INTRODUCTION TO CLOUD COMPUTING

Table of Contents

[MODULE 1 Overview of Cloud Computing 2](#_Toc180777796)

[Lesson 1 Summary: Introduction to Cloud Computing 2](#_Toc180777797)

[Lesson 2 Summary: Business Case for Cloud Computing 2](#_Toc180777798)

[Lesson 3 Summary: Emerging Technologies Accelerated by Cloud 2](#_Toc180777799)

[Module 1 Glossary: Overview of Cloud Computing 3](#_Toc180777800)

[MODULE 2 CLOUD COMPUTING MODELS 3](#_Toc180777801)

[Lesson 1 Summary: Service Models 3](#_Toc180777802)

[Lesson 2 Summary: Deployment Models 4](#_Toc180777803)

[Module 2 Glossary: Cloud Computing Models 4](#_Toc180777804)

[MODULE 3 COMPONENTS OF CLOUD COMPUTING 5](#_Toc180777805)

[Lesson 1 Summary: Cloud Infrastructure 5](#_Toc180777806)

[Lesson 2 Summary: Cloud Storage and Content Delivery Networks 6](#_Toc180777807)

[Module 3 Glossary: Components of Cloud Computing 6](#_Toc180777808)

[MODULE 4 EMERGING TRENDS AND PRACTICES 7](#_Toc180777809)

[Lesson 1 Summary 7](#_Toc180777810)

[DevOps on the Cloud 8](#_Toc180777811)

[Lesson 2 Summary 10](#_Toc180777812)

[Module 4 Glossary: Emergent Trends and Practices 10](#_Toc180777813)

[MODULE 5 CLOUD SECURITY, MONITORING, CASE STUDIES, JOBS 11](#_Toc180777814)

[Policies and Principles of Access Management 11](#_Toc180777815)

[Cloud Monitoring and Benefits 13](#_Toc180777816)

[Lesson Summary: Cloud Security and Monitoring 16](#_Toc180777817)

[Lesson Summary: Case Studies and Jobs 17](#_Toc180777818)

[Module 5 Glossary: Cloud Security, Monitoring, Case Studies, & Jobs 17](#_Toc180777819)

## **MODULE 1 Overview of Cloud Computing**

## Lesson 1 Summary: Introduction to Cloud Computing

* Cloud computing is the delivery of on-demand computing resources over the internet on a pay-as-you-go basis; resources are dynamically assigned and reassigned among multiple users and scale up and down in response to users’ needs.
* The origins of cloud computing can be traced back to the mainframes of the 1950s, with virtualization technologies and hypervisors serving as catalysts for the emergence of modern-day cloud computing.
* Organizations must consider their business needs, investment viability, and risk capacity to create a cloud adoption strategy that delivers desired benefits without causing business disruptions and security, compliance, or performance issues.
* Cloud adoption is growing faster than predicted. Driving this technological wave are cloud service providers with a host of services ranging from Infrastructure, Platform, and Software services. Some major Cloud providers of our time include AWS, Alibaba Cloud, Google, IBM, and Microsoft Azure.

## Lesson 2 Summary: Business Case for Cloud Computing

* The adoption of cloud technologies enables enterprises, big and small, to be agile, innovative, and competitive and to create differentiated customer experiences. Organizations are asking not whether they should move to the cloud but rather what strategy they should adopt to move to the cloud.
* Some case studies that demonstrate the impact businesses have created by adopting the cloud:
  + American Airlines adopting cloud technologies to deliver customer value rapidly across its enterprise
  + UBank leveraging cloud platform services to give more control to their developers, thereby removing barriers to innovation
  + Bitly leveraging the scalability offered by cloud infrastructure for low-latency delivery to its geographically dispersed enterprise customers
  + ActivTrades leveraging the infrastructure, storage, network, and security offerings on the cloud to accelerate execution and delivery of new functions in their online trading systems to their customers

## Lesson 3 Summary: Emerging Technologies Accelerated by Cloud

Emerging technologies powered by the cloud are disrupting existing business models and creating unprecedented opportunities for businesses to grow, innovate, and create value for their customers.

Some case studies that demonstrate how the use of emerging technologies on the cloud is creating value for millions around the world:

* The use of the Internet of Things on the cloud to combat poaching of endangered rhinos in South Africa
* Artificial Intelligence on the cloud is being leveraged to deliver unique digital experiences to millions of fans around the world by the United States Tennis Association
* Blockchain on the cloud helps farmers reduce waste by building traceability and transparency in the food supply chain
* The use of data analytics for driving predictive maintenance solutions for a city’s infrastructure by KONE

## Module 1 Glossary: Overview of Cloud Computing

|  |  |
| --- | --- |
| Term | Definition |
| AI | Artificial intelligence |
| Blockchain | An immutable network allowing members to view only those transactions that are relevant to them |
| Broad Network Access | Cloud computing resources can be accessed through the network |
| Cloud computing | A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction |
| GCP | Google Cloud Platform |
| Hypervisor | A small software layer that enables multiple operating systems to run alongside each other, sharing the same physical computing resources |
| IDC | International Data Corporation |
| IoT | Internet of things |
| Measured Service | You only pay for what you use or reserve as you go |
| NIST | National Institute for Standards and Technology |
| PaaS | Platform as a service |
| Pay-As-You-Go | Users can order cloud resources from a larger pool of available resources and pay for them on a per-use basis |
| POP | Post office protocol |
| Rapid elasticity | You can increase or decrease resources as per your demand because of the elastic property of the cloud |
| SaaS | Software as a service |
| Utility model of billing | You are charged after the usage and at the end of the pre-defined period |
| VM | Virtual machine |

## **MODULE 2 CLOUD COMPUTING MODELS**

## Lesson 1 Summary: Service Models

* With IaaS, the cloud provider manages physical resources.
* With PaaS, the provider manages the platform infrastructure.
* In the SaaS model, the provider hosts and manages the applications and data.
* Infrastructure-as-a-Service is a form of cloud computing that delivers fundamental computer, network, and storage resources to consumers on-demand, over the network, on a pay-as-you-go basis.
* The key components of cloud infrastructure are:
  + Physical data centers
  + Compute
  + Network
  + Storage
* Platform-as-a-Service is a cloud computing model that provides customers with a complete platform—hardware, software, and infrastructure.
* The high level of abstraction, support services, runtime environments, rapid deployment mechanisms, and middleware capabilities distinguishes PaaS clouds.
* PaaS advantages are:
  + Scalability
  + Faster time to market products and services.
  + Greater agility and innovation
* Software-as-a-Service is a cloud offering that provides users with access to a service provider’s cloud-based software.
* SaaS characteristics are:
  + Multitenant architecture
  + Security, compliance, and maintenance
  + Customization of applications
  + Subscription model
  + Scaling
* SaaS advantages are:
  + Direct procurement of solutions
  + Improved workforce productivity and efficiency
  + Enable distribution of software costs

## Lesson 2 Summary: Deployment Models

* Deployment models indicate where the infrastructure resides, who owns and manages it, and how cloud resources and services are made available to users. There are four main deployment models available on the cloud—public, private, hybrid, and community.
* In the public cloud model, the service provider owns, manages, provisions, and maintains the physical infrastructure such as data centers, servers, networking equipment, and storage, with users accessing virtualized computing, networking and storage resources as services.
* In the private cloud model, the provider provisions the cloud infrastructure for exclusive use by a single organization. The private cloud infrastructure can be internal to the organization and run or on-premises. Or it can be on a public cloud, as in the case of Virtual Private Clouds (VPC), and be owned, managed, and operated by the cloud provider.
* In the hybrid cloud model, an organization’s on-premise private cloud and a third-party, public cloud are connected as a single, flexible infrastructure that leverages the features and benefits of both Public and Private clouds.
* In the community cloud model, the provider provisions the cloud infrastructure for use by a community of organizations with shared concerns. One or more of the organizations in the community, a third-party provider, or both are responsible for the ownership, management, and operation of this infrastructure.

## Module 2 Glossary: Cloud Computing Models

|  |  |
| --- | --- |
| Term | Definition |
| BPM | Business Process Management |
| Composite multicloud | A variant of hybrid multicloud, distributes single applications across multiple providers, allowing you to move application components across cloud services and vendors as needed |
| CRM | Customer Relationship Management |
| HCM | Human Capital Management |
| Hybrid cloud | A computing environment that connects an organization’s on-premises private cloud and third-party public cloud into a single, flexible infrastructure for running the organization’s applications and workloads |
| Hybrid monocloud | A hybrid cloud with one cloud provider |
| Hybrid multicloud | An open standards-based stack that can be deployed on any public cloud infrastructure |
| IaaS | Infrastructure as a service is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the network, on a pay-as-you-go basis |
| IoT | Internet of things |
| MDM | Master Data Management |
| PaaS | Platform as a service is a cloud computing model that provides customers a complete platform—hardware, software, and infrastructure—to develop, deploy, manage, and run applications created by them or acquired from a third-party |
| Pay-as-you-go | Users can order cloud resources from a larger pool of available resources and pay for them on a per-use basis |
| Private Cloud | Cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers, such as the business units within the organization |
| Public cloud | Users get access to servers, storage, network, security, and applications as services delivered by cloud service providers over the internet |
| SaaS | Software as a service is a cloud offering that provides users with access to a service provider’s cloud-based software |
| SIP | SaaS integration platforms |
| TCO | Total cost for ownership |
| VM | Virtual machine |
| VPC | Virtual Private Cloud |

## **MODULE 3 COMPONENTS OF CLOUD COMPUTING**

## Lesson 1 Summary: Cloud Infrastructure

* Cloud infrastructure consists of data centers, storage, networking components, and computing resources.
* Virtualization is the process of creating a software-based version of physical resources, made possible by hypervisors.
* A few different types of Virtual Machines can be provisioned on the cloud. These include:
  + Shared or Public Cloud VMs that are provider-managed, multi-tenant deployments that can be provisioned on-demand with predefined sizes
  + Transient or Spot VMs that take advantage of unused capacity in a cloud data center
  + Reserved VMs that allow you to reserve capacity and guarantee resources for future deployments
  + Dedicated hosts that offer single-tenant isolation
* Bare metal servers are single-tenant physical servers that are dedicated to a single customer. Bare metal servers fulfill the demanding needs of high-performance computing (HPC) and data-intense applications. They are ideal for applications that have a high degree of security or compliance requirements.
* Networking capabilities in the cloud are delivered as a service rather than in the form of rack-mounted devices. Cloud resources such as VMs (or VSIs), storage, network connectivity, and load balancers are deployed into subnets within Virtual Private Clouds (VPCs). Using private and public subnets allows users to deploy multi-tier enterprise applications securely. Load balancers distribute the traffic and allow applications to be responsive.
* Containers are executable units of software in which application code, its libraries, and its dependences are packaged in a common way, so that it can be run anywhere, from desktops, traditional IT, to the cloud. Containers are more lightweight and consume fewer resources than Virtual Machines, helping streamline the development and deployment of cloud native applications.

## Lesson 2 Summary: Cloud Storage and Content Delivery Networks

* Cloud storage is available in four main types–Direct Attached, File, Block, and Object Storage. These storage types differ in how they can be accessed, the capacity they offer, how much they cost, the types of data they are best suited to store, and their read-write speed.
* Direct Attached (or Local) Storage is storage that is presented directly to a cloud-based server and is effectively either within the host server chassis or within the same rack.
* File Storage is typically presented to compute nodes as a Network File System (NFS), which means that the storage is connected to compute nodes over a standard ethernet network.
* Block Storage is presented to compute nodes using high-speed fiber connections, typically provisioned in volumes, which are mounted onto a compute node.
* Object Storage is accessed via an API and doesn’t need an underlying compute node.
* Object Storage offers infinite capacity as you can keep adding files to it and just pay for what you use. Compared to the other storage types, object storage is slowest in terms of read and write speeds.
* A Content Delivery Network (CDN) is a distributed server network that accelerates internet content delivery by delivering temporarily stored or cached copies of website or media content to users based on their geographic location.

## Module 3 Glossary: Components of Cloud Computing

|  |  |
| --- | --- |
| Term | Definition |
| ACL | Access Control Lists |
| AZ | Availability Zones are distinct Data Centers with their own power, cooling, and networking resources. These Zones can have names like DAL-09 or us-east-1. |
| Bare-metal hypervisor | Installed directly on top of the physical server. They're more secure, have lower latency, and are usually the ones you see in the market the most |
| Block storage | Is presented to compute nodes using high-speed fiber connections, which means that read and write speeds are typically much faster and reliable than with file storage |
| CDNs | Content Delivery Networks is a distributed server network that delivers temporarily stored, or cached, copies of website content to users based on the user’s geographic location |
| Cloud Region | A geographic area or location where a Cloud provider’s infrastructure is clustered, and may have names like NA South or US East |
| Containers | Are an executable unit of software in which application code is packaged, along with its libraries and dependencies, in common ways so that it can be run anywhere, whether it be on desktop, traditional IT, or the cloud |
| Data center | A huge room or a warehouse containing cloud infrastructure |
| Dedicated hosts | Offer single-tenant isolation |
| Direct Attached storage | Or Local storage is storage which is presented directly to a cloud-based server and is effectively either within the host server chassis or within the same rack |
| File storage | Is typically presented to compute nodes as ‘NFS Storage’. NFS stands for Network File System and means that the storage is connected to compute nodes over a standard ethernet network |
| Hosted hypervisor | There's a layer of host OS between the physical server and the hypervisor. These hypervisors are less frequently used and mostly used for “end-user” virtualization |
| HPC | High-performance computing |
| Hypervisor | A piece of software that runs above the physical server or host |
| IOPS | Input/Output Operations Per Second and refers to the speed at which the disks can write and read data |
| NFS | Network File Storage |
| Object storage | Storage not attached to a compute node, rather it is accessed via an API |
| Reserved virtual server | Instances allow you to reserve capacity and guarantee resources for future deployments |
| SDN | Software Defined Networking |
| Shared or Public Cloud VMs | Are provider-managed, multi-tenant deployments that can be provisioned on-demand with predefined sizes |
| Transient or Spot VMs | Take advantage of unused capacity in a cloud data center |
| Virtualization | Process of creating a software-based or virtual version of something whether that be compute, storage, networking, servers, or applications |
| VLANs | Virtual Local Area Networks |
| VM | Virtual machines are software-based computers, based on virtualization technologies |
| VPC | Virtual Private Cloud |
| VPN | Virtual Private Networks |

## **MODULE 4 EMERGING TRENDS AND PRACTICES**

## Lesson 1 Summary

* Hybrid multi-cloud is a cloud adoption strategy that makes it possible for public clouds, private clouds, and on-premises IT to interoperate seamlessly while leveraging the best cloud-based services from different public cloud providers.
* Microservices architecture is an approach in which an application is built as a collection of loosely coupled and independently deployable components or services, leading to efficient development, maintenance, and upgradation cycles.
* Serverless computing is an approach to computing that offloads responsibility for common infrastructure management tasks for application runtimes to cloud providers, allowing developers to focus their time and effort on development and testing, and not have to worry about provisioning, maintaining and scaling compute resources.

## DevOps on the Cloud

**Harnessing the Power of DevOps on Cloud Platforms**

**Introduction:**

Organizations strive to deliver software solutions swiftly, reliably, and efficiently in our ever-evolving digital landscape. DevOps, a collaborative approach that unifies software development and operations, has emerged as a significant change. This topic will explain the essence of DevOps, explore its benefits when applied to cloud platforms, and provide real-world use cases that demonstrate its transformative capabilities on popular cloud providers such as AWS, Azure, GCP, and IBM Cloud.

**What is DevOps?**

DevOps is an approach that fosters collaboration between development and operations teams, streamlining the entire software delivery lifecycle. By promoting a culture of collaboration, automation, and continuous feedback, DevOps enables organizations to deliver software products more efficiently and reliably.

**The DevOps Process:**

To better understand the DevOps process, let's explore its key components:

* **Continuous Integration (CI):** Developers integrate their code changes into a shared repository frequently, ensuring early detection of integration issues. Version control systems like Git and Subversion support this process.
* **Continuous Delivery (CD):** Continuous delivery ensures that code changes are always in a state that can be released immediately. This state allows organizations to deploy software anytime with minimal manual intervention. Tools like Jenkins and Bamboo facilitate the automation of build, test, and deployment processes.
* **Continuous Deployment (CDep):** Continuous deployment takes automation further, enabling organizations to automatically deploy software changes into production environments after passing the necessary tests.
* **Continuous Monitoring (CM):** Continuous monitoring provides real-time insights into application and infrastructure performance, allowing organizations to detect issues promptly and take proactive measures. Tools like Prometheus and ELK Stack are commonly used for monitoring in DevOps.

**Benefits of DevOps on Cloud Platforms:**

Implementing DevOps practices on cloud platforms offers several significant advantages:

* **Scalability and Flexibility:** Cloud platforms provide the scalability and flexibility required for DevOps workflows. Organizations can leverage cloud resources to scale infrastructure dynamically, accommodate varying workloads, and optimize resource utilization based on demand.
* **Rapid Provisioning and Deployment:** DevOps on the cloud facilitates rapid provisioning and deployment of infrastructure and applications. Cloud services offer pre-configured environments, automated provisioning, and deployment pipelines, enabling faster time-to-market and reducing manual effort.
* **Cost Optimization:** Cloud-based DevOps enables cost optimization by leveraging the pay-as-you-go model. Organizations can scale resources up or down based on demand, eliminating the need for upfront infrastructure investments, and reducing operational costs.
* **Collaboration and Team Efficiency:** DevOps practices on the cloud foster collaboration and enhance team efficiency. Cloud platforms provide centralized repositories, version control systems, and collaboration tools that facilitate seamless communication and shared code repositories, enabling effective collaboration across teams.
* **Continuous Integration and Delivery:** Cloud services seamlessly integrate with popular DevOps tools, enabling continuous integration and delivery (CI/CD). This automation streamlines build, test, and deployment processes, reducing errors and facilitating faster, more reliable software releases.

**DevOps Use Cases on Cloud Platforms**

Let's explore real-world use cases that highlight the benefits of DevOps on different cloud platforms:

* **DevOps on Amazon Web Services (AWS):** Organizations leveraging DevOps on AWS can take advantage of services such as AWS CodePipeline for CI/CD pipelines, AWS Elastic Beanstalk for simplified application deployment, and AWS Lambda for serverless computing. This use case enables seamless scalability, efficient resource management, and rapid delivery of software solutions.
* **DevOps on Microsoft Azure:** DevOps on Azure empowers organizations with services like Azure DevOps for collaboration, Azure Kubernetes Service (AKS) for container orchestration, and Azure Functions for serverless computing. Organizations can achieve automated deployments, efficient scaling, and improved application performance by leveraging these services.
* **DevOps on Google Cloud Platform (GCP):** DevOps on GCP offers services such as Cloud Build for CI/CD pipelines, Google Kubernetes Engine (GKE) for container management, and Cloud Functions for serverless computing. This use case enables organizations to automate infrastructure provisioning, manage complex containerized applications effectively and optimize resource utilization.
* **DevOps on IBM Cloud:** DevOps on IBM Cloud provides services like IBM Continuous Delivery for automated deployments, IBM Kubernetes Service (IKS) for container orchestration, and IBM Functions for serverless computing. These use cases allow organizations to achieve streamlined software delivery, efficient infrastructure management, and seamless scaling on the IBM Cloud platform.

**Conclusion**

When combined with cloud platforms, DevOps empowers organizations to streamline software delivery, enhance collaboration, and leverage scalable resources. By implementing DevOps on popular cloud providers such as AWS, Azure, GCP, and IBM Cloud, organizations can accelerate their software delivery cycles, reduce time-to-market, and adapt to changing business needs effectively. It is a winning combination that enables organizations to stay competitive in today's fast-paced digital landscape

## Lesson 2 Summary

* Cloud native applications are applications that are built or refactored to work in the cloud environment. These applications, developed using DevOps methodologies, consist of microservices packaged in containers that can run in any environment—making it possible to create and update features in quick iterative cycles.
* DevOps is a collaborative approach that enables development and operations teams to continuously deliver software in quick iterative cycles while reducing overhead, duplication, and rework. DevOps’ tools, practices, and processes help tackle the complexities and challenges posed by the cloud, allowing solutions to be delivered and updated quickly and reliably.
* Application modernization helps organizations accelerate their digital transformation, take advantage of new technologies and services, and become more responsive to changing market dynamics. Cloud computing is one of the key enablers of application modernization.

## Module 4 Glossary: Emergent Trends and Practices

|  |  |
| --- | --- |
| Term | Definition |
| API | Application Programming Interface |
| Application modernization | Helps organizations accelerate their digital transformation, take advantage of new technologies and services, and become more responsive to changing market dynamics |
| Cloud native application | An application developed from the outset to work only in the cloud environment, or an existing app that has been refactored and reconfigured with cloud native principles |
| Continuous delivery | Delivering small, well-designed, high-quality increments of software to customers |
| Continuous deployment | Progressing each new packaged build through the deployment lifecycle as rapidly as possible |
| Continuous integration | Creating packaged builds of the code changes released as immutable images |
| Continuous monitoring | Monitoring with tools that help developers understand the performance and availability of their applications, even before they’re deployed to production |
| Delivery pipeline | An automated sequence of steps that involves the stages of Ideation, Coding, Building, Deploying, Managing, and Continuous Improvement |
| DevOps | Collaborative approach where business owners and the development, operations, and quality assurance teams collaborate to continuously deliver software |
| Hybrid multicloud | An open standards-based stack that can be deployed on any public cloud infrastructure |
| Microservices | Break down large applications into their core functions |
| Microservices architecture | Approach in which a single application is composed of many loosely coupled and independently deployable, smaller components or services |
| Monolithic architecture | Approach in which a single application is built out of one piece of software |
| Serverless | Approach to computing that offloads responsibility for common infrastructure management tasks |
| Service discovery | Creates a roadmap for microservices to communicate |

## **MODULE 5 CLOUD SECURITY, MONITORING, CASE STUDIES, JOBS**

## Policies and Principles of Access Management

**Policies**

A policy in cloud security refers to a set of rules and guidelines that determine how users should access and protect resources within a cloud environment. These policies provide a framework for maintaining security, ensuring compliance with industry regulations, and mitigating potential risks.

The format of a policy typically includes the following:

* A title that provides a descriptive name or identifier for the policy
* The scope of the policy, which defines the specific resources, systems, or individuals to which the policy applies
* The objective of the policy, or its goals and purpose
* A policy statement that lists the rules, procedures, and restrictions of the policy
* The roles and responsibilities of the individuals and groups that are enforcing and adhering to the policy
* Compliance and enforcement details or the measures taken to monitor and ensure policy compliance
* A review and revision section which outlines how often to review and update the policy to remain relevant and effective

**Service provider and customer-managed policies**

Cloud service providers (CSPs) typically have security policies that govern the overall security of their infrastructure, data centers, and services. These policies ensure a baseline level of security and protection for customer data. Service provider policies cover various aspects such as physical security, network security, data encryption, access controls, and incident response.

In addition to service provider policies, customers can implement their own policies, also known as customer-managed policies. These policies allow customers to tailor security measures according to their requirements, industry regulations, and risk tolerance. Customer-managed policies can include additional security controls, access restrictions, data protection measures, and compliance frameworks.

By combining service provider and customer-managed policies, organizations can establish a comprehensive security framework that aligns with their unique needs while benefiting from the underlying security measures provided by the cloud service provider.

**Principle of Least Privilege**

The principle of least privilege is a key concept in access control that minimizes the risk of unauthorized access or accidental misuse of resources. It dictates that organizations should grant users only the minimum necessary permissions required to perform their tasks. By following the principle of least privilege, organizations limit the potential damage caused by compromised user accounts.

**User Access Level**

In a cloud environment, user access levels vary depending on their roles and responsibilities. Some users may only need access to the console, or the graphical user interface (GUI) provided by the cloud service provider for resource management and configuration. These users interact with the cloud through the console to perform tasks such as provisioning resources, monitoring, and administration.

On the other hand, users involved in software development may require access to the development environment. This environment includes tools, APIs, and services necessary for building, testing, and deploying applications in the cloud. These users interact with the cloud infrastructure using APIs and command-line interfaces (CLIs) rather than relying solely on the console.

Depending on the organization’s requirements, certain users may have access to both the console and development environment, enabling them to perform a broader range of tasks and responsibilities.

**Identity and Access Management (IAM)**

Identity and Access Management (IAM) enables organizations to manage and authenticate users’ identities and access to resources in a cloud environment. It involves the processes and policies that ensure that only authorized individuals have access privileges to sensitive systems, applications, and data. IAM simplifies user management by centralizing user provisioning, authentication, and authorization processes, making granting or revoking access rights easier as needed. This process helps organizations enhance security, protect sensitive information, enforce compliance with regulations, and streamline administrative tasks related to user access.

**Standard Password Policy**

A standard password policy for users logging into the cloud should adhere to best practices to ensure strong password security. Typically, a password policy includes requirements for password complexity, such as a minimum length and a combination of upper and lowercase letters, numbers, and special characters. The policy may also define password expiration intervals, after which users must change their passwords. Additionally, enforcing a password history, which is a required number of unique passwords used before reusing an old password, adds an extra layer of protection against password reuse. Other password policies may include account lockout, multi-factor authentication, and user awareness and training. The specific requirements of a password policy will depend on the organization’s needs, requirements, and risk assessments.

**Identity provider standards (SAML, OpenID)**

Identity provider standards are protocols and frameworks that define how identity providers (IdPs) and service providers (SPs) securely exchange authentication and identity information. These standards ensure consistent and standardized approaches to authentication and access management. Two widely used identity provider standards are:

* Security Assertion Markup Language (SAML) - SAML is an XML-based standard for exchanging authorization and authentication data between IdPs and SPs. It enables secure single sign-on (SSO) and identity federation. SAML allows users to authenticate once with their IdP and access multiple SPs without needing separate authentication. SAML assertions contain information about the user’s identity and attributes, which SPs rely on to grant access to their resources.
* OpenID Connect - OpenID Connect is a modern standard built on the OAuth 2.0 protocol. It provides a framework for authentication and identity federation. OpenID Connect allows users to authenticate using their chosen OpenID provider and obtain an ID token that contains information about their identity. Service providers can use the ID token to authenticate users and provide access to their resources.

These identity provider standards offer secure and interoperable solutions for managing authentication and access control in various contexts, including cloud environments, web applications, and enterprise systems. They enable organizations to establish trust relationships between identity providers and service providers, simplify user authentication experiences, and enhance security by centralizing identity management.

## Cloud Monitoring and Benefits

**Introduction:**

Cloud computing has transformed the business landscape, offering scalability, flexibility, and cost-efficiency. However, it also introduces unique challenges in ensuring the security, performance, and availability of cloud-based services. Monitoring plays a critical role in proactively detecting and addressing potential issues. In this blog post, we will explore how monitoring can be achieved in the cloud using techniques such as alarms, logs, metrics, events, and service-based monitoring, including Infrastructure as Code (IaC).

IaC has emerged as a powerful approach to automate the provisioning and configuration of cloud resources. With IaC, organizations define their infrastructure requirements through code, allowing consistent and repeatable deployments. Monitoring IaC deployments is crucial in ensuring a strong infrastructure that can detect any configuration drift. By incorporating IaC monitoring alongside other monitoring approaches, organizations can achieve greater control and visibility over their cloud infrastructure.

Additionally, we will delve into the importance of tracking API calls for audit purposes. API calls are a gateway for interacting with various cloud services, making the calls crucial for security and compliance. Organizations can maintain an audit trail by tracking and storing API calls, ensuring transparency, accountability, and regulatory compliance. Furthermore, we will discuss attacks, vulnerabilities, risks, and mitigation measures associated with cloud monitoring to provide a comprehensive understanding of the potential risks and the steps needed to mitigate them effectively.

Through this exploration, we aim to equip readers with the knowledge and insights to establish robust cloud monitoring practices, effectively track API calls, and mitigate potential risks. By embracing comprehensive monitoring strategies, including service-based and IaC monitoring, organizations can optimize their cloud infrastructure, enhance security, and deliver exceptional services in the dynamic and ever-evolving cloud environment.

**1. The Fundamentals of Cloud Monitoring:**

Monitoring in the cloud environment encompasses several vital components. Alarms are set to be proactive for specific events or thresholds, enabling organizations to respond promptly to critical situations. Logs are essential in collecting and analyzing data to gain insight into system behavior. Log management services provide efficient storage and retrieval capabilities, while log aggregation and analysis tools help detect anomalies and troubleshoot issues.

Metrics allow organizations to collect and visualize performance data through cloud-provided metrics. Establishing baseline metrics makes it easier to identify anomalies and make informed decisions. Monitoring dashboards offer real-time visibility into system health, enabling quick responses to potential issues.

Events capture and process real-time events within the cloud infrastructure. Event-driven architectures leverage them to trigger actions based on specific criteria. Organizations can efficiently mitigate potential threats by integrating event monitoring with incident response workflows.

**2. Service-Based Monitoring for Enhanced Cloud Management:**

Service-based monitoring focuses on specific cloud services to optimize performance and ensure efficient resource utilization. Load balancing monitoring involves tracking workload distribution and identifying potential bottlenecks. Alarms monitor load balancer health and performance issues, enabling organizations to respond promptly.

Content delivery monitoring involves monitoring content delivery networks (CDNs) for efficient content distribution. Performance, latency, and cache hit rates are proactively tracked to ensure an optimal user experience. In the event of content delivery issues, troubleshooting measures can rectify the situation promptly.

Auto-scaling monitoring is essential for dynamically adjusting resource capacity in response to changing demands. By monitoring auto-scaling groups, organizations can track scaling events and evaluate the effectiveness of scaling policies. Coordination between monitoring and scaling activities ensures seamless scalability.

Infrastructure as Code (IaC) monitoring is critical for organizations utilizing automation and provisioning resources through code. Monitoring IaC deployments enables verification of infrastructure changes and detects any drift from the desired state. Configuration issues need to be identified and rectified promptly to maintain the integrity of the infrastructure.

**3. Tracking API Calls for Audit Purposes:**

API monitoring is essential for security and compliance in cloud environments. Organizations must recognize the significance of API calls and the risks associated with unauthorized or malicious API activity. By implementing API monitoring, organizations can configure audit trails and access controls to track API activities. Analyzing logs and detecting anomalies help identify suspicious API behavior, ensuring transparency and accountability in cloud service usage.

The following are examples of cloud services that track API calls.

* **Amazon Web Services (AWS) CloudTrail:** AWS CloudTrail is a service that enables organizations to monitor, log, and retain API activity across their AWS accounts. It records API calls made to AWS services and provides detailed information such as the caller's identity, the time of the API call, and the parameters used. By enabling CloudTrail, organizations can maintain an audit trail of API activities, ensuring transparency and accountability. The CloudTrail logs are analyzed to identify unauthorized or suspicious API behavior.
* **Google Cloud Audit Logging:** Google Cloud Platform (GCP) provides Audit Logging, which captures API calls and system events across various GCP services. It allows organizations to track activities related to resource creation, deletion, modification, and access control changes. Audit Logging provides detailed logs that are monitored and analyzed to detect anomalous API behavior. By leveraging Audit Logging, organizations can maintain an audit trail for API activities and enforce compliance with security policies.
* **Microsoft Azure Activity Logs:** Azure Activity Logs record API calls and other administrative actions performed. These logs capture the operation type, resource actions, and the caller's identity. By enabling Azure Activity Logs, organizations can track API activities, detect unauthorized or malicious behavior, and maintain an audit trail for compliance.
* **Salesforce Event Monitoring:** Salesforce offers Event Monitoring, a service that logs API calls and user activities within the Salesforce platform. It provides detailed information about API operations, user logins, data exports, and other system events. Event Monitoring enables organizations to track API activities, monitor user behavior, and identify potential security risks or policy violations.

These examples highlight how specific cloud services can track API calls and maintain audit trails. Organizations can effectively monitor and analyze API activities by utilizing services like AWS CloudTrail, Google Cloud Audit Logging, Azure Activity Logs, and Salesforce Event Monitoring, ensuring transparency, accountability, and compliance with security policies and regulations.

**4. Likely Attacks, Vulnerabilities, Risks, and Mitigation Measures:**

Cloud environments are susceptible to various attacks and vulnerabilities. Distributed Denial of Service (DDoS) attacks can overwhelm cloud resources with excessive traffic, leading to disruptions. Data breaches risk unauthorized access to sensitive data stored in the cloud. Misconfigurations, such as insecure or improper setup of cloud services, can also expose vulnerabilities.

To mitigate these risks, organizations must implement strong authentication and access controls. Data encryption at rest and in transit is crucial for protecting sensitive information. Regular vulnerability assessments and penetration testing help identify potential weaknesses while monitoring network traffic and behavior analytics enable the detection of anomalies and early response to potential threats.

Cloud environments face various attacks, vulnerabilities, and risks. Let's explore some examples:

* **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks aim to overwhelm cloud resources by flooding them with excessive traffic, leading to service disruptions. Cloud service providers offer services that help mitigate DDoS attacks. For instance, AWS provides AWS Shield, a managed DDoS protection service. It automatically detects and mitigates DDoS attacks, ensuring the availability of cloud resources even during an attack. Similarly, Google Cloud offers the Cloud Armor service, which protects against DDoS attacks through global HTTP(S) load balancing and security system rules.
* **Data Breaches:** Data breaches pose a significant risk in cloud environments, as they can result in unauthorized access to sensitive data stored in the cloud. Cloud service providers offer robust security measures to protect data. For example, Microsoft Azure provides Azure Key Vault, enabling organizations to store and manage cryptographic keys and secrets securely. AWS offers AWS Key Management Service (KMS), allowing organizations to encrypt data at rest and control access to encryption keys.
* **Misconfigurations:** Misconfigurations in cloud services can lead to security vulnerabilities and expose sensitive data to unauthorized access. For example, misconfigured access control policies or open storage buckets can provide unintended access to data. Cloud service providers often offer security configuration tools and services. AWS provides AWS Config, allowing organizations to continuously assess and audit resource configurations. Google Cloud delivers Cloud Security Command Center, a centralized security management and data risk assessment platform.
* **Insider Threats:** Insider threats involve unauthorized or malicious actions by individuals with legitimate access to cloud resources. These individuals may intentionally abuse their privileges or inadvertently cause security incidents. Cloud service providers offer identity and access management services to mitigate insider threats. For instance, Azure Active Directory provides robust authentication and access controls to ensure only authorized users can access resources.

**Conclusion:**

Monitoring is vital to cloud management, ensuring cloud-based services' security, performance, and availability. Organizations can proactively address potential issues and optimize their cloud infrastructure by utilizing techniques such as alarms, logs, metrics, events, service-based monitoring, and tracking API calls for audit purposes. Understanding attacks, vulnerabilities, risks, and mitigation measures help organizations fortify their cloud environment. Robust monitoring practices and thorough audit trail tracking are essential for maintaining a secure and efficient cloud ecosystem. By embracing comprehensive cloud monitoring strategies, organizations can optimize their cloud infrastructure and deliver exceptional services while mitigating potential risks.

## Lesson Summary: Cloud Security and Monitoring

* Cloud security refers to the policies, technological procedures, services, and solutions designed to secure enterprise applications and data on the cloud against insider threats, data breaches, compliance issues, and organized security threats.
* Cloud security is a shared responsibility between the cloud provider and the user organization.
* Security architecture and methods for achieving continuous security need to be embedded through the life cycle of an application to ensure that the application runs on a safe platform, the code is free from vulnerabilities, and the operational risks are understood.
* Identity and Access Management, also known as access control, helps authenticate and authorize users and provides user-specific access to cloud resources, services, and applications.
* As part of their Identity and Access Management services, most cloud providers offer users the ability to define access groups and create access policies that define permissions for users on account resources.
* Cloud encryption, often called the last line of defense, encrypts data and provides robust data access control, key management, and certificate management.
* Data needs encryption in three states:
  + Encryption at rest: Protecting data while it is stored
  + Encryption in transit: Protecting data while it is transmitted from one location to another
  + Encryption in use: Protecting data when it is in use in memory
* All connected systems and cloud-based services should be monitored to maintain visibility of all data exchanges between public, private, and hybrid cloud environments. This ensures that the cloud provides a trusted platform to integrate with your enterprise data centers securely.

## Lesson Summary: Case Studies and Jobs

* Businesses all over the world are realizing tangible benefits from the use of cloud technologies and services, including:
  + The Weather Company migrating to the cloud to reliably deliver critical weather data at high speed, especially during major weather events such as hurricanes and tornadoes
  + American Airlines using the cloud platform and technologies to deliver digital self-service tools and customer value more rapidly across its enterprise
  + Cementos Pacasmayo achieving operational excellence and insight to help drive strategic transformation and reach new markets using cloud services
  + Welch choosing cloud storage to drive business value from hybrid cloud
  + LiquidPower using cloud-based SAP applications to fuel business growth
* The market size of the cloud services industry is at nearly three times the growth of overall IT services, increasing the need for qualified cloud computing professionals. Some common job roles that are available in this domain include Cloud Software Engineers, Cloud Integration Specialists, Cloud Data Engineers, Cloud Security Engineers, Cloud DevOps Engineers, and Cloud Solution Architects.

## Module 5 Glossary: Cloud Security, Monitoring, Case Studies, & Jobs

|  |  |
| --- | --- |
| Term | Definition |
| Access group | A group of users and service IDs is created so that the same access can be assigned to all entities within the group with one or more access policies. |
| Administrative users | Create, update, and delete application and service instances, and need insight into their team members’ activities. |
| API keys | Unique identifiers are passed into an API to identify calling application or user. |
| Application Performance Monitoring (APM) | Measures application availability and performance, providing tools needed to troubleshoot issues in an application's environment. |
| Application users | Users of the cloud-hosted applications. |
| AppSec | Application Security. |
| Audit and compliance | A critical service within identity and access framework used to validate implemented controls against policies. |
| Authentication | Also known as identity service, it enables applications deployed to the cloud to authenticate users at an application level. |
| BYOK | Bring Your Own Keys. |
| Client-side encryption | Occurs before data is sent to cloud storage. |
| Cloud directory services | Used to securely manage user profiles and associated credentials inside a cloud environment. |
| Cloud encryption | Also known as the last line of defense, it encrypts data and provides robust data access control, key management, and certificate management. |
| Cloud monitoring solutions | Assess data, application, and infrastructure behaviors for performance, resource allocation, network availability, compliance, and security risks and threats. |
| Cloud security | Policies, technological procedures, services, and solutions designed to secure the enterprise applications and data on the cloud against insider threats, data breaches, compliance issues, and organized security threats. |
| Database monitoring tools | Help track processes, queries, and availability of services to ensure the accuracy and reliability of database management systems. |
| Decryption key | Defines how the encrypted data will be transformed back to legible data. |
| Developer users | Authorized to read sensitive information and to create, update, and delete applications. |
| Encryption | Scrambling data to make it illegible. |
| Encryption algorithm | Defines the rules by which data will be transformed so that it becomes illegible. |
| Encryption at rest | Protecting data while it is stored. |
| Encryption in transit | Protecting data while it is transmitted from one location to another. |
| Encryption in use | Protecting data when it is in use in memory. |
| Identity and access management | Also known as access control, it helps authenticate and authorize users and provides user-specific access to cloud resources, services, and applications. |
| Infrastructure monitoring tools | Identify minor and large-scale hardware failures and security gaps so that developers and administrators can take corrective action before problems affect user experience. |
| Key management services | Help perform life cycle management for encryption keys that are used in cloud services or customer-build apps. |
| KYOK | Keep Your Own Keys. |
| Multifactor authentication | Adds an additional layer or authentication for application users. |
| Reporting | Provides a user-centric view of access to resources. |
| Server-side encryption | Occurs after cloud storage receives your data but before the data is written to disk and stored. |
| SSL | Secure Sockets Layer. |
| TLS | Transport Layer Security. |
| User and service access management capability | Enables cloud application and service owners to provision and de-provision user profiles with minimal human interaction. |