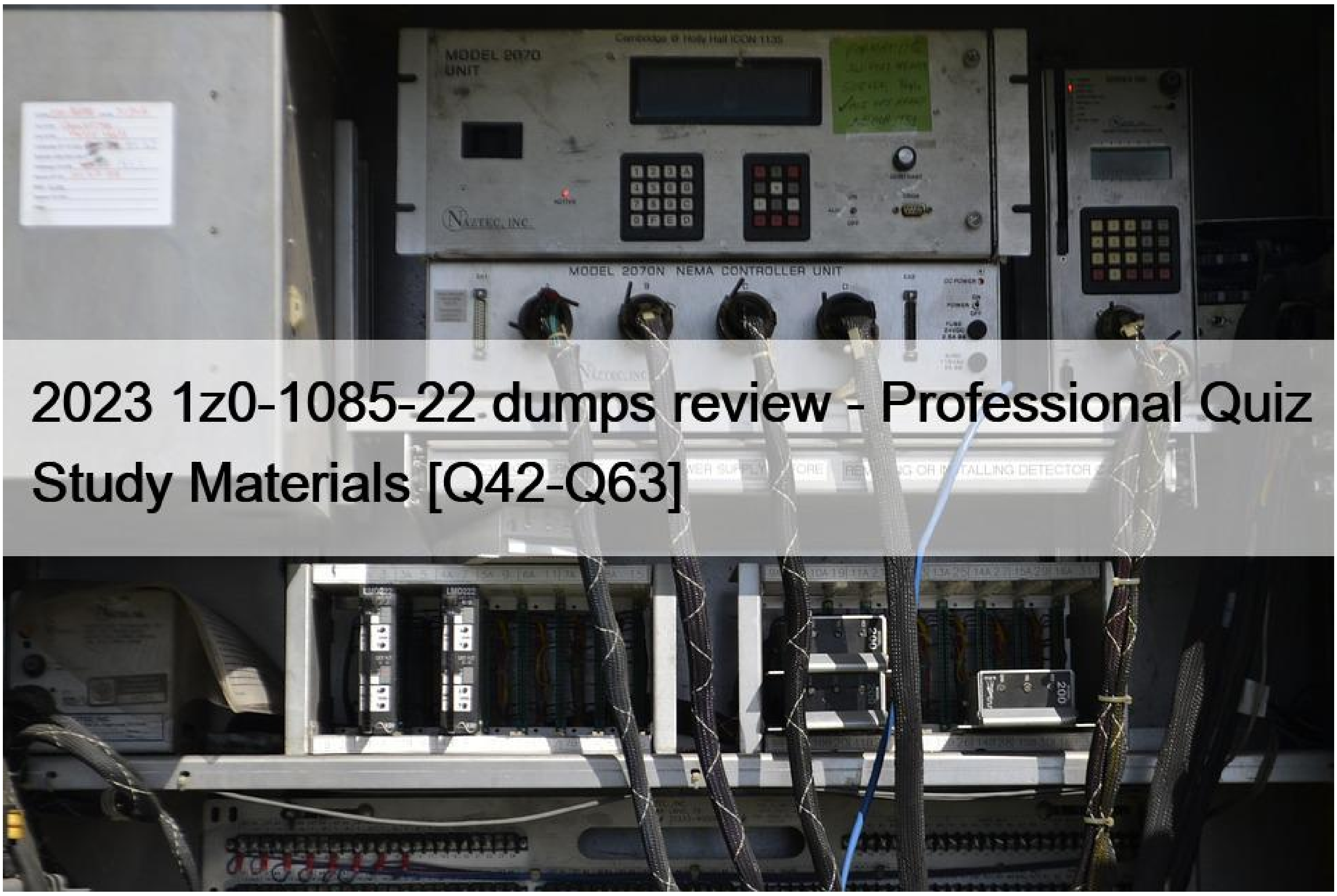
2023 1z0-1085-22 dumps review - Professional Quiz Study Materials [Q42-Q63



2023 1z0-1085-22 dumps review - Professional Quiz Study Materials
1z0-1085-22 Test Prep Training Practice Exam Questions Practice Tests

NEW QUESTION 42

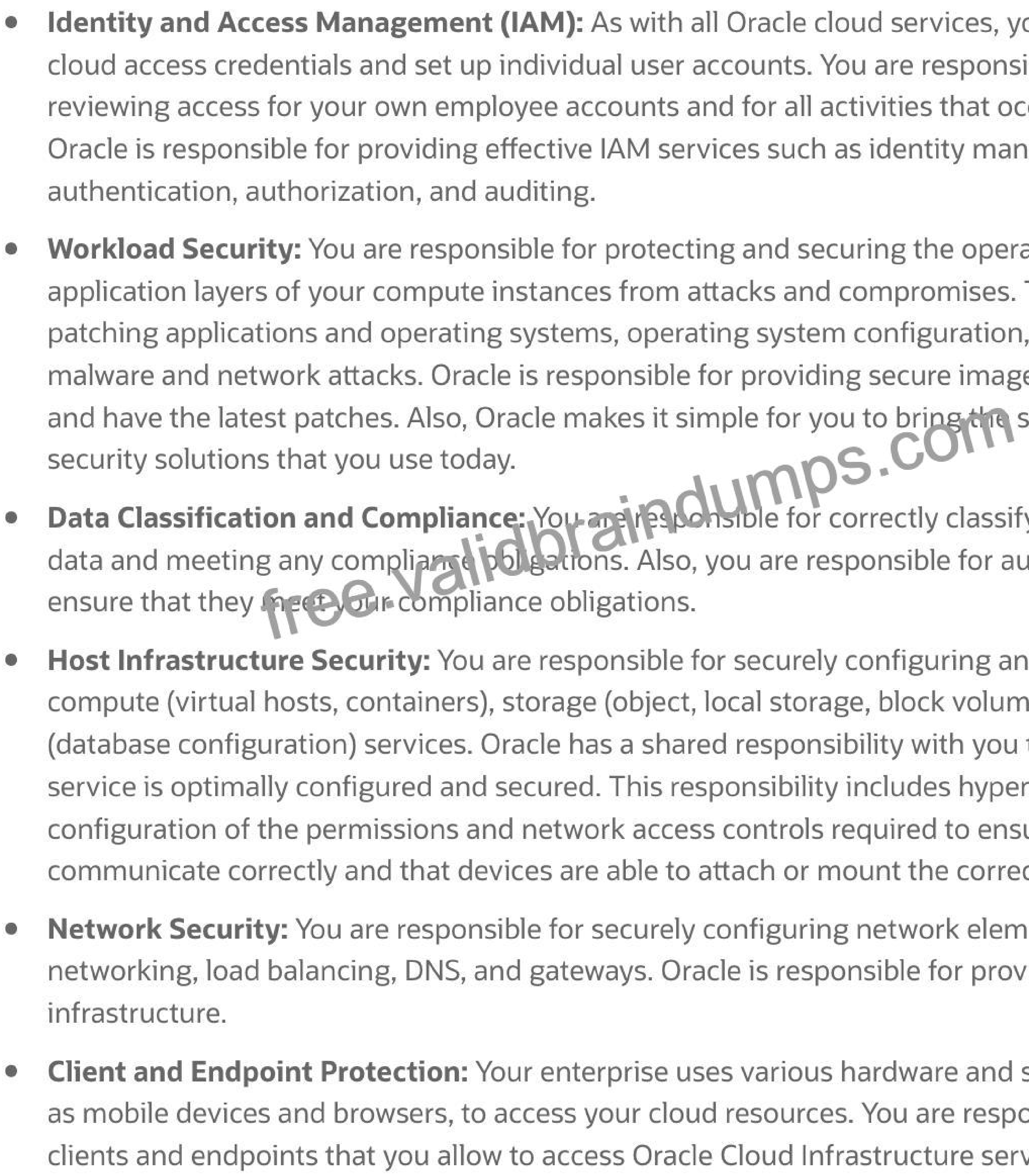
What is Oracle&#8217;s responsibility according to the Oracle Cloud Infrastructure (OCI) shared-security model?
* Configuring OCI services securely
* Data classification and compliance
* Securing application workloads
* Security of data center facilities
Oracle&#8217;s mission is to build cloud infrastructure and platform services for your business to have effective and manageable security to run your mission-critical workloads and store your data with confidence.

Oracle Cloud Infrastructure offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for you to securely run your workloads in Oracle Cloud Infrastructure, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and you are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and Oracle.

In a shared, multi-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data-center facilities, and hardware and software systems) and you are responsible for securing your workloads and configuring your services (such as compute, network, storage, and database) securely.

In a fully isolated, single-tenant, bare metal server with no Oracle software on it, your responsibility increases as you bring the entire software stack (operating systems and above) on which you deploy your applications. In this environment, you are responsible for securing your workloads, and configuring your services (compute, network, storage, database) securely, and ensuring that the software components that you run on the bare metal servers are configured, deployed, and managed securely.

More specifically, your and Oracle&#8217;s responsibilities can be divided into the following areas:



- **Identity and Access Management (IAM):** As with all Oracle cloud services, yo cloud access credentials and set up individual user accounts. You are responsi reviewing access for your own employee accounts and for all activities that oc Oracle is responsible for providing effective IAM services such as identity man authentication, authorization, and auditing.
- **Workload Security:** You are responsible for protecting and securing the opera application layers of your compute instances from attacks and compromises. T patching applications and operating systems, operating system configuration, malware and network attacks. Oracle is responsible for providing secure image and have the latest patches. Also, Oracle makes it simple for you to bring the s security solutions that you use today.
- **Data Classification and Compliance:** You are responsible for correctly classify data and meeting any compliance obligations. Also, you are responsible for au ensure that they meet your compliance obligations.
- **Host Infrastructure Security:** You are responsible for securely configuring an compute (virtual hosts, containers), storage (object, local storage, block volum (database configuration) services. Oracle has a shared responsibility with you t service is optimally configured and secured. This responsibility includes hyper configuration of the permissions and network access controls required to ensu communicate correctly and that devices are able to attach or mount the correc
- **Network Security:** You are responsible for securely configuring network elem networking, load balancing, DNS, and gateways. Oracle is responsible for prov infrastructure.
- **Client and Endpoint Protection:** Your enterprise uses various hardware and s as mobile devices and browsers, to access your cloud resources. You are respo clients and endpoints that you allow to access Oracle Cloud Infrastructure serv

NEW QUESTION 43

Which security issue CANNOT be Identified by using Oracle Cloud Infrastructure (OCI) Vulnerability Scanning Service (VSS)?
* OS packages that require updates and patches to address vulnerabilities
* Ports that are unintentionally left open
* OS configurations that hackers might exploit
* Cross-Site scripting (XSS)

NEW QUESTION 44

Which Oracle Cloud Infrastructure (OCI) database solution will be most economical for a customer looking to have the elasticity of the cloud with minimal administration and maintenance effort for their DBA team?
* OCI Bare Metal DB Systems
* OCI Virtual Machine DB Systems
* OCI Exadata DB Systems.
* OCI Autonomous Database
Exadata DB systems allow you to leverage the power of Exadata within the Oracle Cloud Infrastructure. An Exadata DB system consists of a base system, quarter rack, half rack, or full rack of compute nodes and storage servers, tied together by a high-speed, low-latency InfiniBand network and intelligent Exadata software. You can configure automatic backups, optimize for different workloads, and scale up the system to meet increased demands.

Oracle now offers the Zero Downtime Migration service, a quick and easy way to move on-premises Oracle Databases and Oracle Cloud Infrastructure Classic databases to Oracle Cloud Infrastructure. You can migrate databases to the following types of Oracle Cloud Infrastructure systems: Exadata, Exadata Cloud@Customer, bare metal, and virtual machine.

Zero Downtime Migration leverages Oracle Active Data Guard to create a standby instance of your database in an Oracle Cloud Infrastructure system. You switch over only when you are ready, and your source database remains available as a standby. Use the Zero Downtime Migration service to migrate databases individually or at the fleet level. See Move to Oracle Cloud Using Zero Downtime Migration for more information.

NEW QUESTION 45

Which three services Integrate with Oracle Cloud Infrastructure (OCI) Key Management?
* Functions
* Block Volume
* Object Storage
* Auto Scaling
* Identity and Access Management
* File Storage
DATA ENCRYPTION

Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management The Oracle Cloud Infrastructure 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. 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.

The File Storage service encrypts all file system and snapshot data at rest. By default all file systems are encrypted using Oracle-managed encryption keys. You have the option to encrypt all of your file systems using the keys that you own and manage using the Vault service.

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.

Reference:

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Concepts/overview.htm

https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm

https://docs.cloud.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm Oracle Cloud Infrastructure Key Management is a managed service that enables you to encrypt your data using keys that you control.

IAM, Autoscaling and functions cannot be used with Key Management and hence are incorrect options.

NEW QUESTION 46

Oracle Cloud Infrastructure Budgets can be set on which two options?
* Free-form tags
* Compartments
* Tenancy
* Virtual Cloud Network
* Cost-tracking tags
A budget can be used to set soft limits on your Oracle Cloud Infrastructure spending. You can set alerts on your budget to let you know when you might exceed your budget, and you can view all of your budgets and spending from one single place in the Oracle Cloud Infrastructure console.

How Budgets Work:

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.

All budgets alerts are evaluated every 15 minutes. To see the last time a budget was evaluated, open the details for a budget. You will see fields that show the current spend, the forecast and the &#8220;Spent in period&#8221; field which shows you the time period over which the budget was evaluated. When a budget alert fires, the email recipients configured in the budget alert receive an email.

NEW QUESTION 47

Which statement is correct regarding the oracle cloud infrastructure Compute services?
* When you stop a compute instance, all data on the boot volume is lost
* You can attach a maximum of one public to each compute instance
* You can launch either virtual machines or bare metal instances
* You cannot attach a block volume to a compute instance
Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances

. You can launch instances as needed to meet your compute and application requirements. After you launch an instance, you can access it securely from your computer, restart it, attach and detach volumes, and terminate it when you&#8217;re done with it. Any changes made to the instance&#8217;s local drives are lost when you terminate it. Any saved changes to volumes attached to the instance are retained.

Oracle Cloud Infrastructure offers both bare metal and virtual machine instances:

1) Bare Metal: A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

2) Virtual Machine: A virtual machine (VM) is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are ideal for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine.

An Oracle Cloud Infrastructure VM compute instance runs on the same hardware as a bare metal instance, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure.

NEW QUESTION 48

You were recently assigned to manage a project to deploy Oracle E-Business Suite on Oracle Cloud Infrastructure (OCI). The application will require a database, several servers, and a shared file system.

Which three OCI services are best suited for this project?
* OCI virtual or Bare Metal DB Systems
* OCI Streaming Service
* Object Storage Service
* Virtual Machine (VM) or Bare Metal (BM) compute Instances
* File Storage Service
* Oracle Container Engine for Kubernetes
https://docs.oracle.com/en/solutions/deploy-ebusiness-suite-oci/index.html#GUID-0CA881FD-D96F-4885-BC77-62E3A66EFF95

NEW QUESTION 49

Which is NOT a valid target for the Oracle Cloud Infrastructure (OCI) Cloud Guard service?
* Region
* Tenancy
* Root Compartment
* Compartment and its sub-compartments

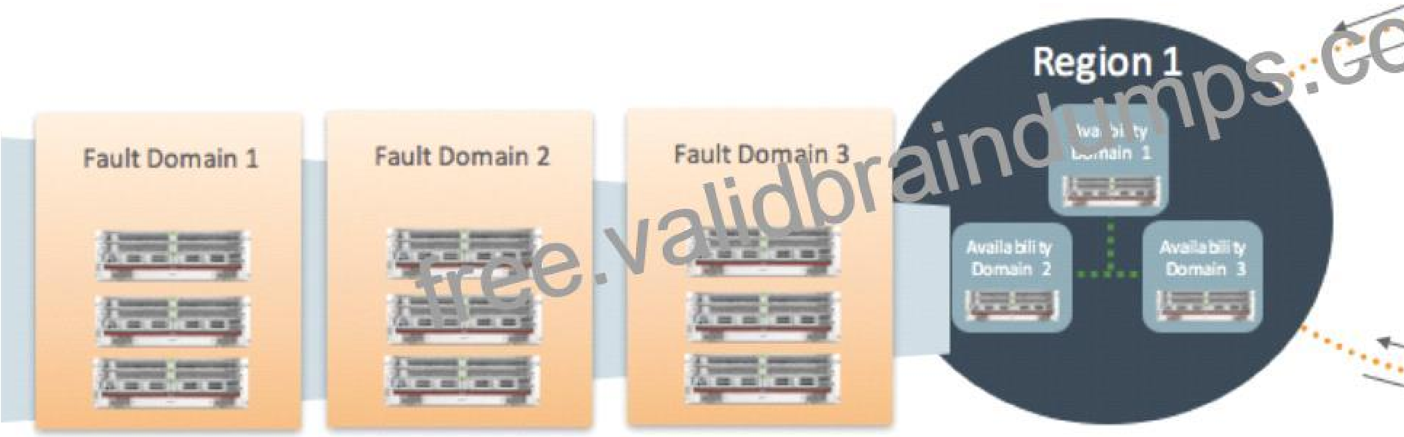
NEW QUESTION 50

Which capability can be used to protect against unexpected hardware or power supply failures within an availability domain?
* Fault Domains
* Compartments
* Top of Rack Switches
* Power Distribution Units
A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains provide anti-affinity: they let you distribute your instances so that the instances are not on the same physical hardware within a single availability domain. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains. In addition, the physical hardware in a fault domain has independent and redundant power supplies, which prevents a failure in the power supply hardware within one fault domain from affecting other fault domains.

Usually fault domains to do the following things:

1) Protect against unexpected hardware failures or power supply failures.

2) Protect against planned outages because of Compute hardware maintenance.



NEW QUESTION 51

Oracle Cloud Infrastructure is complement with which three industry standard?
* USA E-WALLED
* PRACE UK
* HIPPA
* PCI-DSS
* IG Toolkit-UK
https://www.oracle.com/cloud/cloud-infrastructure-compliance/

NEW QUESTION 52

Which TWO are valid regarding Oracle Cloud Infrastructure (OCI) Virtual Cloud Network (VCN) peering?

(Choose all correct answers)
* Peered VCNs can have overlapping classless inter-domain routing (CIDR).
* Peered VCNs can exist in the same OCI region.
* Peered VCNs can exist in different OCI regions.
* A VCN peering connection is a VPN based connection.
* Peered VCNs need to be part of the same OCI tenancy.

NEW QUESTION 53

you are analyzing your Oracle Cloud Infrastructure (OCI) usage with Cost Analysis tool in OCI Console.

Which is not a default feature of the tool?
* Filter costs by applications
* Filter costs by compartments
* Filter costs by tags
* Filter costs by date
You can filter Costs Analysis Tools by following three ways

To filter costs by dates

To filter costs by tags

To filter costs by compartments

Reference:

https://www.oracle.com/a/ocom/docs/cloud/ops-billing-100.pdf

NEW QUESTION 54

Which is NOT a benefit associated with Oracle Autonomous Database?
* Self-repairing
* Self-loading
* Self-securing
* Self-driving

NEW QUESTION 55

Which TWO statements are true regarding Oracle Cloud Infrastructure (OCI) Regions?

(Choose al correct answers)
* Some regions provide multiple subregions.
* Some regions provide multiple availability domains.
* Some regions provide a single availability domain.
* Some regions only provide test/dev environments.
* Some regions provide a single fault domain.

NEW QUESTION 56

Which two security capabilities are offered by Oracle Cloud Infrastructure?
* Always on data encryption for data-at-rest.
* Certificate Management service
* Captcha
* Key Management service
* Managed Active Directory service

Oracle Cloud Infrastructure&#8217;s security approach is based on seven core pillars. Each pillar has multiple solutions designed to maximize the security and compliance of the platform and to help customers to improve their security posture.

High Availability: Offer fault-independent data centers that enable high-availability scale-out architectures and are resilient against network attacks, ensuring constant uptime in the face of disaster and security attack.

Customer Isolation: Allow customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle&#8217;s staff.

Data Encryption: Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements with respect to cryptographic algorithms and key management.

Security Controls: Offer customers effective and easy-to-use application, platform, and network security solutions that allow them to protect their workloads, have a secure application delivery using a global edge network, constrain access to their services, and segregate operational responsibilities to reduce the risk associated with malicious and accidental user actions.

Visibility: Offer customers comprehensive log data and security analytics that they can use to audit and monitor actions on their resources, allowing them to meet their audit requirements and reduce security and operational risk.

Secure Hybrid Cloud: Enable customers to use their existing security assets, such as user accounts and policies, as well as third-party security solutions, when accessing their cloud resources and securing their data and application assets in the cloud.

Verifiably Secure Infrastructure: Follow rigorous processes and use effective security controls in all phases of cloud service development and operation. Demonstrate adherence to Oracle&#8217;s strict security standards through third-party audits, certifications, and attestations. Help customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

Reference:

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

NEW QUESTION 57

In what two ways does Oracle Cloud Infrastructure (OCI) offer industry leading price-performance?
* OCI leverages advanced encryption that results In fast performance
* With OCI, pricing Is low and predictable across all regions and services.
* OCI hypervisor provides Industry loading performance.
* OCI backs performance claims with Service Level Agreements.
* OCI does not over subscribe CPU, but only memory.

OCI leverages advanced encryption that leads to fast performance, OCI does not over subscribe CPU, but only memory, and OCI hypervisor provides industry leading performance are WRONG.

However, OCI does back claims with SLAs and offers predictable pricing for all services.

Reference:

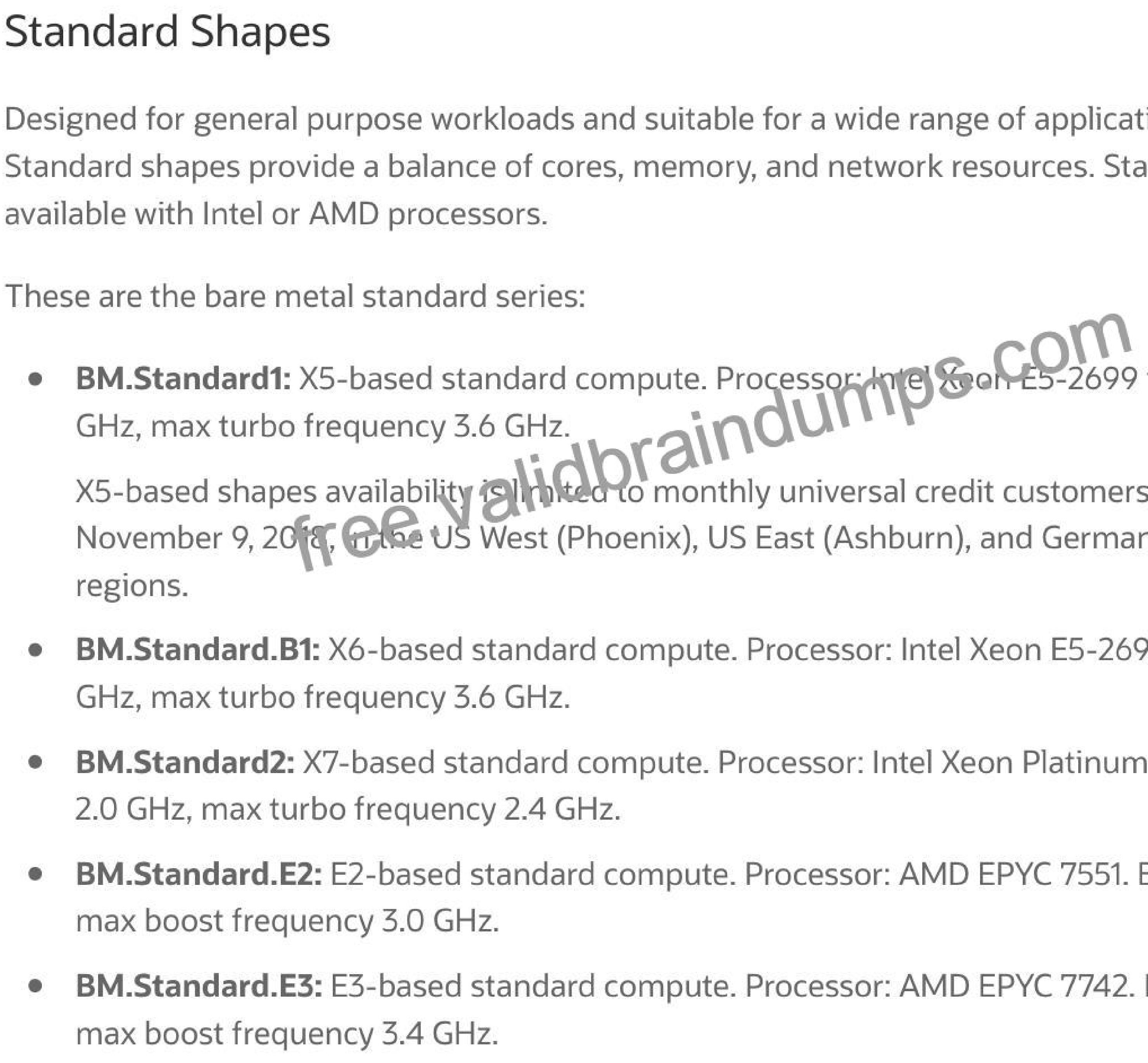
https://www.oracle.com/in/cloud/pricing.html

NEW QUESTION 58

Which Oracle Cloud Infrastructure compute shapes does not incur instance billing in a STOPPED state?
* Dense I/O
* Standard
* GPU
* HPC
Explanation

A shape is a template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance.

Standard shapes don&#8217;t incur costs in a STOPPED state.



Standard Shapes

Designed for general purpose workloads and suitable for a wide range of applicati
Standard shapes provide a balance of cores, memory, and network resources. Sta
available with Intel or AMD processors.

These are the bare metal standard series:

- **BM.Standard1:** X5-based standard compute. Processor: Intel Xeon E5-2699 v
GHz, max turbo frequency 3.6 GHz.

  X5-based shapes availability is limited to monthly universal credit customers
November 9, 2018, in the US West (Phoenix), US East (Ashburn), and Germar
regions.
- **BM.Standard.B1:** X6-based standard compute. Processor: Intel Xeon E5-269
GHz, max turbo frequency 3.6 GHz.
- **BM.Standard2:** X7-based standard compute. Processor: Intel Xeon Platinum
2.0 GHz, max turbo frequency 2.4 GHz.
- **BM.Standard.E2:** E2-based standard compute. Processor: AMD EPYC 7551. E
max boost frequency 3.0 GHz.
- **BM.Standard.E3:** E3-based standard compute. Processor: AMD EPYC 7742. I
max boost frequency 3.4 GHz.

NEW QUESTION 59

Which Oracle Cloud Infrastructure (OCI) capability allows you to set up alerts to notify you if a budget forecast exceeds or spending surpasses a certain amount?
* Cost Analysis
* Budget
* Events
* Monitoring

NEW QUESTION 60

Which should you use to distribute Incoming traffic between a set of web servers?
* Load Balances
* Internet Gateway
* Autoscallng
* Dynamic Routing Gateway
The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth.

A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability. You can configure multiple load balancing policies and application-specific health checks to ensure that the load balancer directs traffic only to healthy instances. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance.

HOW LOAD BALANCING WORKS:

The Load Balancing service enables you to create a public or private load balancer within your VCN. A public load balancer has a public IP address that is accessible from the internet. A private load balancer has an IP address from the hosting subnet, which is visible only within your VCN. You can configure multiple listeners for an IP address to load balance transport Layer 4 and Layer 7 (TCP and HTTP) traffic. Both public and private load balancers can route data traffic to any backend server that is reachable from the VCN.

1) Public Load Balancer

To accept traffic from the internet, you create a public load balancer. The service assigns it a public IP address that serves as the entry point for incoming traffic. You can associate the public IP address with a friendly DNS name through any DNS vendor.

A public load balancer is regional in scope. If your region includes multiple availability domains, a public load balancer requires either a regional subnet (recommended) or two availability domain-specific (AD-specific) subnets, each in a separate availability domain. With a regional subnet, the Load Balancing service creates a primary load balancer and a standby load balancer, each in a different availability domain, to ensure accessibility even during an availability domain outage. If you create a load balancer in two AD-specific subnets, one subnet hosts the primary load balancer and the other hosts a standby load balancer. If the primary load balancer fails, the public IP address switches to the secondary load balancer. The service treats the two load balancers as equivalent and you cannot specify which one is &#8220;primary&#8221;.

Whether you use regional or AD-specific subnets, each load balancer requires one private IP address from its host subnet. The Load Balancing service supplies a floating public IP address to the primary load balancer. The floating public IP address does not come from your backend subnets.

If your region includes only one availability domain, the service requires just one subnet, either regional or AD-specific, to host both the primary and standby load balancers. The primary and standby load balancers each require a private IP address from the host subnet, in addition to the assigned floating public IP address. If there is an availability domain outage, the load balancer has no failover.

2) Private Load Balancer

To isolate your load balancer from the internet and simplify your security posture, you can create a private load balancer. The Load Balancing service assigns it a private IP address that serves as the entry point for incoming traffic.

When you create a private load balancer, the service requires only one subnet to host both the primary and standby load balancers. The load balancer can be regional or AD-specific, depending on the scope of the host subnet. The load balancer is accessible only from within the VCN that contains the host subnet, or as further restricted by your security rules.

The assigned floating private IP address is local to the host subnet. The primary and standby load balancers each require an extra private IP address from the host subnet.

If there is an availability domain outage, a private load balancer created in a regional subnet within a multi-AD region provides failover capability. A private load balancer created in an AD-specific subnet, or in a regional subnet within a single availability domain region, has no failover capability in response to an availability domain outage.

NEW QUESTION 61

Which TWO are valid regarding the Oracle Cloud Infrastructure (OCI) Logging service?

(Choose all correct Answers)
* It enables you to analyze cloud resources using custom metrics.
* It is a centralized single pane of glass for all logs in a tenancy.
* It enables you to monitor cloud resources using metrics and alarms.
* It can index, enrich, and aggregate log data from application.
* It can analyze critical diagnostic information that describes how resources are performing and being accessed.

NEW QUESTION 62

Oracle cloud Infrastructure is compliant with which three industry standards?
* SOC 1 Type 2 and SOC 2 Type 2 attestations
* NERC Critical Infrastructure Protection Standards
* Health Insurance Portability and Accountability Act (HIPAA)
* ISO 27001:2013 certification
* Health Care Compliance Association (HCCA)
Here is the official list of all industry standards that OCI complies with :
https://www.oracle.com/in/cloud/cloud-infrastructure-compliance/

NEW QUESTION 63

Which is NOT considered a security resource within Oracle Cloud Infrastructure?
* Network Security Group
* Web Application Firewall
* File Storage Service
* Security Lists
Oracle Cloud Infrastructure File Storage service provides a durable, scalable, secure, enterprise-grade network file system. You can connect to a File Storage service file system from any bare metal, virtual machine, or container instance in your Virtual Cloud Network (VCN).

You can control the access of the file system from FSS by applying some security rules and others but the services it self not related to security but it related to shared storage Reference:

https://docs.cloud.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm

Oracle 1z0-1085-22 Exam Syllabus Topics:

TopicDetailsTopic 1- Describe OCI App Dev services- Describe OCI Compute servicesTopic 2- Describe OCI Identity and Access Management services- Discuss OCI Regions and Availability DomainsTopic 3- Explain the OCI Pricing model- Explain the OCI Security modelTopic 4- Describe OCI Hybrid offerings- Describe OCI Storage servicesTopic 5- Describe OCI Observability and Management services- Describe the key features and components of OCITopic 6- Explain the OCI SLA and Support model- Describe OCI Networking servicesTopic 7- Describe OCI Analytics and AI services- Describe OCI Security services

Exam Questions Answers Braindumps 1z0-1085-22 Exam Dumps PDF Questions: https://www.validbraindumps.com/1z0-1085-22-exam-prep.html]