Cloud Computing Final Assessment Questionnaires

Topic Cloud Concepts,IAM,Application Security&BC DR

Name	
Registration No	
Class	**Cloud Computing- Section-A**
Batch	**4**

Q1.What is cloud computing or Cloud or Cloud Characteristics ?

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

Q2: What is the difference between virtualization and Cloud Computing?

- virtualization abstracts resources, but it typically lacks the orchestration to pool them together and deliver them to customers on demand, instead relying on manual processes.
- Cloud Computing uses Virtualization tools but it have both abstraction and Orchestration or Cloud computing uses virtualization to create resource pools of compute,storage,networks and memory and then uses orchestration or automation via APIs to deliver them to customers on demand .

Q3: Why cloud are multitenants or What is multi-tenancy in the cloud?

Cloud underlying infrastructure is shared by multiple customers therefore cloud are multi tenants in nature .This feature of cloud is driven by the concept of economy of scale or resource pooling to reduce the cost for its customers or cloud users.

- Clouds are *multitenant* by nature.
- Multiple different consumer constituencies share the same pool of resources but are *segregated* and *isolated* from each other.
- Segregation allows the cloud provider to divvy up resources to the different groups
- Isolation ensures they can’t see or modify eachother’s assets.

Q4 Ex[lain cloud Characteristics ,service models and deployment models?

Cloud Computing Final Assessment Questionnaires

1. **Cloud Characteristics:**

Resource pooling is the most fundamental characteristic, as discussed above. The provider
abstracts resources and collects them into a pool, portions of which can be allocated to different consumers (typically based on policies).

- Consumers provision the resources from the pool using *on-demand self-service*. They manage their resources themselves, without having to talk to a human administrator.
- *Broad network access* means that all resources are available over a network, without any need for direct physical access; the network is not necessarily part of the service.
- *Rapid elasticity* allows consumers to expand or contract the resources they use from the pool (provisioning and deprovisioning), often completely automatically. This allows them to more closely match resource consumption with demand (for example, adding virtual servers as demand increases, then shutting them down when demand drops).
- *Measured service* meters what is provided, to ensure that consumers only use what they are allotted, and, if necessary, to charge them for it.
- . The only addition is *multitenancy*, which is distinct from resource pooling.

2.Cloud Service Model

NIST defines three *service models* which describe the different foundational categories of cloud services:

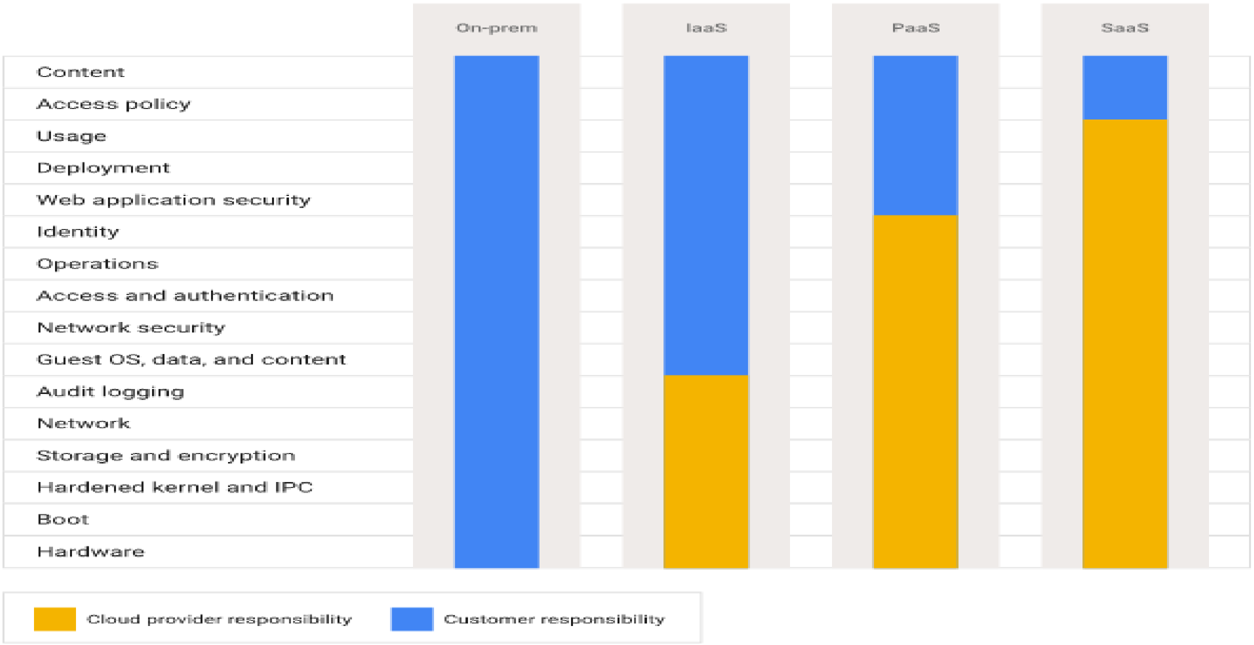
- *Software as a Service (SaaS)* is a full application that's managed and hosted by the provider. Consumers access it with a web browser, mobile app, or a lightweight client app.
- *Platform as a Service (PaaS)* abstracts and provides development or application platforms, such as databases, application platforms (e.g. a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, you don't manage the underlying servers, networks, or other infrastructure.
- *Infrastructure as a Service (IaaS)* offers access to a resource pool of fundamental computing infrastructure, such as compute, network, or storage.

3.Cloud Deployment Model

Both NIST and ISO/IEC use the same four cloud deployment models. These are how the technologies are deployed and consumed, and they apply across the entire range of service models:

- *Public Cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Private Cloud.* The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premises or off-premises.
- *Community Cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or by a third party and may be located on-premises or off-premises.
- *Hybrid Cloud.* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Hybrid is also commonly used to describe a non-cloud data center bridged directly to a cloud provider.

Q5:What is the shared responsibility model in the cloud



Q6 What is I.A.M?

Gartner defines IAM as “the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.”

- AWS
  - AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

Q7:Define Authentication,MFA and access control,authorization ,entitlement and federated identity management.

- Authentication: the process of confirming an identity. When you log in to a system you present a username (the identifier) and password (an attribute we refer to to as an authentication factor).Also known as Authn.
- Multi factor Authentication (MFA): use of multiple factors in authentication. Common

options include

❏ one-time passwords generated by a physical or virtual device/token (OTP),

❏ out-of- band validation through an OTP sent via text message, or confirmation from a mobile device,

❏ biometrics, or plug-in tokens.

❏ Access control: restricting or granting access to a resource. Access management is the process of managing access to the resources.

❏ Authorization: allowing an identity access to something (e.g. data or a function). Also known as Authz.

❏ Entitlement: mapping an identity (including roles, personas, and attributes) to an authorization.

The entitlement is what they are allowed to do, and for documentation purposes we keep these in an entitlement matrix.

❏ Federated Identity Management: the process of asserting an identity across different systems
or organizations. This is the key enabler of Single Sign On and also core to managing IAM

❏ Authoritative source: the “root” source of an identity, such as the directory server that manages
employee identities.

❏ Identity Provider: the source of the identity in federation. The identity provider isn’t always the
authoritative source, but can sometimes rely on the authoritative source, especially if it is a broker for the process.

❏ Relying Party: the system that relies on an identity assertion from an identity provider.

Q7 What are IAM standards in the cloud? What are the federated IAM protocols in the cloud?

IAM Standards	Purpose	Remarks
❏ Security Assertion Markup Language (SAML) 2.0 is an OASIS standard for federated identity	Both Authentication Authorization	
❏ IETF-OAUTH	Authorization	IETF Standard

OpenID Connect(OIDC)	Authentication	Deployed on top of OAuth2.0 To provide authentication Authorization
❑ eXtensible Access Control Markup Language (XACML)	Attribute based access control /Authorization	Work or deploy with both SAML and OAuth
❑ System for Cross-domain Identity Management (SCIM)	Exchanging Identity info b/w domains	\provisioning/De-provisioning accounts across domains

Q8 How Does Federated IDM works?

How Federated Identity Management Works: Federation involves an identity provider making assertions to a relying party after building a trust relationship. At the heart are a series of cryptographic operations to build the trust relationship and exchange credentials.

Q9:What are the multiple options for MFA?

- ❑ There are multiple options for MFA, including:
  - ❑ Hard tokens are physical devices that generate one time passwords for human entry or need to be plugged into a reader. These are the best option when the highest level of security is required.
  - ❑ Soft tokens work similarly to hard tokens but are software applications that run on a phone or computer. Soft tokens are also an excellent option but could be compromised if the user's device is compromised, and this risk needs to be considered in any threat model.
  - ❑ Out-of-band Passwords are text or other messages sent to a user's phone (usually) and are then entered like any other one time password generated by a token. Although also a good option, any threat model must consider message interception, especially with SMS.
  - ❑ Biometrics are growing as an option, thanks to biometric readers now commonly available on mobile phones. For cloud services, the biometric is

a local protection that doesn’t send biometric information to the cloud provider and is instead an attribute that can be sent to the provider. As such the security and ownership of the local device needs to be considered.

Q10:How to manage Privilege users in the cloud?

In terms of controlling risk, few things are more essential than privileged user management.

❏ The requirements mentioned above for strong authentication should be a strong consideration for any privileged user.

❏ In addition, account and session recording should be implemented to drive up accountability and visibility for privileged users.

❏ In some cases, it will be beneficial for a privileged user to sign in through a separate tightly controlled system using higher levels of assurances for credential control, digital certificates,physically and logically separate access points, and/or jump hosts.

Q11 Compare attribute based access control and Role based access control?

Attribute based access control(ABAC)

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. Or tags.

Role based Access Control (RBAC)

The traditional authorization model used in IAM is called role-based access control (RBAC). RBAC defines permissions based on a person's job function.

Q12:What are resource based policies and inline policies? Are resource based polices are in-line policies?

Resources based policies

Resource-based policies are permissions policies that you attach to a resource such as an Amazon S3 bucket or an IAM role trust policy.

Resource-based policies control what actions a specified principal can perform on that resource and under what conditions. Resource-based policies are inline policies, and there are no managed resource-based policies.

- **Inline policies – Policies that you create and manage and that are embedded directly into a single user, group**

Q13 Define stages or phases of secure design application development?

Training	Define	Design	Develop	Test
❑ Secure Coding Practices ❑ Writing security tests ❑ Provider/ Platform Technical Training	❑ Code Standards ❑ Security functional requirements	❑ Threat Modeling ❑ Secure Design	❑ Code review ❑ Unit testing ❑ Static Analysis ❑ Dynamic Analysis	Vulnerability Assessment ❑ Dynamic Analysis ❑ Functional tests ❑ QA

Q14 What is Static Application Security Testing (SAST): ?

- ❑ Static application security testing (SAST) analyzes your source code for anomalous security patterns, and provides indications for defect prone code.
- ❑ SAST relies on static inputs, such as
  - ❑ documentation(requirements specification, design documentation, and design specifications) and
  - ❑ application source code to test for a range of known security issues.
  - ❑ Static code analyzers can help expedite the analysis of large volumes of code.
- ❑ On top of the normal range of tests, these should ideally incorporate checks on API calls to the cloud service.
- ❑ They should also look for any static embedded credentials for those API calls, which is a growing problem.

Q15 What is **Dynamic Application Security Testing (DAST)?**

- **DAST methodologies, which performs tests against the running application to identify potentially unexpected behavior.**
- **Dynamic testing can be used to detect potential issues that are not detectable via static analysis.**
- **Testing at the code repository, build, and pipeline stages allows you to check for different types of potential issues from entering into your code.**
- **DAST tests running applications and includes tests such as web vulnerability testing and fuzzing.**
- **Due to the terms of service with the cloud provider DAST may be limited and/or require pre-testing permission from the provider.**
- **With cloud and automated deployment pipelines it is possible to stand up entirely functional test environments using infrastructure as code and then perform deep assessments before approving changes for production.**

Q16 Impact on Vulnerability Assessment

- **Vulnerability assessment can be integrated into CI/CD pipelines and implemented in cloud fairly easily, but it nearly always requires compliance with the provider's terms of service.**
- **There are two specific patterns we commonly see. The first is running full assessments against images or containers as part of the pipeline in a special testing area of the cloud (a segment of a virtual network) that you define for this purpose. The image is only approved for production deployments if it passes this test.**
- **We see a similar pattern used to test entire infrastructures by building a test environment using infrastructure as code.**
- **In both cases production is tested less, or not at all, since it should be immutable and exactly resemble the test environment (both are based on the same definition files).**
- **Organizations can also use host-based vulnerability assessment tools, which run locally in a virtual machine and thus do not require coordination with or permission of the cloud provider.**

Q17 Impact on Penetration Testing

  - **As with vulnerability assessment there will almost certainly be limits on performing penetration tests without the permission of the cloud provider.**
  - **The CSA recommends adapting penetration testing for cloud using the following guidelines:**
    - **Use a testing firm that has experience on the cloud provider where the application is deployed.**
    - **Include developers and cloud administrators within the scope of the test. Many cloud breaches attack those who maintain the cloud, not the application on the cloud itself. This includes the cloud management plane.**
    - **If the application is a multitenant app, then allow the penetration testers**

authorized access as a tenant to see if they can compromise the tenancy isolation and use their access to break into another tenant's environment or data.

Q19 What is DEVOPs or CI/CD pipeline?

DevOps refers to the deeper integration of development and operations teams through better collaboration and communications, with a heavy focus on automating application deployment and infrastructure operations. There are multiple definitions, but the overall idea consists of a culture, philosophy, processes, and tools.

- ❏ At the core is the combination of Continuous Integration and/or Continuous Delivery (CI/CD) through automated deployment pipelines, and the use of programmatic automation tools to better manage infrastructure.
- ❏ DevOps is not exclusive to cloud, but as discussed it is highly attuned to cloud and is growing to become the dominant cloud application delivery model.

Q20 : What is management plane?

- ❏ The management plane refers to the interfaces for managing your assets in the cloud..
- ❏ In Iaas/Paas If you deploy virtual machines on a virtual network the management plane is how you launch those machines and configure that network.
- ❏ For SaaS, the management plane is often the "admin" tab of the user interface and where you configure things like users, settings for the organization, etc.

Q21 How do we access the management plane?

- ❏ Most web consoles offer a user interface for the same APIs that you can access directly. Although, depending on the platform or provider's development process, you may sometimes encounter a mismatch where either a web feature or an API call appear on one before the other.
- ❏ *APIs* are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over HTTP/S and thus work well across diverse environments.
- ❏ These can use a variety of authentication mechanisms, as there is no single

standard for authentication in REST.

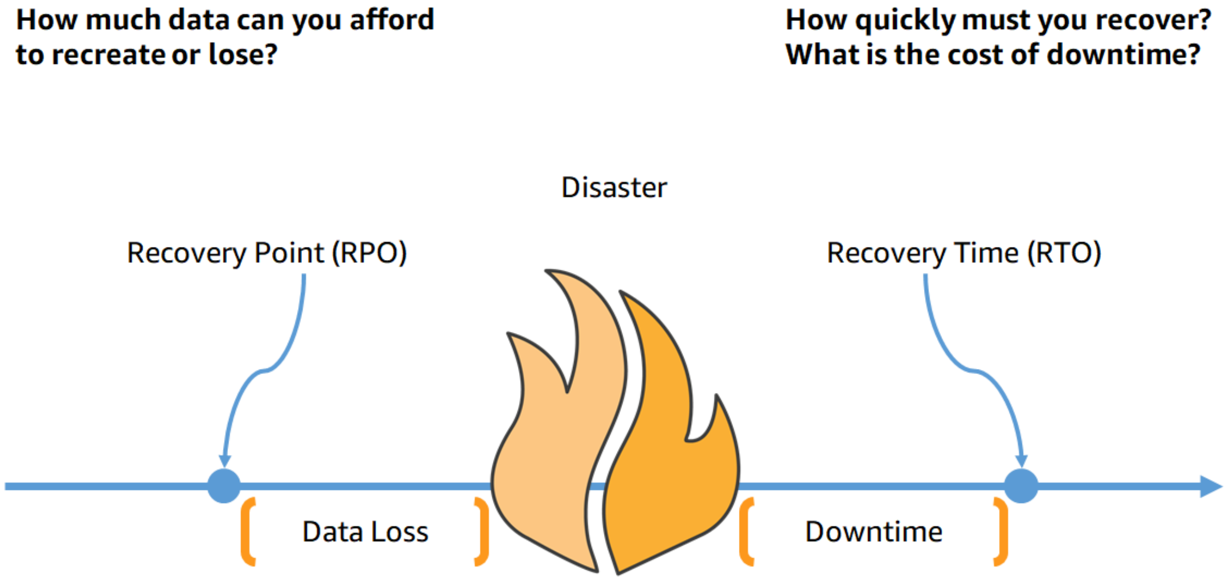
- ❑ HTTP request signing and OAuth are the most common; both of these leverage cryptographic techniques to validate authentication requests.

Q22: What is the difference between Disaster recovery and availability?

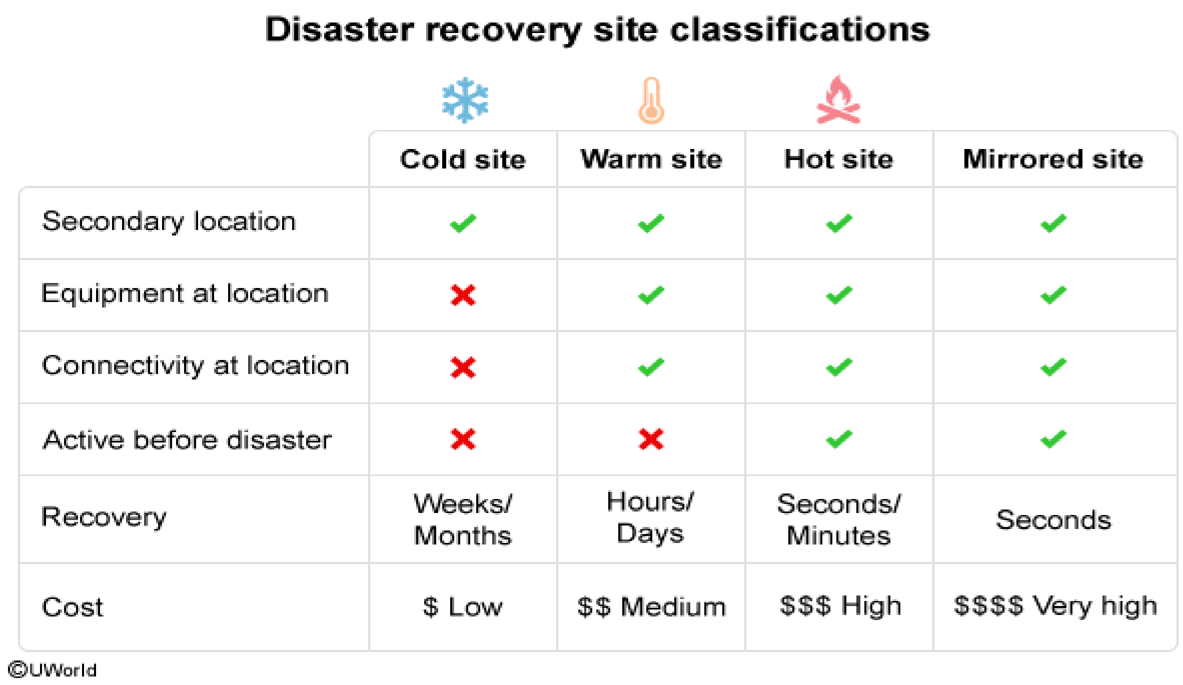
❑ Disaster recovery(DR) ❑ Disaster recovery measures objectives for one-time events, ❑ Disaster recovery focuses on disaster events, ❑ The objective of disaster recovery is business continuity. ❑ DR is the part of resiliency strategy.	❑ Availability ❑ Availability objectives measure mean values over a period of time ❑ Availability focuses on more common disruptions of smaller scale such as component failures, network issues, software bugs, and load spikes. ❑ The Objective of availability is maximizing the time ❑ that a workload is available to perform its intended business functionality. $Availability = \frac{Available\ for\ Use\ Time}{Total\ Time} = \frac{MTBF}{MTBF + MTTR}$ Availability is calculated using Mean Time Between Failures (MTBF) and Mean Time to Recover (MTTR): This approach is often referred to as “nines”, where a 99.9% availability target is referred to as “three nines”.

Q24:What do you mean by RPO or RTO?

Recovery Time Objective (RTO) is the maximum acceptable delay between the interruption of service and restoration of service. This objective determines what is considered an acceptable time window when service is unavailable and is defined by the organization.	Recovery Point Objective (RPO) is the maximum acceptable amount of time since the last data recovery point. This objective determines what is considered an acceptable loss of data between the last recovery point and the interruption of service and is defined by the organization.


How much data can you afford to recreate or lose?
How quickly must you recover? What is the cost of downtime?
Disaster
Recovery Point (RPO)
Recovery Time (RTO)
Data Loss
Downtime

Q25: What are DR options ?



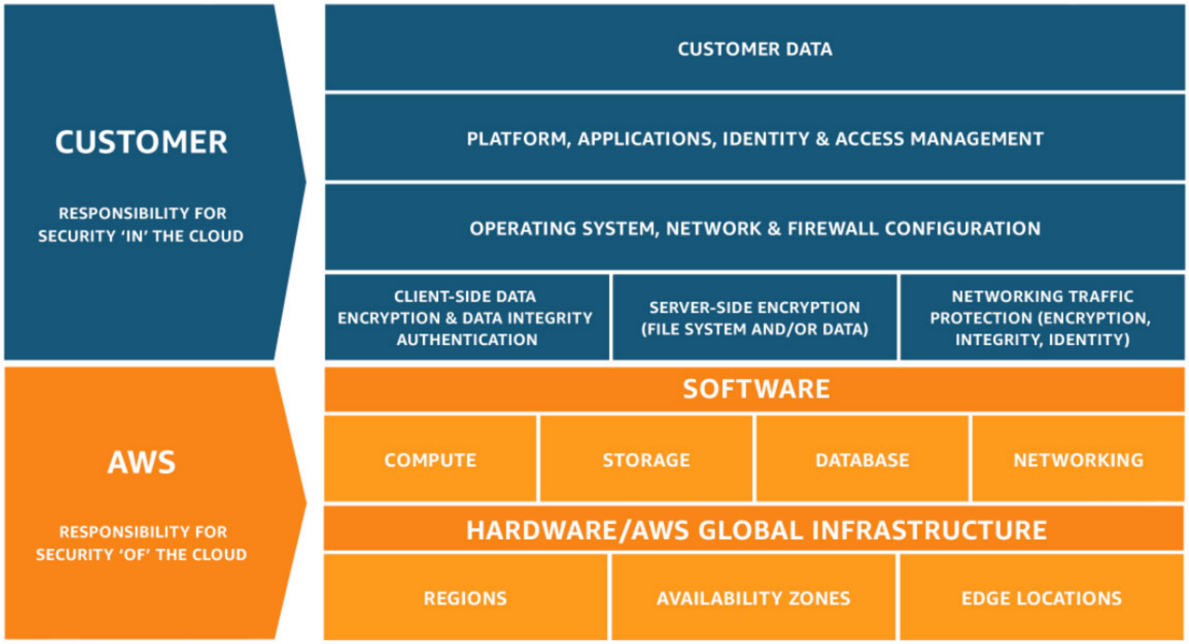
Disaster recovery site classifications

	Cold site	Warm site	Hot site	Mirrored site
Secondary location	✓	✓	✓	✓
Equipment at location	✗	✓	✓	✓
Connectivity at location	✗	✓	✓	✓
Active before disaster	✗	✗	✓	✓
Recovery	Weeks/ Months	Hours/ Days	Seconds/ Minutes	Seconds
Cost	$ Low	$$ Medium	$$$ High	$$$$ Very high

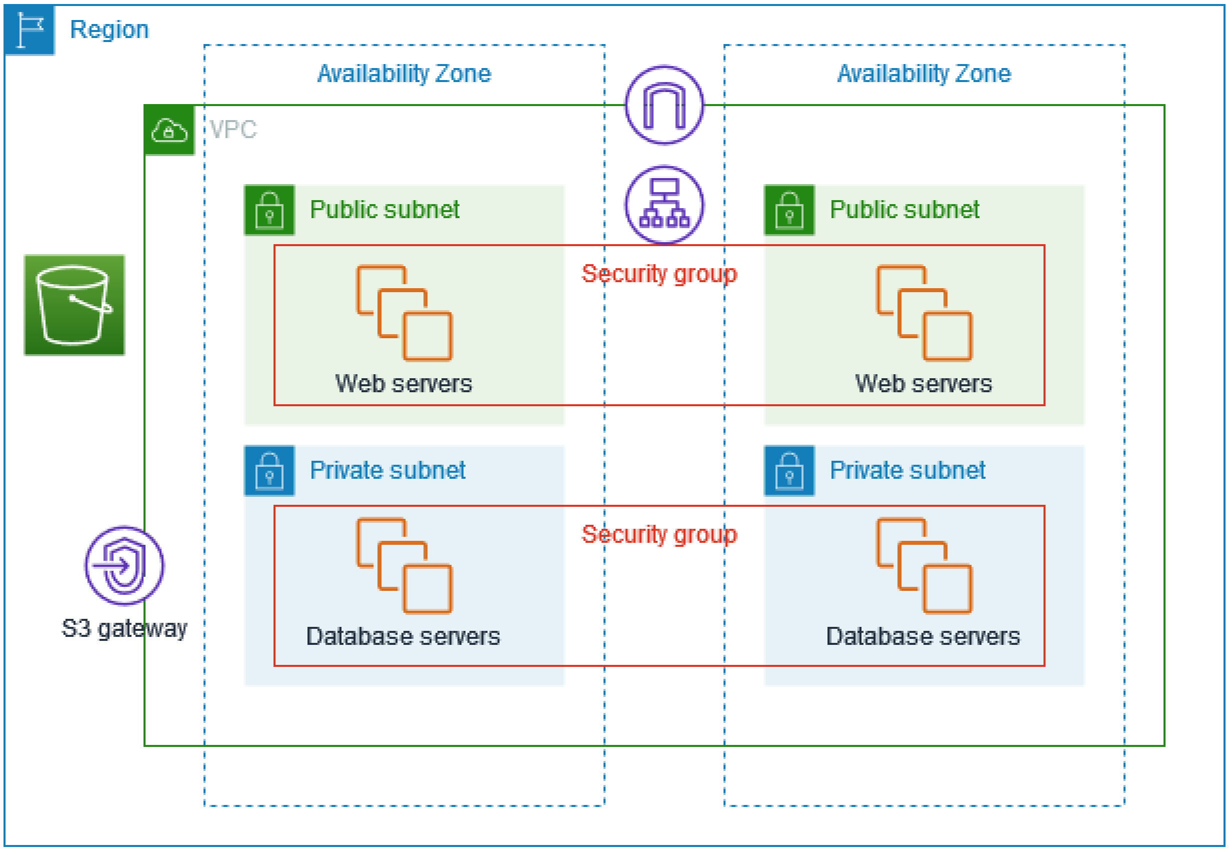
©UWorld

Q26: Cloud users and Cloud Provider shared responsibility model?

E


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Q Explain the following diagram?



The following diagram provides an overview of the resources included in this example. The VPC has public subnets and private subnets in two Availability Zones. The web servers run in the public subnets and receive traffic from clients through a load balancer. The security group for the web servers allows traffic from the load balancer. The database servers run in the private subnets and receive traffic from the web servers. The security group for the database servers allows traffic from the web servers. The database servers can connect to Amazon S3 by using a gateway VPC endpoint.