoryscript.htm

NEW QUESTION: 4
Which of the following are essential components of the Oracle Cloud Infrastructure Notifications service?
A. An alarm with a name unique across the tenancy, a subscription, and a metric with the measurement of interest.
B. A topic with a name unique across the compartment, a subscription, and a message where content Is published.
C. A topic with a name unique across the tenancy, a subscription, and a message where content is published.
D. An alarm with a name unique across the compartment, a subscription, and a metric with the measurement of interest.
Answer: C (LEAVE A REPLY)
The Oracle Cloud Infrastructure Notifications service broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally. Use Notifications to get notified when event rules are triggered or alarms are breached, or to directly publish a message.
MESSAGE
The content that is published to a topic. Each message is delivered at least once per subscription. Every message sent out as email contains a link to unsubscribe from the related topic.
SUBSCRIPTION
An endpoint for a topic. Published messages are sent to each subscription for a topic. For supported subscription protocols.
TOPIC
A communication channel for sending messages to the subscriptions in the topic. Each topic name is unique across the tenancy.

NEW QUESTION: 5
You have been asked to update the lifecycle policy for object storage using the Oracle Cloud Infrastructure (OCI) Command Line Interface (CLI).
Which command can successfully update the policy?
A. oci os object-lifecycle-policy delete -ns <object_storage_namespace> -bn <bucket_name>

B. oci os object-lifecycle-policy put -ns <object_storage_namespace> -bn <bucket_name> -Items <json_formated_lifecycle_policy>
C. oci os object-lifecycle-policy put -ns <object_storage_namespace> -bn <bucket_name> O
D. oci os object-lifecycle-policy get -ns <object_storage_namespace> -bn <bucket_name>
Answer: B (LEAVE A REPLY)
To create or replace a lifecycle policy for a bucket
Open a command prompt and run oci os object-lifecycle-policy put to create or replace the object lifecycle policy for a bucket. To edit individual rules, replace the bucket's existing policy with a new version of the policy that includes the changes to your rules.
oci os object-lifecycle-policy put -ns <object_storage_namespace> -bn <bucket_name> --items <json_formatted_lifecycle_policy> The --items option requires that you provide key-value pair input as valid formatted JSON
https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm

NEW QUESTION: 6
You are tasked with creating a group called volumeBackcupAdmins to manage only block volume backups. Which of the following set of policy/policies would you need to write to meet this requirement?
A)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
```

B)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to use volume-attachments in tenancy
Allow group VolumeBackupAdmins to use instances in tenancy
```

C)

```
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
```

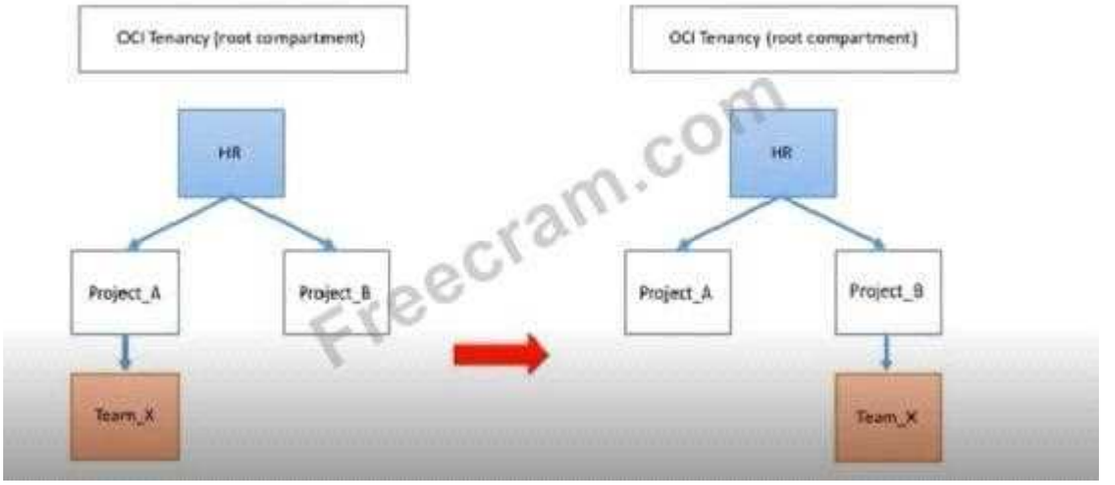
D)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to use volume-attachments in tenancy
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: A (LEAVE A REPLY)
Let volume backup admins manage only backups
Type of access: Ability to do all things with volume backups, but not create and manage volumes themselves. This makes sense if you want to have a single set of volume backup admins manage all the volume backups in all the compartments. The first statement gives the required access to

the volume that is being backed up; the second statement enables creation of the backup (and the ability to delete backups). The third statement enables the creation and management of user defined backup policies; the fourth statement enables assignment and removal of assignment of backup policies.
Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes and backups in a particular compartment, specify that compartment instead of the tenancy.
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
If the group will be using the Console, the following policy gives a better user experience:
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to inspect volume-attachments in tenancy Allow group VolumeBackupAdmins to inspect instances in tenancy

NEW QUESTION: 7
Your company has restructured its HR departments. As part of this change, you also need to re-organize compartments within Oracle Cloud Infrastructure (OCI) to align them to the company's new organizational structure. The following change is required:
Comportment Team_x needs to be moved under a new parent compartment, Project_B



The tenancy has the following policies defined for compartments Project_A and Project_B:
Policy1 Allow group G1 to manage instance-family in compartment HR:Project_A Policy2 Allow group G2 to manage instance-family in compartment HR:Project_B Which two statements describe the impacts after the compartment Team_x is moved?
A. Group G2 can now manage instance-families in compartment Project_B compartment Project_A and compartment Team_x
B. Group G1 can now manage instance-families in compartment Project_A but not in compartment Team_x
C. Group G1 can now manage instance-families in compartment project_A,compartment project_B and compartment Team_x

D. Group G2 can now manage instance-families in compartment Project_B and compartment Team_x
E. Group G2 can now manage instance-families in compartment Project_A but not in compartment Team_x
Answer: B,D (LEAVE A REPLY)
Understanding the Policy Implications When You Move a Compartment
After you move a compartment to a new parent compartment, the access policies of the new parent take effect and the policies of the previous parent no longer apply. Before you move a compartment, ensure that:
- You are aware of the policies that govern access to the compartment in its current position.
- You are aware of the polices in the new parent compartment that will take effect when you move the compartment.
Groups with Permissions in the Current Compartment Lose Access; Groups with Permissions in the Destination Compartment Gain Access

NEW QUESTION: 8
Your company recently adopted a hybrid cloud architecture which requires them to migrate some of their on-premises web applications to Oracle Cloud Infrastructure OCI). You created a Terraform template which automatically provisions OCI resources such as compute instances, load balancer, and a database instance. After running the stack using the terraform apply command, it successfully launched the compute Instances and the load balancer, but it failed to create a new database Instance with the following error:
Service error:NotAuthorizedOrNotFound. shape VM.Standard2.4 not found, http status code: 404
You discovered that the resource quotas assigned to your compartment prevent you from using VM.Standard2.4 instance shapes available in your tenancy. You edit the Terraform script and replace the shape with VM.Standard2.2.
Which option would you recommend to re-run the terraform command to have required OCI resources provisioned with the least effort?
A. terraform apply -target=ocl_database_db_system.db_system
B. terraform refresh -target=oci_database_db_system.db_system
C. terraform apply -auto-approve
D. terraform plan -target=oci_database_db_system.db_system
Answer: C (LEAVE A REPLY)
Command: refresh
The terraform refresh command is used to reconcile the state Terraform knows about (via its state file) with the real-world infrastructure. This can be used to detect any drift from the last-known state, and to update the state file.
This does not modify infrastructure, but does modify the state file. If the state is changed, this may cause changes to occur during the next plan or apply.
Command: plan

The terraform plan command is used to create an execution plan. Terraform performs a refresh, unless explicitly disabled, and then determines what actions are necessary to achieve the desired state specified in the configuration files.
This command is a convenient way to check whether the execution plan for a set of changes matches your expectations without making any changes to real resources or to the state Command: apply The terraform apply command is used to apply the changes required to reach the desired state of the configuration, or the pre-determined set of actions generated by a terraform plan execution plan.
Adding the -auto-approve option avoids having to type 'yes' at a confirmation prompt Note: Terraform will automatically refresh the state before running a command that would rely on it (such as plan, apply, destroy)

NEW QUESTION: 9
You have been asked to provision a new production environment on Oracle Cloud Infrastructure (OCI). After working with the solution architect you dockte that you are going to automate this process.
Which OCI service can help automate the provisioning of this new environment?
A. OCI Resource Manager
B. Oracle Container Engine for Kubernetes
C. Oracle Functions
D. OCI Streaming Service
Answer: (SHOW ANSWER)
Oracle Cloud Infrastructure Container Engine for Kubernetes is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications to the cloud. Use Container Engine for Kubernetes (sometimes abbreviated to just OKE) when your development team wants to reliably build, deploy, and manage cloud-native applications. You specify the compute resources that your applications require, and Container Engine for Kubernetes provisions them on Oracle Cloud Infrastructure in an existing OCI tenancy. Container Engine for Kubernetes uses Kubernetes - the open-source system for automating deployment, scaling, and management of containerized applications across clusters of hosts.

NEW QUESTION: 10
You are using Oracle Cloud Infrastructure (OCI) console to set up an alarm on a budget to track your OCI spending. Which two are valid targets for creating a budget In OCI?
A. Select Tenancy as the type of target for your budget.
B. Select Cost-Tracking Tags as the type of target for your budget.
C. Select Compartment as the type of target for your budget.
D. Select group as the type of target for your budget.
E. Select user as the type of target for your budget.
Answer: (SHOW ANSWER)
The following concepts are essential to working with budgets:

BUDGET
A monthly threshold you define for your Oracle Cloud Infrastructure spending. Budgets are set on cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments. Note: the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.
ALERT
You can define email alerts that get sent out for your budget. You can send a customized email message body with these alerts. Alerts are evaluated every 15 minutes, and can be triggered when your actual or your forecasted spending hits either a percentage of your budget or a specified set amount Select the target for your budget For budgets targeting a compartment: Select a target compartment for your budget from the Target Compartment drop-down list. Note that while the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.
For budgets targeting a cost-tracking tag: Select a tag namespaceSelect a target cost-tracking tag key.Enter a value for the cost-tracking tag.

NEW QUESTION: 11
Which technique does NOT help you get the optimal performance out of the Oracle Cloud Infrastructure (OC1) File Storage service?
A. Serialize operations to the file system to access consecutive blocks as much as possible.
B. Limit access to the same Availability Domain (AD) as the File Storage service where possible.
C. Right size compute instances from where file system is accessed based on their network capacity.
D. Store files across multiple directories in the file system.
E. Increase concurrency by using multiple threads, multiple clients, and multiple mount targets.
Answer: A (LEAVE A REPLY)
Oracle Cloud Infrastructure File Storage is a fully managed file storage service that can be accessed concurrently by thousands of compute instances.
To optimize the performance of File Storage, consider the following guidelines:
- While it is possible to access mount targets from any availability domain in a region, for optimal performance, place File Storage resources in the same availability domain as the Compute instances that access them.
- File Storage performance increases with parallelism. Increase concurrency by using multiple threads, multiple clients, and multiple mount targets. In particular, scalability will be greatest when clients and threads are accessing independent portions of the file system
- Use tools to run file operations in parallel. The File Storage engineering team has developed parallel tar and untar (puntar), parallel copy (parcp), and parallel remove (parrm) tools. These tools are available in the fss-parallel-tools package in Oracle Linux.

- The available bandwidth to a file system can significantly impact its performance. In Oracle Cloud Infrastructure, larger instances (more CPUs) are entitled to more network bandwidth. File Storage performance is best with Oracle bare metal instances or large VM shapes
- To minimize latency, clients, mount targets, and file systems should be in the same availability domain.
- For best performance, don't set any mount options such as rsize or wsize when mounting the file system. In the absence of these options, the system automatically negotiates optimal window sizes.
- Due to the limitations of Oracle Cloud Infrastructure's VNICs, each mount target is limited to about 600 MB/s of read or write traffic. If you have bandwidth-heavy workloads, consider spreading your workload across multiple mount targets after your file system exceeds 10 TB.

NEW QUESTION: 12
You launched a Linux compute Instance to host the new version of your company website via Apache HTTPS server on HTTPS (port 443).
The Instance is created in a public subnet along with other Instances. The default security list associated to the subnet is:

Ingress					*Egress*				
CIDR	IP Protocol	Source Port	Destination Port	State	CIDR	IP Protocol	Source Port	Destination Port	State
0.0.0.0/0	TCP	All	22	Stateful	0.0.0.0/0	All			Stateful
0.0.0.0/0	ICMP			Stateful					

You want to allow access to the company website from public Internet without exposing websites eventually hosted on the other instances In the public subnet.
Which two actions should you do?
A. Access the Linux instance via SSH and configure Iptables to allow HTTPS access on port 443.
B. Create a new security list with a stateful rule to allow ingress access on port 443 and associate it to the public subnet.
C. In default security list, add a stateful rule to allow ingress access on port 443.
D. Create a network security group, add a stateful rule to allow ingress access on port 443 and associate It to the public subnet that host the company website.
E. Create a network security group, add a stateful rule to allow ingress access on port 443 and associate it to the instance that host the company website.
Answer: A,D (LEAVE A REPLY)
The NSG is created and then displayed on the Network Security Group page in the compartment you chose. You can specify this NSG when creating or managing instances or other types of parent resources.

NEW QUESTION: 13
You have been contracted by a local e-commerce company to assist with enhancing their online shopping application. The application is currently deployed In a single Oracle Cloud Infrastructure

(OCI) region. The application utilizes a public load balancer, application servers in a private subnet and a database in a separate, private subnet.
The company would like to deploy another set of similar Infrastructure In a different OCI region that will act as standby site. In the event of a failure at the primary site, all customers should be routed to the failover site automatically.
After deploying the additional infrastructure within the second region, how should you configure automated failover requirements?
A. Create a new A record in DNS that points to the public load balancer at the secondary site. Create a CNAME for the sub-domain failover that will resolve to the new A record. Inform customers to prepend the website URL with failover If the primary site Is unavailable.
B. Create a load balancer policy in the Traffic Management service. Configure one answer for each site. Set the answer for the primary site with a weight of 10 and the answer for the secondary site with a weight of 100.
C. Create a failover policy in the Traffic Management service. Set the IP address of the public load balancer for the primary site in answer pool 1 Set the IP address of the public load balancer for the secondary site in answer pool 2. Define a health check to monitor both sites.
D. Deploy a new load balancer in the primary region. Create one backend set for the primary application servers and a second backend set for the standby application servers. Create a listener for the primary backend set with a timeout of 3 minutes. Create a listener for the secondary backend set with a timeout of 10 minutes.
Answer: C (LEAVE A REPLY)
You can leverage Traffic Management Steering Policies to provide automated failover between primary and secondary servers.

NEW QUESTION: 14
You have created a geolocation steering policy in the Traffic Management service, with this configuration.

What happens to requests that originate in Africa?
A. The traffic will be forwarded randomly to any of the pools mentioned in the rules.
B. The traffic will be dropped.

C. The traffic will be forwarded to Pool 1. If Pool 1 is not available, then will be forwarded to Pool 2.
D. The traffic will be forwarded at the same time to both Pool 1 and Pool 2.
Answer: B (LEAVE A REPLY)
The Oracle Cloud Infrastructure Traffic Management Steering Policies service is a critical component of DNS. Traffic Management Steering Policies enables you to configure policies to serve intelligent responses to DNS queries, meaning different answers (endpoints) may be served for the query depending on the logic the customer defines in the policy. Traffic Management Steering Policies can account for health of answers to provide failover capabilities, provide the ability to load balance traffic across multiple resources, and account for the location where the query was initiated to provide a simple, flexible and powerful mechanism to efficiently steer DNS traffic.
WORLDWIDE GEOLOCATION TREATMENT
You can divide your global users into geographically defined regions (for example, state/province level in NA, country level for rest of world) and steer customers to specified resources based on their location. This helps to ensure global, high performing internet resolution, and supports functions such as ring fencing. For example, keeping traffic from China in China and block traffic outside of China into China.

NEW QUESTION: 15
You have a group of developers who launch multiple VM.Standard2.2 compute Instances every day into the compartment Dev. As a result your OCI tenancy quickly hit the service limit for this shape. Other groups can no longer create new instances using VM.Standard2.2 shape.
of this, your company has Issued a new mandate that the Dev compartment must include a quota to allow for use of only 20 VM.Standar2.2 shapes per Availability Domain. Your solution should not affect any other compartment In the tenancy.
Which quota statement should be used to implement this new requirement?
A)

```
zero compute quotas in tenancy
set compute quota vm-standard2-2-count to 20 in tenancy dev
```

B)

```
zero compute quotas in tenancy
set compute quota vm-standard2-2-count to 20 in compartment dev
```

C)

```
set compute quota vm-standard2-2-count to 20 in compartment dev
```

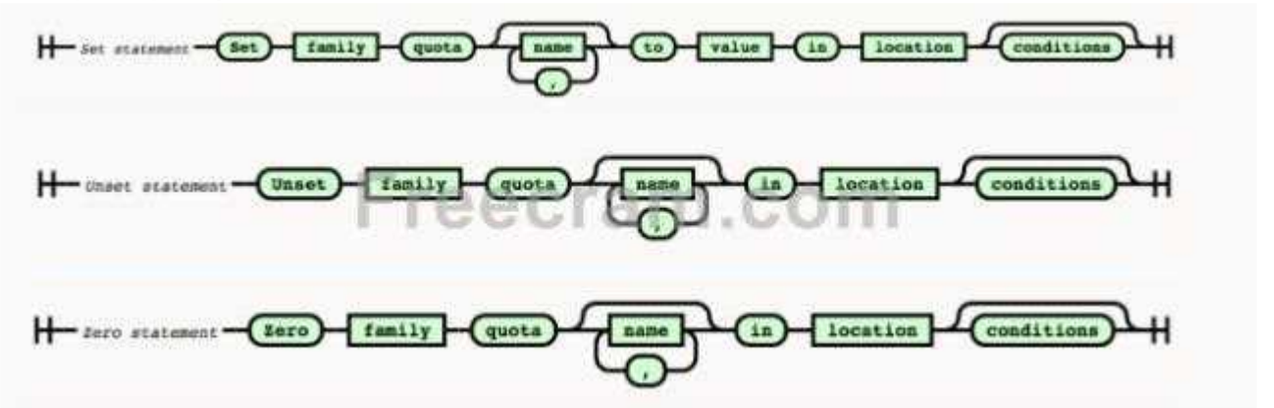
D)

```
set compute quota vm-standard2-2-count to 20 in compartment dev where request.region = us-phoenix-1
```

E)

```
zero compute quotas in tenancy
set compute quota vm-standard2-2-count to 20 in tenancy dev
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E
Answer: (SHOW ANSWER)
Compartment quotas give tenant and compartment administrators better control over how resources are consumed in Oracle Cloud Infrastructure.
There are three types of quota policy statements:
- set - sets the maximum number of a cloud resource that can be used for a compartment
- unset - resets quotas back to the default service limits
- zero - removes access to a cloud resource for a compartment
The quota policy statements look like this:



To sets the quota for VM.Standard2.2 Compute instances to 20 on compartment Dev set compute quota vm-standard2-2-count to 20 in compartment dev No need to make a whitelist, by setting every quota in a family to zero zero compute quotas in tenancy

NEW QUESTION: 16
A subscriber of on Oracle Cloud Infrastructure (OCI) Notifications service topic complained about not receiving messages from the service. Which of the following options can help you debug this issue?
A. If OCI Notifications service does not receive an acknowledgement from a subscription endpoint, the service tries to redeliver messages for up to two hours. Configure an alarm on the NumberofNotificationFailed metric through the OCI Monitoring service to help debug the issue.
B. If OCI Notifications service does not receive an acknowledgement from a subscription endpoint, the service drops the message. Confirm that the subscriber is always online to receive messages to help debug the issue.
C. If OCI Notifications service does not receive an acknowledgement from a subscription endpoint, the service tries to redeliver messages for up to one day. Make sure that the subscriber is online at least once a day to help debug the Issue.
D. If OCI Notifications service does not receive an acknowledgement from a subscription endpoint, check the NumberofNotificationFailed metric through the OCI Monitoring service for

failed messages. Copy these messages to an OCI Object Storage bucket. Make sure the subscriber has the required credentials to access this bucket to help debug the Issue

Answer: A (LEAVE A REPLY)

The Oracle Cloud Infrastructure Notifications service broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally. Use Notifications to get notified when event rules are triggered or alarms are breached, or to directly publish a message.

If Notifications doesn't receive an acknowledgement from a subscription endpoint, the service tries to redeliver messages for up to two hours. This situation can occur when the endpoint is offline.

You can configure an alarm on the NumberOfNotificationFailed metric through the Monitoring service

NEW QUESTION: 17

You have been asked to investigate a potential security risk on your company's Oracle Cloud Infrastructure (OCI) tenancy. You decide to start by looking through the audit logs for suspicious activity.

How can you retrieve the audit logs using the OCI Command Line Interface (CLI)?

A. oci audit event list --start-time $start-time --end-time $end-time --compartment-id $compartment-id

B. oci audit event list --start-time $start-time --end-time $end-time --tenancy-id $tenancy-id

C. oci audit event list --start-time $start-time --compartment-id $compartment-id

D. oci audit event list --end-time $end-time --compartment-id $compartment-id

Answer: A (LEAVE A REPLY)

Retrieving Audit events

In order to make use of audit events, the first step is to retrieve and store audit events. Let's take a look into the ways in which an Audit event can be retrieved:

Oracle Cloud Infrastructure Web Console - With user credentials, customers can log in to the web console to access the Audit service. For example, when customers are trying the service for the first time; this helps with a first look into a handful of events.

Oracle Cloud Infrastructure CLI [3] - With CLI customers can make use of the service to retrieve events for a defined compartment and for a region specified as per CLI's config. The CLI command would look like:
#oci audit event list --start-time $start-time --end-time $end-time --compartment-id $compartment-id Oracle Cloud Infrastructure SDKs [4][5] - With SDKs customers can choose a supported language and retrieve Audit events with the ListEvents API [6]. For production use cases, this would be the best suitable option.
https://blogs.oracle.com/cloud-infrastructure/operating-oracle-cloud-infrastructure-tenancies-retrieving-audit-logs

NEW QUESTION: 18
You have been tasked with allocating an identity to one of your compute instances that needs to retrieve and process static files that are stored in an Object Storage bucket. After creating a dynamic group with a matching rule that specifies the OCID of the compute instance, you discover the that API calls are failing.
Which step should you take to resolve this issue?
A. Create IAM policies to permit users in these groups to make API calls against Oracle Cloud Infrastructure services.
B. Initial credentials must be initialized using OCI console for the Instance in dynamic group. This can be a bulk operation.
C. Create IAM policies to permit instances in these groups to make API calls against Oracle Cloud Infrastructure services.
D. Once instance are in dynamic group no additional steps are required.
Answer: (SHOW ANSWER)
Dynamic groups allow you to group Oracle Cloud Infrastructure computer instances as "principal" actors (similar to user groups). You can then create policies to permit instances to make API calls against Oracle Cloud Infrastructure services. When you create a dynamic group, rather than adding members explicitly to the group, you instead define a set of matching rules to define the group members.

NEW QUESTION: 19
Several development teams in your company have each been provided with a budget and a dedicated compartment to be used for testing purpose u are asked to help them to control the costs and avoid any overspending.
What should you do?
A. Associate a Budget Tag to each resource with monthly budget amount and use that Information to prepare a weekly report to send to each team.
B. Contact Oracle support and ask them to associate the monthly budget with the Service Limits In every region for which your tenancy is subscribed. The tenancy administrator will receive an alert email from Oracle when the limit Is reached.

C. Associate a Budget Tag to each compartment with the monthly budget amount and set an alert rule to notify the developers' teams when they reached a specific percentage of the budget
D. Configure a Quota for each compartment to prevent provisioning of any bare metal instances.
Answer: C (LEAVE A REPLY)
Budgets are set on cost-tracking tags or on compartments (including the root compartment) to track all spending in that cost-tracking tag or for that compartment and its children.
The following concepts are essential to working with budgets:
BUDGET
A monthly threshold you define for your Oracle Cloud Infrastructure spending. Budgets are set on cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments. Note: the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.
ALERT
You can define email alerts that get sent out for your budget. You can send a customized email message body with these alerts. Alerts are evaluated every 15 minutes, and can be triggered when your actual or your forecasted spending hits either a percentage of your budget or a specified set amount.
Using Cost-Tracking Tags
You can use cost-tracking tags to help manage costs in your tenancy. Use cost-tracking tags to do any of the following:
- Filter projected costs
- Set budgets
You can only use cost-tracking tag with defined tags. You cannot specify free-form tags as cost-tracking tags.
You can set email alerts on your budgets. You can set alerts that are based on a percentage of your budget or an absolute amount, and on your actual spending or your forecast spending.

NEW QUESTION: 20
You need to set up daily Incremental backups of your database In Oracle Cloud Infrastructure (OCI) Database Service. The backups need to be retained for at least 50 days.
Which of the following method allows you do accomplish this Is an efficient and cost effective manner?
A. Enable automatic backups and choose the preset retention period of 60 days.
B. Enable automatic backups and set the retention period to 50 days.
C. Set up a cron job with OCI Database Service CreateBackuP API call to take periodic full-backups to OCI Object Store. Delete backups older than 50 days.
D. Use Recovery Manager (RMAN) to take backups to an OCI Object Store bucket. Delete backups older than 50 days.
Answer: (SHOW ANSWER)

When you enable the Automatic Backup feature, the service creates daily incremental backups of the database to Object Storage. The first backup created is a level 0 backup. Then, level 1 backups are created every day until the next weekend. Every weekend, the cycle repeats, starting with a new level 0 backup.
Backup Retention
If you choose to enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The system automatically deletes your incremental backups at the end of your chosen retention period.
https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm Also, you can u se Recovery Manager (RMAN) to manage backups of your Bare Metal or Virtual Machine DB system database to your own Object Storage
https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm

NEW QUESTION: 21
You have been brought In to help secure an existing application that leverages Object Storage buckets to distribute content. The data is currently being shared from public buckets and the security team Is not satisfied with this approach. They have stated that all data must be stored In storage buckets. Your application should be able to provide secure access to the dat a. The URL that is provided for access to the data must be rotated every 30 days.
Which design option will meet these requirements?
A. Use Pre-Authenticated request, even though there will be multiple URLs this will provide better security.
B. Create a private bucket only to share the data.
C. Create a new group and map users to this group, create a IAM policy providing access to Object Storage service only to this group. Users can then simply login to OCI console and retrieve needed flies.
D. Create multiple bucket and classify them as Public and Private. Use public bucket for non-sensitive data and private bucket for sensitive data.
Answer: A (LEAVE A REPLY)
Pre-authenticated request has expiration date and can generate new unique URL every 30 days

NEW QUESTION: 22
What is a key benefit of using Oracle Cloud Infrastructure's Resource Manager for your Terraform provisioning and management activities?
A. Resource Manager has administrative privileges by design. Even if your IAM user does not have access, you can leverage Resource Manage provision new resources to any compartment in the Tenancy.
B. You can use Resource Manager to identify and maintain an Inventory of all Compute and Database Instances across your tenancy.
C. You can use Resource Manager to apply patches to all existing Oracle Linux Instances In a specified compartment.

D. Resource Manager manages the Terraform state file for your infrastructure and locks the file so that only one Job at a time can run on a given stack.

Answer: (SHOW ANSWER)

Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. Using Terraform, Resource Manager helps you install, configure, and manage resources through the "infrastructure-as-code" model.

A Terraform configuration codifies your infrastructure in declarative configuration files. Resource Manager allows you to share and manage infrastructure configurations and state files across multiple teams and platforms. This infrastructure management can't be done with local Terraform installations and Oracle Terraform modules alone.

JOB: Instructions to perform the actions defined in your configuration. Only one job at a time can run on a given stack; further, you can have only one set of Oracle Cloud Infrastructure resources on a given stack. To provision a different set of resources, you must create a separate stack and use a different configuration.

The following image represents a generalized view of the Resource Manager workflow.