CC Practical Submission

Name: TEISHA SOANS
Roll No: A068
Msc SDS

Following is the github repository having the write ups and practicals
Link: https://github.com/tia2310/Cloud-Computing.git

Teisha Soans
A068

Topic..Cloud Computing Practical I..Date..20/07/24..

Write up :-

1) Cloud Computing Architecture

Cloud computing has revolutionized the way businesses and individuals access & utilize technology resources. The architecture of cloud computing can be broadly divided into three main components: the front-end, the back-end and the network. The front-end comprises the client devices and interfaces used to interact with cloud services. This include web browsers, mobile applications etc. The back-end, on the other hand encompasses the cloud infrastructure itself, including servers, storage systems, databases & the managem systems that ensure the smooth operation of these resources. The network acts as the bridge connecting the front-end and back-end, facilitating data transfer & communication.

Cloud computing is also categorized into various types based on deployment models. These include public, private, hybrid and community clouds. Public clouds are operated by third-party providers & offer multiple services to clients over the internet. Private clouds are dedicated to a single organization, providing enhanced security & control. Hybrid clouds combine both public & private cloud elements, enabling data & application probability

2) IAAS

Infrastructure as a service (IAAS) is one of the primary service models in cloud computing. It provides virtualized computing resources over the internet, allowing businesses to rent infrastructure components such as servers, storage and networking on a pay-as-you-go basis. Iaas eliminates the need for organizations to invest in and maintain physical hardware, making it a scalable and cost-effective solution.

Teacher's Sign.....

isha Soans
A068

Topic.....Date.....

Iaas solutions typically include virtual machines, which are software based emulations of physical computers, offering flexibility and scalability. Storage options such as block storage and object storage, provide reliable and efficient data storage solutions. Networking components including virtual private networks (VPNs) and load balancers, ensure secure and efficient data transmission. The key benifits of Iaas include scalability, as resources can be scaled up or down based on demand; cost savings, as it eliminates the need for capital expenditures on hardware; and flexibility, allowing businesses to rapidly deploy and manage applications.

3) AWS (Amazon Web Services)

Aws is a leading provider of cloud computing services, offering a comprehensive suite of cloud-based solutions. Launched by amazon in 2006, Aws has become a dominant force in the cloud industry, providing a wide range of services that cater to diverse business needs. Aws's extensive service offerings and global infrastructure make it a preferred choice for different organizations.

Some of the service's Aws provides include compute, storage, databases, networking and more.

One of its flagship services is Elastic Compute Cloud (EC2), which offers resizable compute capacity in the cloud. EC2 enables businesses to quickly scale their computing resources up or down based on demand, making it ideal for applications with varying workloads.

Other notable Aws services include Simple Storage Service (S3) for scalable object storage, Elastic Block Store (EBS) for block storage and Relational Database Service (RDS) for managed relational database.

Teacher's Sign.....

Teisha Soans
A068

Topic.....Date.....

The advantage of Aws include its global reach, with data centers located around the world, ensuring low-latency access to services. AWS's extensive service offerings provide solutions for a wide range of use cases, from web hosting to big data processing. Additionally Aws places a strong emphases on security and compliance, offering tools and services to help businesses meet regulatory requirements.

4) EC2 (Elastic cloud compute cloud)

Amazon EC2 is a core component of AWS providing scalable compute capacity in the cloud. It allows businesses to launch virtual servers, known as instances and manage them as needed. EC2's flexibility and variety of instance types make it suitable for a wide range of applications, from simple web hosting to complex machine learning workloads.

EC2 offers various instance types, each optimized for different use cases. General Purpose instances provide a balance of compute, memory and networking resources, making them suitable for a variety of applications. Compute Optimized instances are designed for compute-intensive tasks, such as high-performance computing and data analysis. Memory Optimized instances are ideal for applications requiring large amounts of memory, such as in-memory databases. Storage Optimized instances offer high performance storage capabilities for applications with intensive data access requirements. Accelerated computing instances, equipped with GPUs or FPGAs are designed for applications requiring hardware acceleration, such as machine learning & scientific simulations.

EC2 pricing models include On-Demand instances, which provide flexible, pay-as-you-go pricing; Reserved Instances & Spot Instances.

Teacher's Sign.....

Teisha Soans
A068

Topic: Cloud Computing Practical II Date: 27/07/24

1) Storage as a Service - S3

Storage as a service (SaaS) is a cloud computing model that provides users with scalable and flexible storage solutions over the internet. One of the most prominent examples of SaaS is offered by AWS is Amazon Simple Storage Service (S3). S3 is designed to provide high durability, availibility and scalability, allowing businesses and developers to store and retrive any amount of data at any time from anywhere on the web.

S3 uses a simple web services interface to store and retrive data, making it easy to integrate with various applications and serices. Data is organized in buckets, which are containers for storing objects. Each object can be upto 5 terabytes in size and is identified by a unique key within the bucket.

S3 provides features like versioning, access controls, and lifecycle policies to manage the data efficiently. It is also supporting a wide range of use cases including backup and restore, data archiving, content distribution, big data analytics, machine learning and compliance. Its integration with other AWS services and robust architecture makes it an essential tool for modern data storage and management needs.

2) S3 usecases

Amazon S3 is highly versatile and can be used for a wide range of applications across different industries. Some common usecases include:

(a) Back up and Restore: S3 is widely used for backing up data from on-premises systems and other cloud services. Its durability and availability make it an ideal solution for disaster recovery & long-term data retention.

Teacher's Sign.....

Teisha Soans
A068

Topic.....Date.....

(b) Data Atrchiving: Organizations can use S3 for archiving large amounts of data that need to be retained for compliance or regulatory purposes. With S3 Glacier and S3 Glacier Deep Archive, businesses can store data at a lower cost while ensuring it remains accessible when needed.

(c) Content Distribution: S3 is often used to store and distribute static content such as images, videos and documents. Combined with Amazon Cloudfront, a content delivery network (CDN), S3 can deliver content to users with low latency and high transfer speeds.

(d) Big Data Analytics: S3 serves as a data lake for storing large datasets that can be analyzed using AWS analytics services like Amazon Redshift, Amazon Athena and Amazon EMR. This enables businesses to gain insights from their data without worrying about storage.

(e) Application Hosting: Developers use S3 as a medium to host static websites, including HTML, CSS, JavaScript and media files. S3 provides a reliable and scalable infrastructure for delivering web content to users globally.

(f) Software Delivery: Companies distribute software packages, updates, and patches using S_3. Its scalable storage and high availability ensure that software can be delivered to users efficiently.

3) Steps for S_3

Setting up and using Amazon S3 involves several key steps:

(1) Create an AWS Account: If you don't already have an AWS account, sign up at the AWS website. This will give you access to the AWS Management Console.

Teacher's Sign.....

Soans

Topic..... Date.....

where you can manage your S3 resources.

(2) Create a Bucket: In the AWS management console, navigate to the S3 service. Click on "create bucket", provide a unique name for your bucket, select the desired region and configure the settings as needed.

(3) Upload Objects: Once your bucket is created, you can start uploading objects. Click on your bucket name, then click the "upload" button. Select the files you want to upload and configure the permissions and properties if necessary.

(4) Manage Permissions: Set permissions for your bucket and objects to control who can access them. You can use bucket policies, access control lists (ACLs) and AWS Identity and Access Management (IAM) policies to define access rules.

(5) Enable Versioning: To keep multiple versions of an object, enable versioning for your bucket. This allows you to recover previous versions of objects and protect against accidental deletions or overwrites.

(6) Configure Lifecycle Policies: Set up lifecycle policies to automate the management of your objects. You can define rules to transition objects to different storage classes or delete them after a certain period.

(7) Access Data: You can access your data using the S3 web interface, AWS SDKs, or AWS CLI. S3 provides a RESTful API for integrating with various applications and services.

(8) Monitor & Optimize: Use AWS cloudwatch & AWS CloudTrail to monitor the usage and performance of your S3 resources. Analyze the data to optimize storage costs & improve efficiency.

Teacher's Sign.....

Teisha Soans
A068
8601230001

Topic: Cloud Computing Practical III Date: 10/08/24

In Amazon web services (AWS), "Users" and "Groups" are fundamental concepts within AWS identity and access management (IAM). They help manage permissions and access to AWS resources efficiently.

1) USERS IN AWS IAM :-

IAM users are individual entities that represent people or services interacting with your AWS environment. Each user in AWS can have their own set of security credentials run as a password for the AWS management console or access keys for programatic access.

When you create a user in IAM, you assign them a name and can configure various properties, including permissions, policies and credentials.

Users can have various credential types:

a) Console Password

It is used to sign in to the AWS management console.

(b) Access Keys

They consists of an access key ID and secret access key, used for programmatic access to AWS via the AWS CLI, SDKs or API's.

(c) MFA (Multi-factor Authentication)

You can require users to provide additional security verification by enabling MFA.

By default, new users have no permissions. Permissions can be granted by attaching policies directly to the user or by assigning the user to one or more groups.

GRAPHS IN AWS IAM :-

IAM groups are collection of users. They make it easier to manage permissions for multiple users simultaneously. Instead of assigning permissions to each

Teacher's Sign.....

a Soan
:8
300017

Topic.....Date.....

Individual / user, you can assign permissions to a group, and all users within that group will inherit those permissions. You can create a group and then assign users to it. Groups are commonly used to represent teams, roles, or functions within an organization. This is often refered to as group creation.
Groups can have policies attached that define the actions that are allowed or denied. All users in a group inherit those permissions. It's a best practice to use groups to manage permissions rather than assigning permissions directly to individual users. This approach simplifies management, especially as the number of users grow.

IAM (Identity and Access management):

Aws Identity and Access management (IAM) is a web service that helps securely control access to Aws resources. IAM is one of the most critical services in Aws because it governs who can access resources & what actions they can perform.
Properly configuring IAM is essential for maintaining security & compliance in your Aws environment.

Key Concepts Of IAM

IAM users: IAM users are entities that you create in Aws to represent a person or application that interacts with Aws.

IAM groups: IAM groups are collection of users. You can use groups to manage permissions for multiple users at once.

IAM Roles: IAM roles are similar to users in that they are identities with permissions policies that

Teacher's Sign.....

Topic.....Date.....

determine what the identity can and cannot do in AWS. However, roles are intended to be assumed by anyone who needs them, not a specific user.

(4) Policies : IAM Policies are JSON documents that define permissions. They specify what actions are allowed or denied on which AWS resources. Policies can be attached to users, groups or roles and they come in different forms.

(a) Managed policies : AWS-managed policies are created & managed by AWS. Customer managed policies are created & managed by you.

(b) Inline policies : These are directly embedded to a single user, group or role, giving them specific permissions that aren't shared.

5) Identity providers : IAM allows you to manage access for federated users, such as those from an external identity providers. (eg. corporate directories or SSO systems). Users can assume roles in your AWS account & gain temporary access to resources based on the policies associated with those roles.

Security Features of IAM

AWS managed policies : Simplify permissions management by using policies maintained by AWS ensuring you stay up-to-date with best practices.

Access Analyzer : IAM access analyzer helps you identify resources in your organization & accounts that are shared with external entities.

Password Policies : Set password requirements such as minimum length & complexity and enforce password expiration & reuse cond^n.

Teacher's Sign.....

Teisha Soans
A065
8606230017

Topic: Cloud Computing Practical V Date: 14/09/24

Write up :-

1) Platform as a service

Platform as a Service (PaaS) on AWS provides developers with managed tools for building, deploying and managing applications without handling infrastructure. Key AWS PaaS offerings include:

- AWS Elastic Beanstalk: Simplifies app development and deployment and scaling across multiple languages by managing infrastructure automatically
- AWS Lambda: Allows code to run in response to events, scaling automatically with a pay-as-you-go model.
- API Gateway: Manages and secures APIs, often paired with lambda for backend services.
- AWS Amplify: Helps front-end developers build and deploy mobile / web apps with easy AWS integration.

Benefits include reduced infrastructure management, cost-effectiveness, scalability and faster deployment, making AWS PaaS ideal for web hosting, data processing, mobile backends, and database management. AWS PaaS enables businesses to focus on app development while AWS manages the backend.

2) Elastic Beanstalk.

AWS Elastic Beanstalk is a PaaS that simplifies deploying and managing applications on AWS. It automates infrastructure tasks such as provisioning, load balancing, scaling, and monitoring, so developers can focus o

Teacher's Sign.....

sha soaws
8
230007

Topic..... Date.....

writing code. Elastic Beanstalk supports multiple programming languages (e.g. Java, Python, .NET, Node.js) and allows easy deployment from the AWS console, CLI or IDEs.

Its key benefits include:

- Automatic scaling: Scales applications to meet demands without manual intervention.
- Integrated Monitoring: Tracks app health and performance via AWS CloudWatch.
- Customizable: Allows control over infrastructure while automating key tasks.
- Cost-effective: No additional cost beyond AWS resource usage.

Elastic Beanstalk automates the underlying AWS resources such as EC2 instances, load balancers, Auto Scaling and RDS databases, based on the application requirements. When you deploy an application, Elastic Beanstalk creates and configures these resources, then continuously monitors the environment to ensure that the application is healthy. It is ideal for web apps, APIs and development environments, Elastic Beanstalk helps businesses quickly deploy, manage and scale applications effortlessly.

3) Components of Beanstalk

AWS Elastic Beanstalk has several core components that work together to simplify application deployment and management on AWS. They are:

① Application: The application is the highest-

Teacher's Sign.....

Topic..... Date.....

level component in Elastic Beanstalk. It acts as a container for related environments, versions and config. Within the application, you can create multiple environments (like dev, staging) for testing and deploying updates.

(2) Application version

An application version is a specific, labeled iteration of your application code that you deploy to an environment.

(3) Environment

An environment is where an application version is deployed. Environments can be (a) Web server environments for applications that handle HTTP requests (b) Worker environments for applications that process background tasks.

(4) Environment tier:

The environment tier defines the type of enviroment.
(a) Web Server Tier: Handles HTTP requests and typically includes load balancing & scaling. (b) Worker Tier: Processes background jobs & tasks, usually through SQS.

(5) Environment Configuration

This includes settings for AWS resources (instance types, Autoscaling, security groups) and software configurations (runtime, platform settings, etc.) You can update configurations to optimize performance or add additional services.

(6) Configuration files.

Configuration files (YAML) can be included in application source code to manage the environment settings.

(7) Platform

The platform is the runtime environment Elastic

Teacher's Sign.....

Teisha Loaiza
1068
8608232009

Topic..... Date.....

Beanstalk uses to run your application.

(8) Elastic Load Balancer (ELB)
ELB is used to distribute incoming traffic across multiple EC2 instances in a webserver environment, providing fault tolerance & improved performance.

(9) Auto Scaling
Elastic Beanstalk configures Auto Scaling to automatically adjust the number of instances based on demand. This ensures optimal resource usage & cost-efficiency by scaling up during high demand & down when demand decreases.

(10) Monitoring & Logging
Elastic Beanstalk integrates with AWS Cloud watch to monitor environment health, performance metrics, and resource usage.

4) IAM
AWS Identity & Access Management (IAM) is a service that helps securely manage access to AWS resources. It enables you to control who (users & roles) can access resources, what actions they can perform, and under what conditions. With IAM, you can create and manage permissions for both internal and external users, as well as for applications. Key features include:

- Users & Groups: You can create individual user accounts with specific permissions & organize them into groups to apply bulk permissions.
- Roles: Roles are used to grant temporary access to AWS resources for applications, services or users from other accounts.
- Policies:

Topic..... Date.....

users, groups and roles. They JSON-based documents specify allowed or denied actions on AWS resources.

- Multi-factor Authentication (MFA): Adds an extra layer of security by requiring users to present two forms of authentication.
- Fine-Grained Access Control: IAM enables detailed permissions management, so you can grant access to specific actions or resources based on user needs.

Benefits include enhanced security since centralized access management helps prevent unauthorized access, granular control i.e. fine-grained permissions let you control access precisely and cost efficiency since IAM is free of charge with users only paying for the resources accessed.

IAM is essential for managing access to AWS services, setting up secure environments, and ensuring compliance with security best practices.

Teisha Soans
A068
60623000

Topic...Cloud Computing Practical VII.....Date...5/10/24.....

Write up:-

1) Bare-metal hypervisors Type 1

A bare-metal hypervisor, also known as a Type 1 hypervisor, is a virtualization software that runs directly on the hardware of a physical server without needing a host operating system. By running directly on the hardware, it provides high performance and resource efficiency.

Key features include:

(a) Direct Hardware Access: Because it operates directly on hardware, a bare-metal hypervisor can efficiently manage resources like CPU, memory and storage, offering near-native performance.

(b) Efficient Resource Management: Type 1 hypervisors allocate resources to virtual machines (VMs) precisely, ensuring optimized performance and isolation.

(c) High Security & Stability: Running independently of a host OS reduces attack vectors & improves stability, making it suitable for production environments.

Benefits include: (a) Performance: Higher performance due to direct hardware interaction.

(b) Isolation: Stronger isolation between VMs for security & fault tolerance.

(c) Scalability: Ideal for data centers & environments requiring high resource utilization.

Some Bare-metal hypervisors are VMware ESXi, Microsoft Hyper-V and Xen.

2) Bare-Metal Hypervisors Type 0.

A Type 0 hypervisor is a ~~typ~~ term sometimes used to describe a specialized bare-metal hypervisor integrated directly into the hardware, often found in high-performance environments like mainframes and specialized system. Key characteristics include:

(a) Hardware Integration: Type 0 hypervisors are

Teacher's Sign.....

Topic..... Date.....

integrated within the system hardware, offering even deeper access to CPU, memory, and I/O resources than standard bare-metal hypervisors.

(b) High Performance & Low Latency: The close integration with hardware enables faster access to resources, which is ideal for workloads requiring minimal latency & high throughput.

(c) Enhanced Security & Stability: Since the hypervisor runs at the lowest possible level, it reduces potential vulnerabilities & enhances system stability.

Type 0 hypervisors are commonly used in IBM mainframes & similar enterprise systems where extreme performance, resource isolation & security are critical such as in banking or large-scale computing environments.

Bare-Metal Hypervisors : Same as Type I Bare Metal Hypervisors.

VMware

VMware is a company specializing in cloud computing & virtualization technology, and it is best known for its Type I hypervisor, VMware ESXi. VMware's suite of products includes both enterprise-level & desktop-level virtualization solutions. VMware ESXi is widely used in enterprise environments due to its reliability, performance & rich feature set, including advanced management and automation tools.

VMware also offers VMware Workstation & VMware Fusion, which are desktop virtualization products (Type 2 hypervisors) that run on top of existing operating systems, such as Windows & macOS. These solutions are geared more toward

Teacher's Sign.....

Topic..... Date.....

individual users or developers rather than large-scale, production-grade virtualization.

5) Virtual Box

Virtual Box is an open-source Type 2 hypervisor developed by Oracle. It allows users to run multiple operating systems on a single machine by installing the hypervisor as an application on a host operating system. Virtual Box is popular among developers, testers and students due to its flexibility, cross-platform support & cost-effectiveness.

As a Type 2 hypervisor, Virtual Box runs on top of an existing operating system, which makes it easy to install and use but may have slighter lower performance and security compared to Type 1 hypervisors. However, it provides an assessible entry point for running virtual machines on personal computers for testing, learning and development.