**DESCRIPTIVE QUESTION BANK**

1. Explain overview and usage of Google Cloud Platform [10 marks]

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, file storage, and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning. Registration requires a credit card or bank account details. Google Cloud Platform provides infrastructure as a service, platform as a service, and serverless computing environments. Google Cloud Platform is a part of Google Cloud, which includes the Google Cloud Platform public cloud infrastructure, as well as Google Workspace (G Suite), enterprise versions of Android and Chrome OS, and application programming interfaces (APIs) for machine learning and enterprise mapping services.

Google cloud features:

1. **Google Cloud resources**

Google Cloud consists of a set of physical assets, such as computers and hard disk drives, and virtual resources, such as virtual machines (VMs), that are contained in Google's data centers around the globe. Each data center location is in a region. Regions are available in Asia, Australia, Europe, North America, and South America. Each region is a collection of zones, which are isolated from each other within the region. Each zone is identified by a name that combines a letter identifier with the name of the region. For example, zone a in the East Asia region is named asia-east1-a. This distribution of resources provides several benefits, including redundancy in case of failure and reduced latency by locating resources closer to clients. This distribution also introduces some rules about how resources can be used together.

1. **Accessing resources through services**

In cloud computing, what you might be used to thinking of as software and hardware products, become services. These services provide access to the underlying resources. The list of available Google Cloud services is long, and it keeps growing. When you develop your website or application on Google Cloud, you mix and match these services into combinations that provide the infrastructure you need, and then add your code to enable the scenarios you want to build.

1. **Global, regional, and zonal resources**

Some resources can be accessed by any other resource, across regions and zones. These global resources include preconfigured disk images, disk snapshots, and networks. Some resources can be accessed only by resources that are located in the same region. These regional resources include static external IP addresses. Other resources can be accessed only by resources that are located in the same zone. These zonal resources include VM instances, their types, and disks.

1. **Projects**

Any Google Cloud resources that you allocate and use must belong to a project. You can think of a project as the organizing entity for what you're building. A project is made up of the settings, permissions, and other metadata that describe your applications. Resources within a single project can work together easily, for example by communicating through an internal network, subject to the regions-and-zones rules. A project can't access another project's resources unless you use Shared VPC or VPC Network Peering.

Each Google Cloud project has the following:

* A project name, which you provide.
* A project ID, which you can provide or Google Cloud can provide for you.
* A project number, which Google Cloud provides.

As you work with Google Cloud, you'll use these identifiers in certain command lines and API calls.

Google Cloud gives you three basic ways to interact with the services and resources:

1. **Google Cloud Console**

The Google Cloud Console provides a web-based, graphical user interface that you can use to manage your Google Cloud projects and resources. When you use the Cloud Console, you either create a new project or choose an existing project, and then use the resources that you create in the context of that project. You can create multiple projects and use them to separate your work in whatever way makes sense for you. For example, you might start a new project if you want to make sure only certain team members can access the resources in that project, while all team members can continue to access resources in another project.

1. **Command-line interface**

If you prefer to work at the command line, you can perform most Google Cloud tasks by using the gcloud command-line tool. The gcloud tool lets you manage development workflow and Google Cloud resources in a terminal window. For example, you can create a Compute Engine virtual machine (VM) instance by running the gcloud compute instances create command in the shell environment.

* You can run gcloud commands in the following ways: You can install the Cloud SDK. The SDK includes the gcloud tool, so you can open a terminal window on your own computer and run commands to manage Google Cloud resources.
* You can use Cloud Shell, which is a browser-based shell. Because it runs in a browser window, you don't need to install anything on your own computer. You can open the Cloud Shell from the Google Cloud Console.

Cloud Shell provides the following:

* + A temporary Compute Engine virtual machine instance.
  + A built-in code editor.
  + 5 GB of persistent disk storage.
  + Pre-installed Cloud SDK and other tools.
  + Language support for Java, Go, Python, Node.js, PHP, Ruby and .NET.
  + Web preview functionality.
  + Built-in authorization for access to Cloud Console projects and resources.

1. **Client libraries**

The Cloud SDK includes client libraries that enable you to easily create and manage resources. Google Cloud client libraries expose APIs for two main purposes:

* App APIs provide access to services. App APIs are optimized for supported languages, such as Node.js and Python. The libraries are designed around service metaphors, so you can work with the services more naturally and write less boilerplate code. The libraries also provide helpers for authentication and authorization.
* Admin APIs offer functionality for resource management. For example, you can use admin APIs if you want to build your own automated tools.

You also can use the Google API client libraries to access APIs for products such as Maps, Drive, and YouTube.

Uses of GCP:

Google lists over 100 products under the Google Cloud brand. Some of the key services are listed below:

1. **Compute**

* App Engine - Platform as a Service to deploy Java, PHP, Node.js, Python, C#, .Net, Ruby and Go applications.
* Compute Engine - Infrastructure as a Service to run Microsoft Windows and Linux virtual machines.
* Google Kubernetes Engine (GKE) or GKE on-prem offered as part of Anthos platform - Containers as a Service based on Kubernetes.
* Cloud Functions - Functions as a Service to run event-driven code written in Node.js, Java, Python, or Go.
* Cloud Run - Compute execution environment based on Knative. Offered as Cloud Run (fully managed) or as Cloud Run for Anthos. Currently supports GCP, AWS and VMware management.

1. **Storage & Databases**

* Cloud Storage - Object storage with integrated edge caching to store unstructured data.
* Cloud SQL - Database as a Service based on MySQL, PostgreSQL and Microsoft SQL Server.
* Cloud Bigtable - Managed NoSQL database service.
* Cloud Spanner - Horizontally scalable, strongly consistent, relational database service.
* Cloud Datastore - NoSQL database for web and mobile applications.
* Persistent Disk - Block storage for Compute Engine virtual machines.
* Cloud Memory store - Managed in-memory data store based on Redis and Memcached.
* Local SSD: High-performance, transient, local block storage.
* Filestore: High-performance file storage for Google Cloud users.

1. **Networking**

* VPC - Virtual Private Cloud for managing the software defined network of cloud resources.
* Cloud Load Balancing - Software-defined, managed service for load balancing the traffic.
* Cloud Armor - Web application firewall to protect workloads from DDoS attacks.
* Cloud CDN - Content Delivery Network based on Google's globally distributed edge points of presence.
* Cloud Interconnect - Service to connect a data center with Google Cloud Platform
* Cloud DNS - Managed, authoritative DNS service running on the same infrastructure as Google.
* Network Service Tiers - Option to choose Premium vs Standard network tier for higher-performing network.

1. **Big Data**

* BigQuery - Scalable, managed enterprise data warehouse for analytics.
* Cloud Dataflow - Managed service based on Apache Beam for stream and batch data processing.
* Cloud Dataproc - Big data platform for running Apache Hadoop and Apache Spark jobs.
* Cloud Composer - Managed workflow orchestration service built on Apache Airflow.
* Cloud Datalab - Tool for data exploration, analysis, visualization and machine learning. This is a fully managed Jupyter Notebook service.
* Cloud Dataprep - Data service based on Trifacta to visually explore, clean, and prepare data for analysis.
* Cloud Pub/Sub - Scalable event ingestion service based on message queues.
* Cloud Data Studio - Business intelligence tool to visualize data through dashboards and reports.

1. **Cloud AI**

* Cloud AutoML - Service to train and deploy custom machine, learning models. As of September 2018, the service is in Beta.
* Cloud TPU - Accelerators used by Google to train machine learning models.
* Cloud Machine Learning Engine - Managed service for training and building machine learning models based on mainstream frameworks.
* Cloud Job Discovery - Service based on Google's search and machine learning capabilities for the recruiting ecosystem.
* Dialogflow Enterprise -  Development environment based on Google's machine learning for building conversational interfaces.
* Cloud Natural Language - Text analysis service based on Google Deep Learning models.
* Cloud Speech-to-Text - Speech to text conversion service based on machine learning.
* Cloud Text-to-Speech - Text to speech conversion service based on machine learning.
* Cloud Translation API - Service to dynamically translate between thousands of available language pairs
* Cloud Vision API - Image analysis service based on machine learning
* Cloud Video Intelligence - Video analysis service based on machine learning.

1. **Management Tools**

* Operations suite (formerly Stackdriver ) - Monitoring, logging, and diagnostics for applications on Google Cloud Platform and AWS.
* Cloud Deployment Manager  - Tool to deploy Google Cloud Platform resources defined in templates created in YAML, Python or Jinja2.
* Cloud Console - Web interface to manage Google Cloud Platform resources.
* Cloud Shell - Browser-based shell command-line access to manage Google Cloud Platform resources.
* Cloud Console Mobile App - Android and iOS application to manage Google Cloud Platform resources.
* Cloud APIs - APIs to programmatically access Google Cloud Platform resources.

1. **Identity & Security**

* Cloud Identity - Single sign-on (SSO) service based on SAML 2.0 and OpenID.
* Cloud IAM - Identity & Access Management (IAM) service for defining policies based on role-based access control.
* Cloud Identity-Aware Proxy - Service to control access to cloud applications running on Google Cloud Platform without using a VPN.
* Cloud Data Loss Prevention API - Service to automatically discover, classify, and redact sensitive data.
* Security Key Enforcement - Two-step verification service based on a security key.
* Cloud Key Management Service - Cloud-hosted key management service integrated with IAM and audit logging.
* Cloud Resource Manager - Service to manage resources by project, folder, and organization based on the hierarchy.
* Cloud Security Command Center - Security and data risk platform for data and services running in Google Cloud Platform.
* Cloud Security Scanner - Automated vulnerability scanning service for applications deployed in App Engine.
* Access Transparency - Near real-time audit logs providing visibility to Google Cloud Platform administrators.
* VPC Service Controls - Service to manage security perimeters for sensitive data in Google Cloud Platform services.

1. **IoT**

* Cloud IoT Core - Secure device connection and management service for Internet of Things.
* Edge TPU - Purpose-built ASIC designed to run inference at the edge. As of September 2018, this product is in private beta.
* Cloud IoT Edge - Brings AI to the edge computing layer.

1. **API Platform**

* Maps Platform - APIs for maps, routes, and places based on Google Maps.
* Apigee API Platform - Lifecycle management platform to design, secure, deploy, monitor, and scale APIs.
* API Monetization - Tool for API providers to create revenue models, reports, payment gateways, and developer portal integrations.
* Developer Portal - Self-service platform for developers to publish and manage APIs.
* API Analytics - Service to analyse API-driven programs through monitoring, measuring, and managing APIs.
* Apigee Sense -  Enables API security by identifying and alerting administrators to suspicious API behaviours.
* Cloud Endpoints - A NGINX-based proxy to deploy and manage APIs.
* Service Infrastructure - A set of foundational services for building Google Cloud products.

1. Explain in detail 12 Factors app. [10 marks]

https://12factor.net/

1. Short note on: Spring boot fundamental, APIfication [5 marks each]

Spring Boot is an open-source Java-based framework used to create a micro-Service. It is developed by Pivotal Team and is used to build stand-alone and production ready spring applications. This chapter will give you an introduction to Spring Boot and familiarizes you with its basic concepts.

Spring Boot provides a good platform for Java developers to develop a stand-alone and production-grade spring application that you can just run. You can get started with minimum configurations without the need for an entire Spring configuration setup.

Advantages:

* Easy to understand and develop spring applications
* Increases productivity
* Reduces the development time

Goals:

* To avoid complex XML configuration in Spring
* To develop a production ready Spring applications in an easier way
* To reduce the development time and run the application independently
* Offer an easier way of getting started with the application

Spring boor features:

* It provides a flexible way to configure Java Beans, XML configurations, and Database Transactions.
* It provides a powerful batch processing and manages REST endpoints.
* In Spring Boot, everything is auto configured; no manual configurations are needed.
* It offers annotation-based spring application
* Eases dependency management
* It includes Embedded Servlet Container

Spring Boot Working:

Spring Boot automatically configures your application based on the dependencies you have added to the project by using @EnableAutoConfiguration annotation. For example, if MySQL database is on your classpath, but you have not configured any database connection, then Spring Boot auto-configures an in-memory database. The entry point of the spring boot application is the class contains @SpringBootApplication annotation and the main method. Spring Boot automatically scans all the components included in the project by using @ComponentScan annotation. Handling dependency management is a difficult task for big projects. Spring Boot resolves this problem by providing a set of dependencies for developer’s convenience. For example, if you want to use Spring and JPA for database access, it is sufficient if you include spring-boot-starter-data-jpa dependency in your project.

Note that all Spring Boot starters follow the same naming pattern spring-boot-starter- \*, where \* indicates that it is a type of the application.

Application programming interfaces (APIs) enable to drive new business by offering external and internal consumers seamless engagement with a company’s data and functions. APIs expose critical parts of an application to enable better utilization of technology investments. With technical advancements, APIs are also driving digital transformation initiatives and enabling IoT devices to communicate.

APIfication is creating APIs by businesses and organizations to expose assets to internal and external groups strategically. It makes access to information much more accessible and promotes the rapid development of new capabilities. APIfication also significantly reduces the amount of rework required should you switch to a different vendor or data source.

**APIfication benefits**

* Outsourcing the data and functionality through a standard interface helps in providing excellent services, making better applications, and improve customer experiences.
* APIs act as a layer of abstraction between data and logic required to run a task at the source.
* APIs are applied to increase Mobility and Developer Productivity by taking an existing feature and using it anywhere instead of re-creating those features. Using existing features helps in minimizing application development time from months to weeks.
* By eliminating barriers, customers can easily access your interface, which allows them to use your product according to their needs.
* Focusing on analysing the API services rather than application usability, you can utilize Customer Insights in making improvements that matter most to your top customers.
* Automating requests and providing open access to your API is an invaluable way to streamline operations and create and maintain long-term, profitable business relationships.
* An API allows ease of integration by allowing different platforms, applications, and systems to connect and share information and carry out different tasks. APIs automate tasks, provide better integration, and simplify the implementation of new applications and business models.

1. What is asymmetric cryptography. Explain any one algorithm in detail. [10 marks]

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key. A private key -- also known as a secret key -- is shared only with key's initiator. When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory and use it to encrypt the message before sending it. The recipient of the message can then decrypt the message using their related private key. If the sender encrypts the message using their private key, the message can be decrypted only using that sender's public key, thus authenticating the sender. These encryption and decryption processes happen automatically; users do not need to physically lock and unlock the message.

Many protocols rely on asymmetric cryptography, including the transport layer security (TLS) and secure sockets layer (SSL) protocols, which make HTTPS possible. The encryption process is also used in software programs that need to establish a secure connection over an insecure network, such as browsers over the internet, or that need to validate a digital signature. Increased data security is the primary benefit of asymmetric cryptography. It is the most secure encryption process because users are never required to reveal or share their private keys, thus decreasing the chances of a cybercriminal discovering a user's private key during transmission.

The various algorithms for Asymmetric Cryptography are:

* Diffie-Hellman
* RSA
* ECC
* El Gamal
* DSA

**Digital Signature Algorithm:**

The DSA algorithm works in the framework of public-key cryptosystems and is based on the algebraic properties of modular exponentiation, together with the discrete logarithm problem, which is considered to be computationally intractable. The algorithm uses a key pair consisting of a public key and a private key. The private key is used to generate a digital signature for a message, and such a signature can be verified by using the signer's corresponding public key. The digital signature provides message authentication (the receiver can verify the origin of the message), integrity (the receiver can verify that the message has not been modified since it was signed) and non-repudiation (the sender cannot falsely claim that they have not signed the message).

With DSA, the entropy, secrecy, and uniqueness of the random signature value k are critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to reveal the private key x.

This issue affects both DSA and ECDSA – in December 2010, a group calling itself fail0verflow announced recovery of the ECDSA private key used by Sony to sign software for the PlayStation 3 game console. The attack was made possible because Sony failed to generate a new random k for each signature. This issue can be prevented by deriving k deterministically from the private key and the message hash, as described by RFC 6979. This ensures that k is different for each H(m)and unpredictable for attackers who do not know the private key x. In addition, malicious implementations of DSA and ECDSA can be created where k is chosen in order to subliminally leak information via signatures. For example, an offline private key could be leaked from a perfect offline device that only released innocent-looking signatures.

1. Explain in detail cloud monitoring and various monitoring tools.

Cloud monitoring is a method of reviewing, observing, and managing the operational workflow in a cloud-based IT infrastructure. Manual or automated management techniques confirm the availability and performance of websites, servers, applications, and other cloud infrastructure. This continuous evaluation of resource levels, server response times, and speed predicts possible vulnerability to future issues before they arise.

Cloud monitoring works through a set of tools that supervise the servers, resources, and applications running the applications. These tools generally come from two sources:

* In-house tools from the cloud provider — This is a simple option because the tools are part of the service. There is no installation, and integration is seamless.
* Tools from independent SaaS provider — Although the SaaS provider may be different from the cloud service provider, that doesn’t mean the two services don’t work seamlessly. These providers also have expertise in managing performance and costs.

Cloud monitoring tools look for problems that can prevent or restrict businesses from delivering service to their customers. Generally, these tools offer data on performance, security, and customer behaviour:

* Cybersecurity is a necessary part of keeping networks safe from cyber-attacks. IT teams can use it to detect breaches and vulnerabilities early and secure the network before the damage gets out of hand.
* By testing at regular intervals, organizations can detect errors quickly and rectify them in order to mitigate any damage to performance and functionality, which improves the customer experience and, as a result, can boost sales and enhance customer retention.
* Speed — like functionality and user experience — is a primary driver of customer satisfaction. Speed metrics can be monitored and generate data that helps organizations optimize websites and applications.

There are various cloud tools available in the market:

1. Amazon Cloudwatch

Amazon Web Services offers to monitor cloud resources and applications running on Amazon AWS. It lets you view and track metrics on Amazon EC2 instances and other AWS resources such as Amazon EBS volumes and Amazon RDS DB instances. You can also use it to set alarms, store log files, view graphs and statistics, and monitor or react to AWS resource changes. Amazon Cloudwatch gives you an insight into your system’s overall health and performance. You can use this information to optimize your application’s operations. The best part of this monitoring solution is you don’t need to install any additional software. It is an excellent practice to have multi-cloud management strategies. They give you cover in case of incidences such as when Amazon Web Services went dark in March 2017.

1. Microsoft Cloud Monitoring

If you run your applications on Microsoft Azure, you can consider Microsoft Cloud Monitoring to monitor your workload. MCM gives you immediate insights across your workloads by monitoring applications, analyzing log files, and identifying security threats. Its built-in cloud monitoring tools are easy to set up. They provide a full view of the utilization, performance, and health of your applications, infrastructure, and workloads. Similar to Amazon Cloudwatch, you don’t have to download any extra software as MCM is inbuilt into Azure.

1. AppDynamics

Cisco Systems acquired AppDynamics in early 2017. AppDynamics provides cloud-based network monitoring tools for assessing application performance and accelerating operations shift. You can use the system to maximize the control and visibility of cloud applications in crucial IaaS/PaaS platforms such as Microsoft Azure, Pivotal Cloud Foundry, and AWS. AppDynamics competes heavily with other application management solutions such as SolarWinds, Datadog, and New Relic. The software enables users to learn the real state of their cloud applications down to the business transaction and code level. It can effortlessly adapt to any software or infrastructure environment. The new acquisition by Cisco Systems will only magnify AppDynamic’s capabilities.

1. BMC TrueSight Pulse

BMC helps you boost your multi-cloud operations performance and cost management. It helps measure end-user experience, monitor infrastructure resources, and detect problems proactively. It gives you the chance to develop an all-around cloud operations management solution. With BMC, you can plan, run, and optimize multiple cloud platforms, including Azure and AWS, among others. BMC can enable you to track and manage cloud costs, eliminate waste by optimizing resource usage, and deploy the right resources at the right price. You can also use it to break down cloud costs and align cloud expenses with business needs.

1. DX Infrastructure Manager (IM)

DX Infrastructure Manager is a unified infrastructure management platform that delivers intelligent analytics to the task of infrastructure monitoring. DX IM provides a proactive method to troubleshooting issues that affect the performance of cloud infrastructure. The platform manages networks, servers, storage databases, and applications deployed using any configuration. DX IM makes use of intelligent analytics to map out trends and patterns which simplify troubleshooting and reporting activities. The platform is customizable, and enterprises can build personalized dashboards that enhance visualization. The monitoring tool comes equipped with numerous probes for monitoring every aspect of a cloud ecosystem. You can also choose to integrate DX IM into Incident Management Tools to enhance their infrastructure monitoring capabilities.

1. New Relic

New Relic aims at intelligently managing complex and ever-changing cloud applications and infrastructure. It can help you know precisely how your cloud applications and cloud servers are running in real-time. It can also give you useful insights into your stack, let you isolate and resolve issues quickly, and allow you to scale your operations with usage. The system’s algorithm takes into account many processes and optimization factors for all apps, whether mobile, web, or server-based. New Relic places all your data in one network monitoring dashboard so that you can get a clear picture of every part of your cloud. Some of the influential companies using New Relic include GitHub, Comcast, and EA. If you are interested in free and premium cloud monitoring options, check out our article on the 13 best New Relic alternatives.

1. Hyperic

vRealize Hyperic, a division of VMware, is a robust monitoring platform for a variety of systems. It monitors applications running in a physical, cloud, and virtual environments, as well as a host of operating systems, middleware, and networks. One can use it to get a comprehensive view of all their infrastructure, monitor performance, utilization, and tracklogs and modifications across all layers of the server virtualization stack. Hyperic collects performance data across more than 75 application technologies. That is as many as 50,000 metrics, with which you can watch any component in your app stack.

1. Solarwinds

Solarwinds provides cloud monitoring, network monitoring, and database management solutions within its platform for enterprises to take advantage of. Solarwinds cloud management platform monitors the performance and health status of applications, servers, storage, and virtual machines. The platform is a unified infrastructure management tool and has the capacity to monitor hybrid and multi-cloud environments. Solarwinds offers an interactive virtualization platform that simplifies the process of receiving insight from the thousands of metrics collected from an IT environment. The platform includes troubleshooting and remediation tools that enable real-time response to discovered issues.

1. ExoPrise

The ExoPrise SaaS monitoring service offers you comprehensive security and optimization services to keep your cloud apps up and running. The tool expressly deals with SaaS applications such as Dropbox, Office 365, Salesforce.com, and Box. It can assist you to watch and manage your entire Office 365 suite, while simultaneously troubleshooting, detecting outages, and fixing problems before they impact your business. ExoPrise also works to ensure SLA compliance for all your SaaS and Web applications. Some of the major clients depending on ExoPrise include Starbucks, PayPal, Unicef, and P&G.

1. Retrace

Retrace is a cloud management tool designed with developers’ use in mind. It gives developers more profound code-level application monitoring insights whenever necessary. It tracks app execution, system logs, app & server metrics, errors, and ensures developers are creating high-quality code at all times. Developers can also find anomalies in the codes they generate before the customers do. Retrace can make your developers more productive, and their lives less complicated. Plus, it has an affordable price range to fit small and medium businesses.

1. Aternity

Aternity is a top End User Experience (EUE) monitoring system that was acquired by Riverbed Technology in July 2016. Riverbed integrated the technology into its Riverbed SteelCentral package for a better and more comprehensive cloud ecosystem. SteelCentral now combines end-user experience, infrastructure management, and network assessments to give better visibility of the overall system’s health. Aternity is famous for its ability to screen millions of virtual, desktop, and mobile user endpoints. It offers a more comprehensive approach to EUE optimization by the use of synthetic tests. Synthetic tests allow the company to find crucial information on the end user’s experience by imitating users from different locations. It determines page load time and delays, solves network traffic problems, and optimizes user interaction. Aternity’s capabilities offer an extensive list of tools to enhance the end user’s experience in every way possible.

1. Redgate

If you use Microsoft Azure, SQL Server, or.NET, then Redgate could be the perfect monitoring solution for your business. Redgate is ingenious, simple software that specializes in these three areas. It helps teams in managing SQL Server environments to be more proactive by providing real-time alerts. It also allows you to unearth defective database deployments, diagnose root problem causes fast, and gain reports about the server’s overall well-being. Redgate also allows you to track the load on your cloud system down to the database level, and its SQL monitor gives you all the answers about how your apps are delivering. Redgate is an exceptional choice for your various Microsoft server stacks. It is a top choice for over 90% of the Fortune 100 companies.

1. Datadog

Datadog started as an infrastructure monitoring service but later expanded into application performance monitoring to rival other APM providers like New Relic and AppDynamics. This service swiftly integrates with hundreds of cloud applications and software platforms. It gives you full visibility of your modern apps to observe, troubleshoot, and optimize their speed or functionality. Datadog also allows you to analyze and explore logs, build real-time interactive dashboards, share findings with teams, and receive alerts on critical issues. The platform is simple to use and provides spectacular visualizations. Datadog has a set of distinct APM tools for end-user experience test and analysis. Some of its principal customers include Sony, Samsung, and eBay.

1. Opsview

Opsview helps you track all your public and private clouds together with the workloads within them under one roof. It provides a unified insight to analyze, alert, and visualize occurrences and engagement metrics. It also offers comprehensive coverage, intelligent notifications, and aids with SLA reporting. Opsview features highly customizable dashboards and advanced metrics collection tools. If you are looking for a scalable and consistent monitoring answer for now and the future, Opsview may be a perfect solution for you.

1. Logic Monitor

Logic Cloud Monitor was named the Best Network Monitoring Tool by PC magazine for two years in a row (2016 & 2017). This system provides pre-configured and customizable screening solutions for apps, networks, large and small business servers, cloud, virtual machines, databases, and websites. It automatically discovers, integrates, and watches all components of your network infrastructure. Logic is also compatible with a vast range of technologies, which gives it coverage for complex networks with resources within the premises or spread across multiple data centers. The system gives you access to infinite dashboards to visualize system execution data in ways that inform and empower your business.

1. PagerDuty

PagerDuty gives users comprehensive insights on every dimension of their customer experience. It’s enterprise-level incident management and reporting tool to help you respond to issues fast. It connects seamlessly with various tracking systems, giving you access to advanced analytics and broader visibility. With PagerDuty, you can quickly assess and resolve issues when every second on your watch counts. PagerDuty is a prominent option for IT teams and DevOps looking for advanced analysis and automated incident resolution tools. The system can help reduce incidents in your cloud system, increasing the happiness of your workforce and overall business outcome.

1. Dynatrace

Dynatrace is a top app, infrastructure, and cloud monitoring service that focuses on solutions and pricing. Their system integrates with a majority of cloud service providers and micro-services. It gives you full insight into your user’s experience and business impact by screening and managing both cloud infrastructure and application functionality. AI powers Dynatrace.  It offers a fast installation process to allow users quick free tests. The system helps you optimize customer experience by analyzing user behavior, meeting user expectations, and increasing conversion rates. They have a 15-day trial period and offer simple, competitive pricing for companies of all sizes.

1. Sumo Logic

Sumo Logic provides SaaS security monitoring and log analytics for Azure, Google Cloud Platform, Amazon Web Services, and hybrid cloud services. It can give you real-time insights into your cloud applications and security. Sumo Logic monitors cloud and on-premise infrastructure stacks for operation metrics through advanced analytics. It also finds errors and issues warnings quickly actions can be taken. Sumo Logic can help IT, DevOps, and Security teams in business organizations of all sizes. It is an excellent solution for cloud log management and metrics tracking. It provides cloud computing management tools and techniques to help you eliminate silos and fine-tune your applications and infrastructure to work seamlessly.

1. Stack Driver

Stack Driver is a Google cloud service monitoring application that presents itself as intelligent monitoring software for AWS and Google Cloud. It offers assessment, logging, and diagnostics services for applications running on these platforms. It renders you detailed insights into the performance and health of your cloud-hosted applications so that you may find and fix issues quickly. Whether you are using AWS, Google Cloud Platforms, or a hybrid of both, Stack Driver will give you a wide variety of metrics, alerts, logs, traces, and data from all your cloud accounts. All this data will be presented in a single dashboard, giving you a rich visualization of your whole cloud ecosystem.

1. Unigma

Unigma is a management and monitoring tool that correlates metrics from multiple cloud vendors. You can view metrics from public clouds like Azure, AWS, and Google Cloud. It gives you detailed visibility of your infrastructure and workloads and recommends the best enforcement options to your customers. It has appealing and simple-to-use dashboards that you can share with your team or customers. Unigma is also a vital tool in helping troubleshoot and predict potential issues with instant alerts. It assists you to visualize cloud expenditure and provides cost-saving recommendations.

1. Zenoss

Zenoss monitors enterprise deployments across a vast range of cloud hosting platforms, including Azure and AWS. It has various cloud analysis and tracking capabilities to help you check and manage your cloud resources well. It uses the ZenPacks tracking service to obtain metrics for units such as instances. The system then uses these metrics to ensure uptime on cloud platforms and the overall health of their vital apps. Zenoss also offers ZenPacks for organizations deploying private or hybrid cloud platforms. These platforms include OpenStack, VMware vCloud Director, and Apache CloudStack.

1. Netdata.cloud

Netdata.cloud is a distributed systems health monitoring and performance troubleshooting platform for cloud ecosystems. The platform provides real-time insights into enterprise systems and applications. Netdata.cloud monitors slowdowns and vulnerabilities within IT infrastructure. The monitoring features it uses include auto-detection, event monitoring, and machine learning to provide real-time monitoring. Netdata is open-source software that runs across physical systems, virtual machines, applications, and IoT devices. You can view key performance indexes and metrics through its interactive visualization dashboard. Insightful health alarms powered by its Advanced Alarm Notification System makes pinpointing vulnerabilities and infrastructure issues a streamlined process.

1. Sematext Cloud

Sematext is a troubleshooting platform that monitors cloud infrastructure with log metrics and real-time monitoring dashboards. Sematext provides a unified view of applications, log events, and metrics produced by complex cloud infrastructure. Smart alert notifications simplify discovery and performance troubleshooting activities. Sematext spots trends and patterns while monitoring cloud infrastructure. Noted trends and models serve as diagnostic tools during real-time health monitoring and troubleshooting tasks. Enterprises get real-time dynamic views of app components and interactions. Sematext also provides code-level visibility for detecting code errors and query issues, which makes it an excellent DevOps tool. Sematext Cloud provides out-of-the-box alerts and the option to customize your alerts and dashboards.

1. Site 24×7

As the name suggests, Site 24×7 is a cloud monitoring tool that offers round-the-clock services for monitoring cloud infrastructure. It provides a unified platform for monitoring hybrid cloud infrastructure and complex IT setups through an interactive dashboard. Site 24×7 offers cloud monitoring support for Amazon Web Services (AWS), GCP, and Azure. The monitoring tool integrates the use of IT automation for real-time troubleshooting and reporting. Site 24×7 monitors usage and performance metrics for virtual machine workloads. Enterprises can check the status of Docker containers and the health status of EC2 servers. The platform monitors system usage and health of various Azure services. It supports the design and deployment of third-party plugins that handle specific monitoring tasks.

1. CloudMonix

CloudMonix provides monitoring and troubleshooting services for both cloud and on-premise infrastructure. The unified infrastructure monitoring tool keeps a tab on IT infrastructure performance, availability, and health. CloudMonix automates the processes of recovery, which delivers self-healing actions and troubleshoots infrastructural deficiencies. The unified platform offers enterprises a live dashboard that simplifies the visualization of critical metrics produced by cloud systems and resources. The dashboard includes predefined templates of reports such as performance, status, alerts, and root cause reports. The interactive dashboard provides deep insight into the stability of complex systems and enables real-time troubleshooting.

1. Bitnami Stacksmith

Bitnami offers different cloud tools for monitoring cloud infrastructure services from AWS, Microsoft Azure to Google Cloud Platform. Bitnami services help cluster administrators and operators manage applications on Kubernetes, virtual machines, and Docker. The monitoring tool simplifies the management of multi-cloud, cross-platform ecosystems. Bitnami accomplishes this by providing platform-optimized applications and infrastructure stack for each platform within a cloud environment. Bitnami is easy to install and provides an interactive interface that simplifies its use. Bitnami Stacksmith features helps in installing many slacks on a single server with ease.

1. Zabbix

Zabbix is an enterprise-grade software built for real-time monitoring. The monitoring tool is capable of monitoring thousands of servers, virtual machines, network or IoT devices, and other resources. Zabbix is open source and employs diverse metric collection methods when monitoring IT infrastructure. Techniques such as agentless monitoring, calculation and aggregation, and end-user web monitoring make it a comprehensive tool to use. Zabbix automates the process of troubleshooting while providing root cause analysis to pinpoint vulnerabilities. A single pane of glass offers a streamlined visualization window and insight into IT environments. Zabbix also integrates the use of automated notification alerts and remediation systems to troubleshoot issues or escalate them in real-time.

1. Cloudify

Cloudify is an end-to-end cloud infrastructure monitoring tool with the ability to manage hybrid environments. The monitoring tool supports IoT device monitoring, edge network monitoring, and troubleshooting vulnerabilities. Cloudify is an open-source monitoring tool that enables DevOps teams and IT managers to develop monitoring plugins for use in the cloud and on bare metal servers. Cloudify monitors on-premise IT infrastructure and hybrid ecosystems. The tool makes use of Topology and Orchestration Specification for Cloud Applications (TOSCA) to handle its cloud monitoring and management activities. The TOSCA approach centralizes governance and control through network orchestration, which simplifies the monitoring of applications within IT environments.

1. Manage IQ

Manage IQ is a cloud infrastructure monitoring tool that excels in discovering, optimizing, and controlling hybrid or multi-cloud IT environments. The monitoring tool enables continuous discovery as it provides round-the-clock advanced monitoring capabilities across virtualization containers, applications, storage, and network systems. Manage IQ brings compliance to monitoring IT infrastructure. The platform ensures all virtual machines, containers, and storage keep to compliance policies through continuous discovery. Manage IQ captures metrics from virtual machines to discover trends and patterns relating to system performance. The monitoring tool is open-source and provides developers with the opportunity to enhance application monitoring.

1. Prometheus

Prometheus is an open-source platform that offers enterprises with event monitoring and notification tools for cloud infrastructure. Prometheus records real-time metrics through graph queries, which aren’t similar to a virtualized dashboard. The tool must be hooked up to Grafana to generate full-fledged dashboards. Prometheus provides its query language (PrmQL), which allows DevOps organizations to manage collected data from IT environments.

**MCQ QUESTION BANK**

Amazon S3 is which type of storage service?

Object

Block

Simple

Secure

Which of the following AWS tool is used for big data processing and analysis.?

S3

EC2

3. Elastic MapReduce

4.Snowball

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_enables the user to automatically distribute and balance the incoming application’s traffic

Elastic load balancing (ELB)

Amazon S3

Amazon SQS

CloudFront

4. Which of the following provides feature of static website hosting, which is ideal for websites with static content

Amazon S3

Amazon EC2

Amazon SQS

Snowbell

5. Which of the following Windows Azure tool encapsulates all the information to be aware of before attempting the application migration to Windows Azure

Azure Cloud Services

B. Migration Assessment Tool (MAT)

C. Windows Azure Pricing Calculator

D. Windows Azure Pack

6. Which Google Cloud Platform service can be used for serverless file processing and running website backend?

1. Kubernetes Engine

2. App Engine

3. NFS

4. Compute Engine

7. When would developers use microservices?

A. When they want to write cell phone applications that run quickly

B. When they work with ephemeral nano technology

C. When they need to create large, enterprise-level applications that are subject to changes on a frequent basis

D. When they create applications specifically for scientific test equipment

8. Which of the following microservices architectural pattern defines how clients access the services in a microservice architecture?

A. Decomposition patterns

B. API Gateway pattern

C. Service Discovery pattern

D. Observability pattern

9. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_are used to route requests for a client to an available service instance in a microservice architecture

A. Service Discovery pattern

B.API Gateway pattern

C. Database per Service pattern

D.UI pattern

10. Suppose your application is currently using a local PostgreSQL database for its operations and it is afterward replaced with the one hosted on the server of your company by just changing the URL and the database credentials.

Above is the example of which 12 factor app?

Dependencies

Backing Services

Codebase

Build, Release and Run

11. In APIfication process, which step defines digital resources and capabilities of the company?

Development

Design

Production

Discovery

12.Which of API type needs specific access rights to be able to use them and are typically exposed via an API developer portal.

A. partner API

B. Internal API

C. Open API

D. Closed API

13. Which of the following API style of development is a collection of interlinked resources, which is very much how web apps are delivered.

A. Tunnel

B. Query

C. Hypermedia

D. Event

14. Which of the following is part of Data Access layer in Spring framework?

A - Beans

B - Aspects

C - JMS

D - Context

15. Which of the following is not IaaS related security issue?

Multitenancy

Identity management and access control

Hypervisor security

Resource locality

16. Stream Ciphers encrypt pseudorandom sequences with bits of plaintext in order to generate ciphertext, usually with\_\_\_\_\_ operation.

OR

AND

XOR

NOR

17. Which of the following statement is not correct related to Cipher Block Chaining (CBC)?

A. CBC is a mode of operation for stream ciphers.

B. Initialization vector (IV) is used in CBC in the initial phase.

C. It has better resistive nature towards cryptanalysis than ECB

18. Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?

1.CBC (Cipher Block Chaining)

2.ECB (Electronic Code Book)

3.CFB (Cipher text Feed Back)

4.Counter (CTR) Mode

19. Consider the following steps,

Substitution bytes

Shift Rows

Mix columns

Add round key

The above steps are performed in each round of which of the following ciphers?

1.Rail fence cipher

2.Data Encryption Standard (DES)

3.Advance Encryption Standard (AES)

4.RSA

20. What is the output of a cryptographic hash function means?

1.A variable set of bits

2.A fixed set of bits, derived from one-way mathematical operations

3.An output which may be easily discovered by an adversary

4.Outputs of such functions are of no importance

21. Which of the following is strongest encryption technique?

1.DES ( Data Encryption Standard)

2.Double DES

3.Triple DES

4.AES (Advance Encryption Standard)

22.

|  |  |
| --- | --- |
| Which of the following is false for ECB mode of operation?  i) The Plain text is broken into blocks of size 128 bytes  ii) Blocks can be swapped, repeated, replaced without recipient noticing  iii) Good for short data  iv) Encryption of each block is done separately using a randomly generated key for each block |  |
|  |  |
|  |  |

Only i

ii) and iii)

i) and iv)

i) ii) and iv)

23. Which of the following statements are true ?

i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption

ii) The CTR mode does not require an Initialization Vector

iii) The last block in the CBC mode uses an Initialization Vector

iv) In CBC mode repetitions in plaintext do not show up in ciphertext

|  |  |
| --- | --- |
| iii |  |
| b. | ii) and iv) |
| c. | All the Statements are true |
| d. | i) ii) and iv) |

24. Which of the following can be classified under advantages and disadvantages of OFB mode?

i) Transmission errors

ii) A bit error in a ciphertext segment

iii) Cannot recover from lost ciphertext segments

iv) Ciphertext or segment loss

|  |  |
| --- | --- |
| a. | Advantages: None; Disadvantages: All |
| b. | Advantages: All; Disadvantages: None |
| c. | Advantages: i); Disadvantages: ii) iii) iv) |
| d. | Advantages: i); ii) Disadvantages: iii) iv) |