**Final Exam Questions**

1. Which of the following indicates that a user can own some private servers as well as they can distribute some of the workloads on the public cloud--- **Hybrid Cloud**
2. which of the following is the correct order of the phases of the data life cycle?

Ans: **Create, Store, use, Save, Archive, Destroy**

1. Which of the following is a best practice in designing a multi-tier infrastructure that hosts a set of web servers and database servers in an AWS VPC?

**Ans: Use the Public subnet for the webserver and the Private subnet for the Database server.**

1. A customer planning on hosting an AWS RDS instance, needs to ensure that the underlying data is encrypted. Which of the following should be used?

**Ans: Encrypt the database instance during creation.**

1. Assume a web application requires AWS credentials and Authorization to use AWS services. Which IAM should be used?

**Ans: roles**

1. To host web and MySQL Database applications in an AWS VPC, which of the following needs to be used to ensure that the database only allows traffic from the webserver?

**Ans: Security Groups**

1. What is the first step in getting started with AWS lambda?

**Ans: Upload code**

1. Amazon S3 is which type of storage service?

**Ans: Object**

1. Which of the following must be in place to ensure that a Lambda function can write data to a DynamoDB table?

**Ans: Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges.**

1. Amazon Cloud formation is --------------------------------

**Ans: Deployment and Management Service**

1. An application currently consists of an EC2 instance hosting a web application. The web application connects to an AWS RDS database. Which of the following is used to ensure that the database layer is highly available?

**Ans: Enable Multi-Az for AWS RDS Database**

1. Which of the following term is used to encapsulate application software from the underlying operating system on which it is executed?

**Ans: Application Virtualization**

1. The risk that a cloud provider might go out of business and the cloud customer might not be able to recover the data is known as-----------

**Ans: Vendor-Lockout**

1. If a cloud customer wants a secure, isolated environment to conduct software development and testing, which cloud service would probably be best?

**Ans: Paas**

1. Which of the following best describes the model where software applications are hosted by a cloud service provider and made available to customers over network resources?

**Ans: SaaS**

1. Which of the following represents the correct set of cloud deployment models?

**Ans: Public, Private, hybrid, Community**

1. In which cloud service model is the customer required to maintain and update only the applications?
   1. **PaaS**
2. In the cloud, the data owner is usually **-------------------------**

**Ans: Cloud Customer**

1. All of these are reasons an organization may want to consider cloud migration except **------**

**Ans: Elimination of Risks**

1. Which of the following is not a criterion to discriminate whether a service is delivered in the cloud computing style?

**Ans: Negotiation between the service provider and consumers.**

1. If a cloud customer wants a fully operational environment with very little maintenance or administration necessary, which cloud service model would probably be best?

**Ans: SaaS**

1. What is the term used to describe the loss of access to data because the cloud provider has ceased operation?

**Ans: Vendor Lockout**

1. what is a type of cloud infrastructure that is provisioned for open use by the public and is owned by a cloud provider?

**Ans: Public Provider**

1. In the shared responsibility model, for which aspect of securing the cloud is AWS responsible?

**Ans: Security of the Cloud.**

1. In which of the following model does the user not have control over the deployed application in the cloud?
   1. **Ans: Paas**
2. A service on AWS provides offsite backups for images for millions of customers with thousands of images per customer. The images are retrieved infrequently but must be available for retrieval immediately. Which is the following is the most efficient cost storage option?
   1. **Amazon S3 Standard**
3. Which of the following is not true about amazon glacier?
   1. **Optimized for data for which retrieval times of several hours are suitable.**
4. Which of the following is the most secure way of giving access to AWS services to an application running on an EC2 instance?
   1. **Assume role**
5. Which of the following best describes the types of data for which Amazon S3 Glacier is best suited?
   1. **Infrequently and rarely accessed.**
6. Which of the following AWS service should be used to develop a document-sharing application with a storage layer that provides automatic support for versioning?
   1. **Amazon S3.**
7. All these technologies have made the Cloud viable except
   1. **Smart hubs**
8. In which cloud service model is the customer required to least
9. the OS?
   1. **IaaS**
10. Which of the following term is used to describe the general case and efficiency of moving data from one cloud provider to another cloud provider or down from the cloud?
    1. **Migration**
11. Which of the following style belongs to the call and return architecture style of distributed computing?
    1. **Object-Oriented**
12. Which of the following data storage types are associated or used with PaaS?
    1. **Databases and Big Data (Structured and Unstructured Data).**
13. Which of the following doesn’t support parallel computing?
    1. **SISD (Single Instruction Single Data)**
14. Which of the following is the most common multi cloud implementation used in practice?
    1. **Disaster recovery using multi-Cloud**
15. Which of the following is not good practice for security?
    1. **Embed secrets in Code**
16. In which cloud service model, customer is only responsible for the data?
    1. **Saas**
17. Which of the following is an online backup and storage system?
    1. **Amazon Simple Storage System(S3)**
18. Which of the following does not belong to software architectural styles for distributed computing?

**Ans: Client/server**

1. When using an IaaS solution, which of the following is not an essential benefit for the customer?

**Ans: Removing the need to maintain a license library**

Anything-as-a-service, or "XaaS," refers to the growing diversity of services available over the Internet via cloud computing as opposed to being provided locally, or on premises.

**Anything-as-a-Service**

An open source cloud computing and Infrastructure as a Service (IaaS) platform developed to help Infrastructure as a Service make creating, deploying, and managing cloud services easier by providing a complete "stack" of features and components for cloud environments.

**Apache Cloudstack**

This individual is typically responsible for the implementation, monitoring, and maintenance of the cloud within the organization or on behalf of an organization (acting as a third party).

**Cloud Administrator**

Short for cloud application, cloud app is the phrase used to describe a software application that is never installed on a local computer. Instead, it is accessed via the Internet.

**Cloud App**

Typically responsible for adapting, porting, or deploying an application to a target cloud environment.

**Cloud Application Architect**

A specification designed to ease management of applications — including packaging and deployment — across public and private cloud computing platforms.

**Cloud Application Management for Platforms (CAMP)**

He or she will determine when and how a private cloud meets the policies and needs of an organization's strategic goals and contractual requirements (from a technical perspective).

**Cloud Architect**

A third-party entity that manages and distributes remote, cloud-based data backup services and solutions to customers from a central data center.

**Cloud Backup Service Provider**

Enable enterprises or individuals to store their data and computer files on the Internet using a storage service provider rather than storing the data locally on a physical disk, such as a hard drive or tape backup.

**Cloud Backup Solutions**

A type of computing, comparable to grid computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

**Cloud Computing**

Accounting software that is hosted on remote servers.

**Cloud Computing Accounting Software**

A company that purchases hosting services from a cloud server hosting or cloud computing provider and then re-sells them to its own customers.

**Cloud Computing Reseller**

A database accessible to clients from the cloud and delivered to users on demand via the Internet.

**Cloud Database**

Ensures the various storage types and mechanisms utilized within the cloud environment meet and conform to the relevant SLAs and that the storage components are functioning according to their specified requirements.

**Cloud Data Architect**

Focuses on development for the cloud infrastructure itself. This role can vary from client tools or solutions engagements, through to systems components.

**Cloud Developer**

The process of making available one or more of the following services and infrastructures to create a public cloud-computing environment: cloud provider, client, and application.

**Cloud Enablement**

Software and technologies designed for operating and monitoring the applications, data, and services residing in the cloud. Cloud management tools help to ensure a company's cloud computing-based resources are working optimally and properly interacting with users and other services.

**Cloud Management**

The process of transitioning all or part of a company's data, applications, and services from on-site premises behind the firewall to the cloud, where the information can be provided over the Internet on an on-demand basis.

**Cloud Migration**

A phrase frequently used in place of Platform as a Service (PaaS) to denote an association to cloud computing.

**Cloud OS**

The ability to move applications and its associated data between one cloud provider and another — or between public and private cloud environments.

**Cloud Portability**

A service provider who offers customers storage or software solutions available via a public network, usually the Internet.

**Cloud Provider**

The deployment of a company's cloud computing strategy, which typically first involves selecting which applications and services will reside in the public cloud and which will remain on-site behind the firewall or in the private cloud.

**Cloud Provisioning**

A type of hosting in which hosting services are made available to customers on demand via the Internet. Rather than being provided by a single server or virtual server, cloud server hosting services are provided by multiple connected servers that comprise a cloud.

**Cloud Server Hosting**

Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple cloud service providers.

**Cloud Services Broker**

The storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

**Cloud Storage**

Load and performance testing conducted on the applications and services provided via cloud computing — particularly the capability to access these services — in order to ensure optimal performance and scalability under a wide variety of conditions.

**Cloud Testing**

A form of virtual desktop infrastructure (VDI) in which the VDI is outsourced and handled by a third party.

**Desktop-as-a-service**

The term used to describe applications — or software — that a business would use to assist the organization in solving enterprise problems.

**Enterprise Application**

An open source cloud computing and Infrastructure as a Service (IaaS) platform for enabling private clouds.

**Eucalyptus**

Primary goal is to accredit and distinguish secure and well-architected cryptographic modules produced by private sector vendors who seek to have their solutions and services certified for use in regulated industries that collect, store, transfer, or share data that is deemed to be "sensitive" but not classified.

**FIPS 140-2**

A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

**Hybrid cloud storage**

A form of cloud storage that applies to storing an individual's mobile device data in the cloud and providing the individual with access to the data from anywhere.

**Mobile Cloud Storage**

Its primary goal and objective is to ensure that appropriate security requirements and security controls are applied to all U.S. Federal Government information and information management systems.

**NIST SP 800-53**

Leverages the Internet and cloud computing to create an attractive off-site storage solution with little hardware requirements for any business of any size.

**Online Backup**

A form of cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere.

**Personal cloud storage**

A way for customers to rent hardware, operating systems, storage, and network capacity over the Internet from a cloud service provider.

**Platform as a service**

Enable their IT infrastructure to become more capable of quickly adapting to continually evolving business needs and requirements.

**Private cloud Project**

A form of cloud storage where the enterprise data and cloud storage resources both reside within the enterprise's data center and behind the firewall.

Private cloud storage

A form of cloud storage where the enterprise and storage service provider are separate and the data is stored outside of the enterprise's data center.

Public Cloud Storage

A distributed model where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources.

Software as a service

The collection of multiple distributed and connected resources responsible for storing and managing data online in the cloud.

Storage Cloud

A methodology and a set of tools that enables security professionals to leverage a common set of solutions that fulfill their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities and to plan a roadmap to meet the security needs of their business.

TCI Reference Architecture

The optimization of cloud computing and cloud services for a particular vertical (e.g., a specific industry) or specific-use application.

Vertical cloud computing

Enable cloud computing to become a real and scalable service offering due to the savings, sharing, and allocations of resources across multiple tenants and environments.

Virtualization Technologies

An overt secret writing technique that uses a bidirectional algorithm in which humanly readable information (referred to as plaintext) is converted into humanly unintelligible information (referred to as ciphertext).

Encryption

A special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message.

Encryption Key

A model that provides a complete infrastructure (e.g. servers, internetworking devices) and allows companies to install software on provisioned servers and control the configurations of all devices.

Infrastructure as a service

The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy.

Key management

The granting of right of access to a user, program, or process.

Authorization

A service where data is replicated across the global Internet.

**Content Delivery Network**

In essence, a managed database service.

Database as a service

Isolates network elements such as e-mail servers that, because they can be accessed from trustless networks, are exposed to external attacks.

Demilitarized Zone (DMZ)

The set of processes and structure to systematically manage all risks to the enterprise.

Enterprise Risk Management

Objects (files) are stored with additional metadata (content type, redundancy required, creation date, etc.). These objects are accessible through APIs and potentially through a web user interface.

Object Storage

Instead of using one large disk to store data, one can use many smaller disks (because they are cheaper).  
An approach to using many low-cost drives as a group to improve performance, yet also provides a degree of redundancy that makes the chance of data loss remote.

Redundant Array of Inexpensive Disks (RAID

A set of routines, standards, protocols, and tools for building software applications to access a Web-based software application or Web tool

Application Programming Interfaces

Software technology that encapsulates application software from the underlying operating system on which it is executed

Application Virtualization

A method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training

**Data Masking**

The security discipline that enables the right individuals to access the right resources at the right times for the right reasons

Identity and Access Management

A method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories: knowledge factors, such as passwords. Combines two or more independent credentials: what the user knows, what the user has and what the user is.

Multi-factor Authentication

A version of the SAML standard for exchanging authentication and authorization data between security domains

Security Assertion Markup Language

An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

Web Application Firewall

This cloud infrastructure is provisioned for exclusive use by a specific community of organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

Community Cloud

Consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

Honeypot

This cloud infrastructure is a composition of two or more distinct cloud infrastructures (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 Cloud

Data center networks that are logically divided into smaller, isolated networks. They share the physical networking gear but operate on their own network without visibility into the other logical networks.

Multi-tenancy

This cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on- or off-premises.

Private Cloud

A protocol that allows for separate channels for carrying presentation data, serial device communication, licensing information, and highly encrypted data (keyboard, mouse activity).

Remote Desktop Protocol