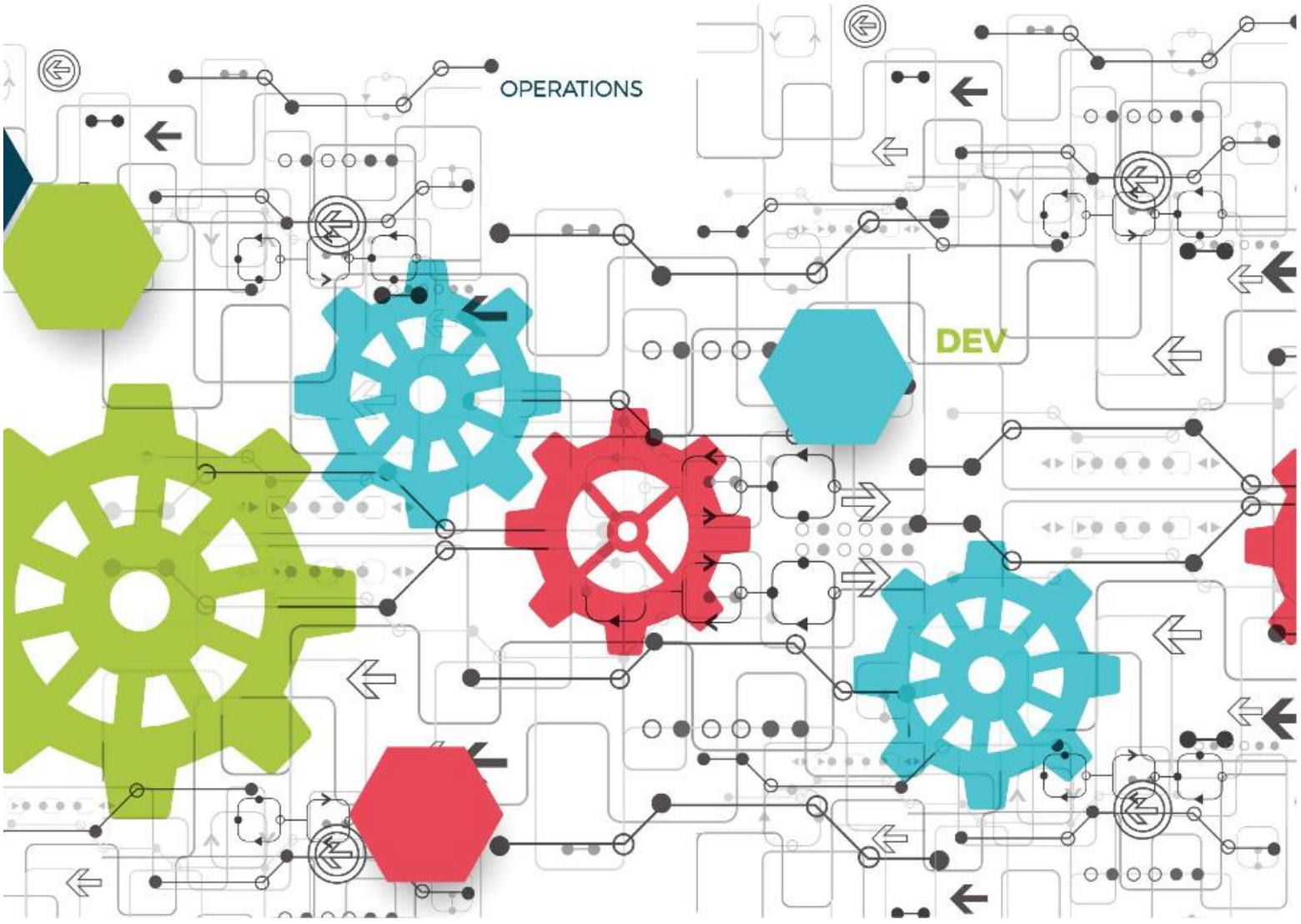
Xebia

B.Tech Computer Science and Engineering in DevOps

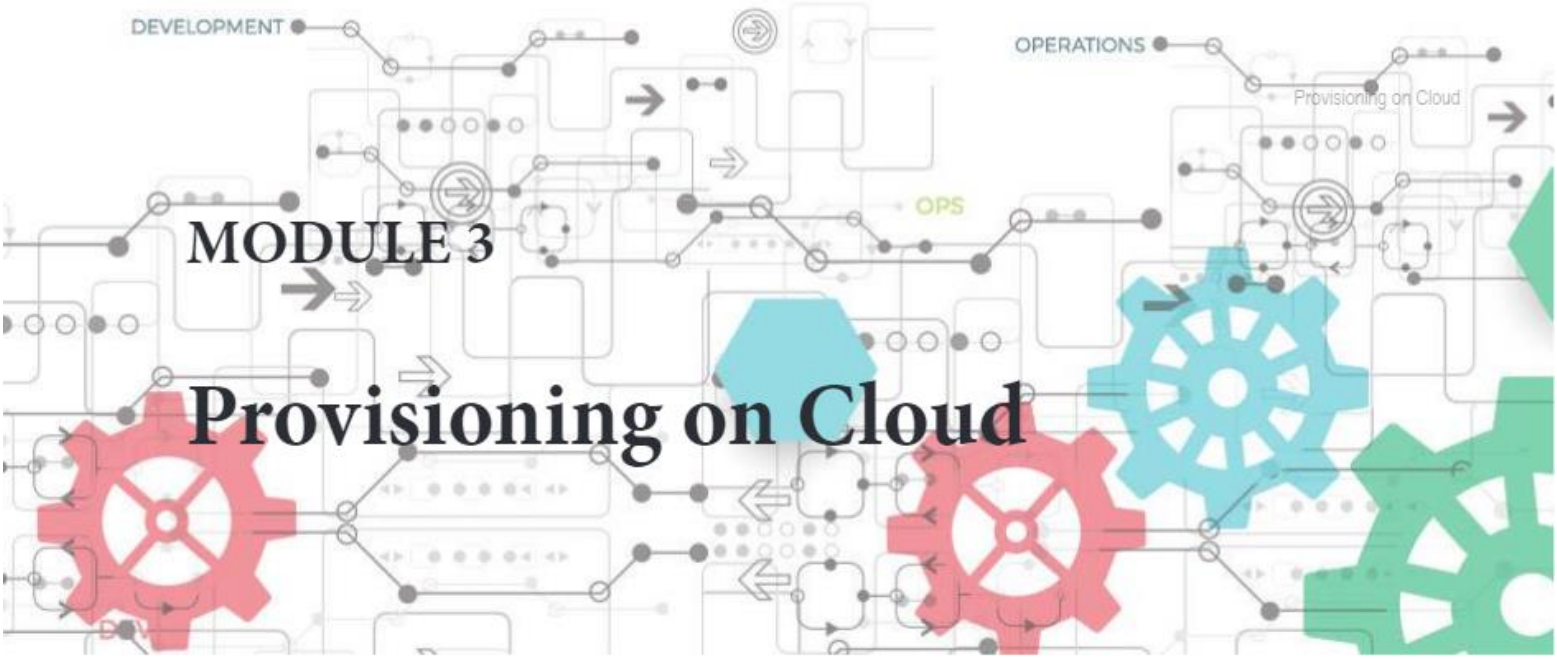
System Provisioning and Configuration Management

MODULE 3

Provisioning on Cloud



Contents



MODULE 3

Provisioning on Cloud

You will learn about 'Provisioning on Cloud' in this module.

Module Objectives

At the end of this module, you will be able to:

- Explain provisioning on cloud
- Identify the types of cloud provisioning
- Describe life-cycle of provisioning on cloud
- Discuss about on premise to cloud migration strategies
- Explain network security enablement from on-premises to cloud
- Describe microservices management in cloud

Module Topics

Let us take a quick look at the topics that we will cover in this module:

- What is Provisioning on Cloud
- Types of Cloud Provisioning
- Life-Cycle of Provisioning on Cloud
- On Premise to Cloud Migration Strategies
- Network Security Enablement from On-Premises to Cloud
- Microservices Management in Cloud

3.1 What is Provisioning on Cloud ?

Basic Definition:

Provisioning on a cloud or cloud computing is the use of a network of remote servers hosted on the Internet to store, manage and process data rather than having all the data stored on a local server.

In simple layman's term Cloud Computing means storing our date in the Internet from anywhere and accessing the date over the Internet from anywhere.

3.1.1 Cloud Providers

Some of the most popular service providers are as follows:

1. Microsoft Azure
2. Amazon Web Services
3. Google Cloud Platform
4. IBM Cloud
5. RackSpace
6. GoDaddy
7. Verizon Cloud
8. VMware
9. Oracle Cloud
10. RedHat

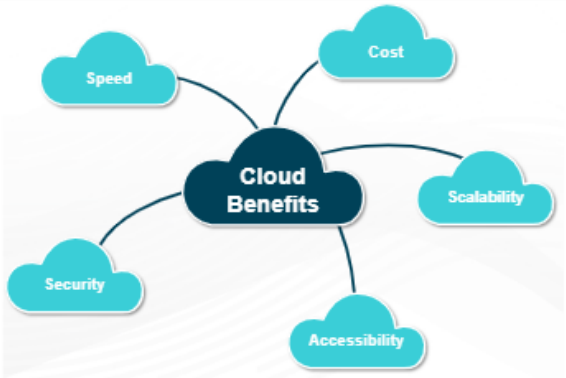
Companies who give us these (Cloud Computing) services are called Cloud Providers. They can do a vast array of activities like they have the ability to manage applications and servers through a Global Network also termed as web management or configuration portal.

Examples – Amazon Web Service and Microsoft Azure

3.1.2 Benefits of Cloud Computing

The benefits of cloud computing are as follows:

1. Speed
2. Cost
3. Scalability
4. Accessibility
5. Security



Speed: A service now on the cloud is available immediately and also ready for production. Resources go live on the same date and hits the market instantaneously. So this leads to revenue generation quite early. And this is not the case with legacy servers. So the speed at which this works is really a huge benefit.

Cost: Planning and buying the licensed hardware and supporting software has always been a challenge in legacy environments and unless we are careful we might have to live with a hardware which can be undersized and once we get to know the quantum of the same, it will again incur cost to update or change it. Cloud computing eliminates this issue. So what happens is we use a hardware and we pay for the amount of time to be used. In case we need to upgrade to a better hardware, then we upgrade the same with a better configuration and we pay for the time which we use it for. So this is quite cost effective.

Scalability: In legacy environments forecasting demand is a full time job, but with cloud we can let the monitoring and automation tool to work for us and rapidly scale up and down the resources based on the need of the hour.

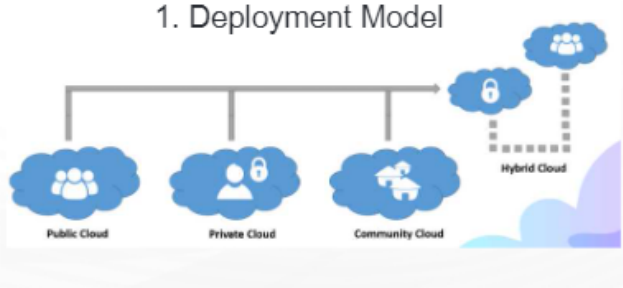
Accessibility: Resources, services, data can be accessed from anywhere as long as we are connected to the Internet. There are tools and techniques now available which will let us work offline as well. And it will sync when the Internet is available.

Better Security: Storing date in a secured fashion is the talk of the business. The data stored in the cloud is encrypted and hard to crack. It is much secure than the data stored at a local server level.

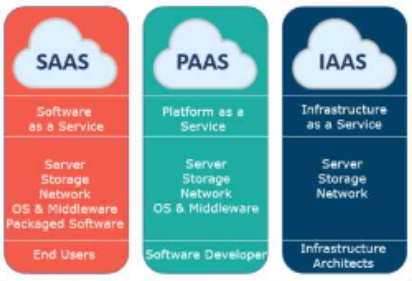
3.2 Types of Cloud Computing

Cloud computing is basically categorized into:

1. Deployment Model



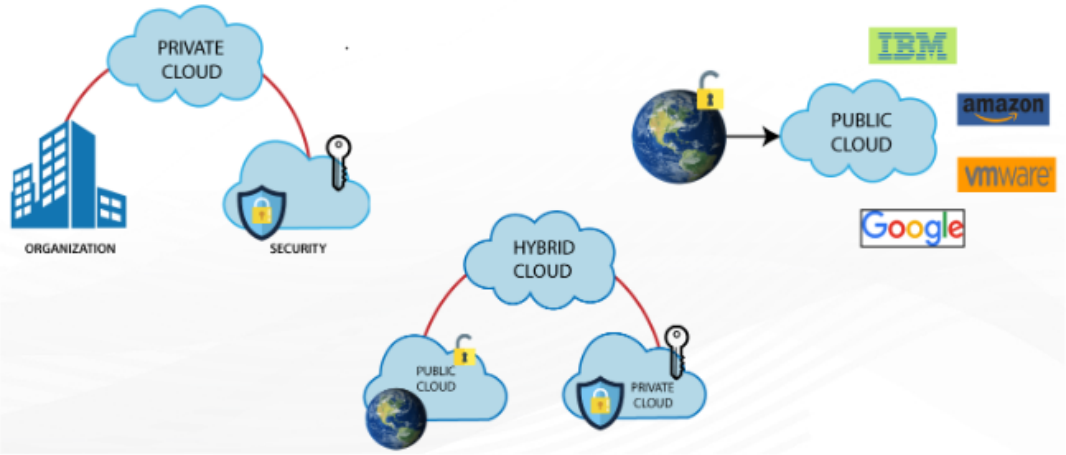
2. Services Model



Cloud computing is basically categorized into deployment model and services model which are further subdivided and we will learn about them in the upcoming slides.

3.2.1 Types of Deployment Model

Deployment model is further categorized into:



Public Cloud: Everything is stored and accessed via the Internet and any Internet user with proper permissions can be given access to some of the resources. In a public cloud there is no ownership of anything. Be it the hardware or the Software. Everything is managed by the Cloud Provider. Example: Microsoft Azure.

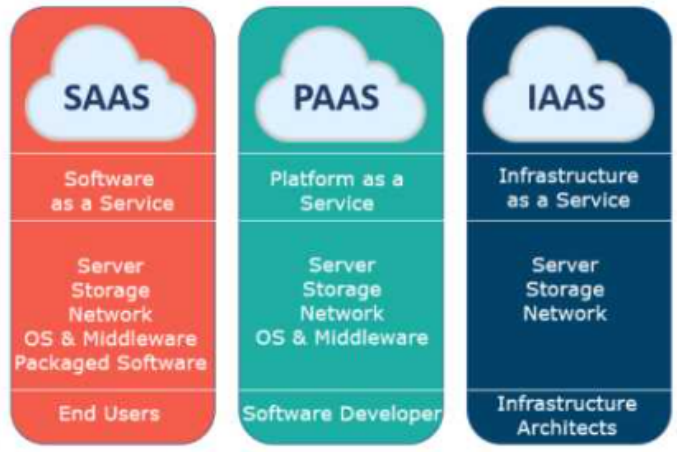
Private Cloud: The infrastructure is exclusively for a single organization. The organization can choose to run the cloud locally or outsource it to a public cloud provider. But when this is done, the infrastructure will be maintained on a private network. Example: VMWare and AWS.

Hybrid Cloud: They have taken things to a whole new level. Here you get the benefit of both public and private cloud. Organizations can choose to customize to keep some locally and rest outsource it.

3.2.2 Types of Service Model

Service model is further categorized into:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (Saas)



Infrastructure as a Service (IaaS): Here we rent an IT infrastructure (servers and networks) and pay on an hourly basis or whatever as per the agreement. We will have access to the resources we provision. For some provisioning you might have even root level access.

Example: AWS Elastic Compute Cloud (EC2)

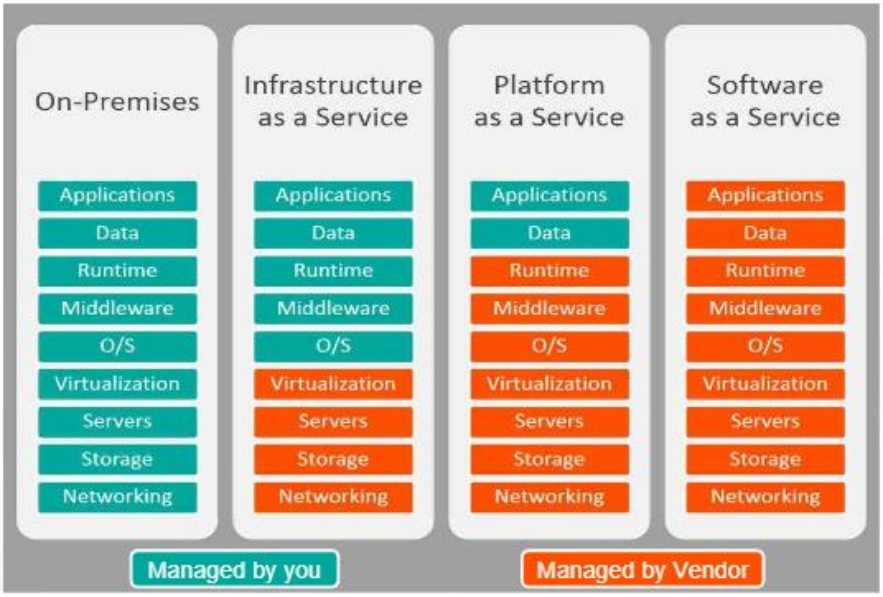
Platform as a Service (PaaS): The providers will give a pre-built platform where we can deploy our code and application and they will be up and running. We only need to manage the code and not the infrastructure.

Example: AWS Elastic BeanStalk

Software as a Service (SaaS): Cloud providers sell the end product which is a software or an application and we directly buy the software on a subscription basis. It's not the infrastructure or the platform, but the end-product. We pay for the hours we use this software. And here client has full control of the software environment and does not maintain any equipment.

Example: Amazon Web Services

3.3 Difference Between IaaS, PaaS and SaaS



The image shows what is managed by the end user and what is managed by the vendor or the service provider. In traditional On Premises format, almost everything is managed by the end user and in the SaaS model, almost everything is managed by the Service Provider.

3.4 Life Cycle of Provisioning on Cloud

Now we will learn about life cycle of provisioning on cloud.

1. Purpose
2. Hardware
3. Storage
4. Network
5. Security
6. Management processes and tools
7. Test the process
8. Pick the analytics

1. **Define the Purpose:** Understand the requirements of the business and determin/e what type of applications to run on the cloud.
2. **Define the Hardware:** Choosing a compute service that will provide the right support where we can resize the compute capacity in the cloud to run application programs.
3. **Define the Storage:** Choose a storage which will be useful to backup and archive data over the Internet.
4. **Define the Network:** Define a network that securely delivers data, videos, applications, etc. They should have low latency and high transfer speed.
5. **Define the Security:** Set up security service which enables services for user authentication or limiting access to a certain set of users on AWS resources.
6. **Define Management Processes and Tools:** Have complete control on the cloud environment by defining management tools, which monitor AWS resources and the customer applications running on AWS platforms.
7. **Testing the Process:** Verify the process using AWS Developer tools where we can build, test and deploy code quickly.
8. **Pick the Analytics:** Analyze and visualize data by using analytics server where we can start querying data instantly and get results.

3.5 Automated Provisioning on Cloud

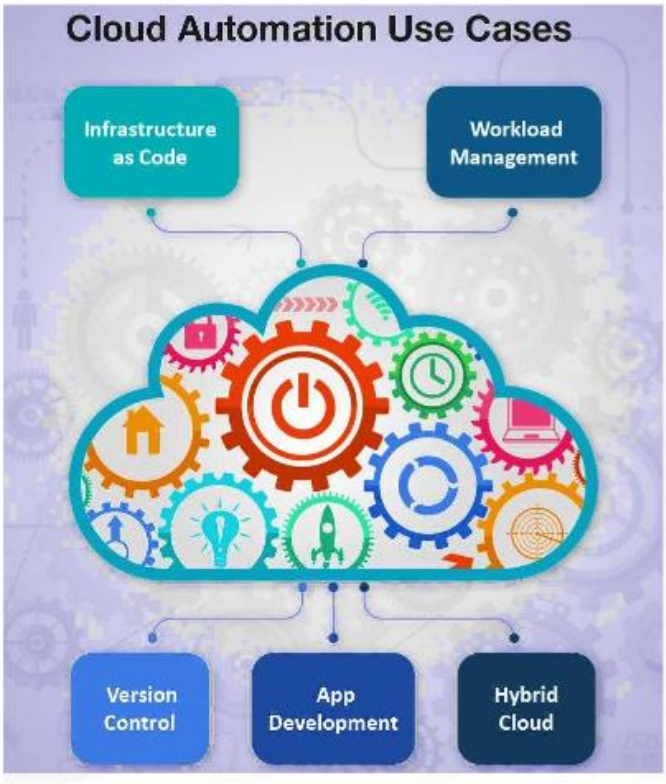
Topics to be covered in this section:

1. What is Cloud Automation?
2. Benefits of Cloud Automation
3. Cloud Automation Usage
4. Understanding Quality Gates like Sonarqube, Code Scanner

Automating provisioning on cloud is not as simple as it sounds. It is a complex process. It involves a lot of dynamism to keep up to the demand in an ever evolving market. We will learn about the same in the upcoming slides.

 |

3.6 What is Cloud Automation?



Automation as the word suggests — it enables the IT people (teams, developers, architects) to create, modify, manipulate the resources available in the cloud server automatically. Cloud automation is not a build in tool or process that aids whenever required. Rather, it requires high levels of skill and expertise to set the configuration right. It has its own level of challenges.

You need specialized tools. Need to get in touch with your service provider and seek the offerings and capabilities which are in service. And if you are using your own private cloud platform, then implement the same in your private platform. In case you are using a third party or public platform, then again, you need to get in sync with your service provider and can do the automation in the public cloud environments suiting your needs.

3.6.1 Benefits of Cloud Automation

The benefits of cloud automation are as follows:

1. Reducing Manual Work
2. Better Security
3. Better Backup Process
4. Better Control

Let's learn more about the benefits of cloud automation.

- **Reducing Manual Work:** The initial setup and configuration and synchronization is the challenge which needs to overcome. Teams need to understand how to use a definitive

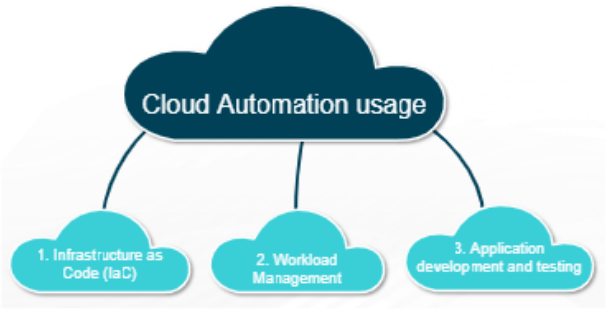
Integrated Development Environment to work in tandem with the cloud server. Once this setup is complete and successful, then life becomes much easier. It reduces a lot of manual effort and intervention.

- **Better Security:** Local server need configuration set up from local IT Teams. The security aspect of things for every organization to cover becomes a challenge with respect to expertise, skills, safety and security from latest Black Hat hacking operations. Data Encryption at a local server level within an organization is always debatable when it comes to breaking it. But the data stored in cloud.
- **Better BackUp Process:** Quick backup is much essential in organizations. And this is basically required to guard the system against Accidental Erase, certain configuration mistakes, hardware failure, power outage or even a cyber hack attack. Cloud does help in backing up data much faster, efficient and secured way.
- **Better Control: A** local Server setup might have less proximity of visible vicinity for IT and other system administrators. Cloud automation helps set up all resources in a governed manner which makes the governance much easier. It helps in controlling the infrastructure better.

3.6.2 Cloud Automation Usage

Let's discuss cloud automation usage.

1. Infrastructure as Code (IaC)
2. Workload Management
3. Application development and testing



There is a lot of configuration setup in IaC. So the infrastructure needs to be defined as per the configuration files. These configuration files need to be handled well in a proper version control tool like Git, with regular updates and have a good maintenance life cycle. They should be thoroughly tested. What cloud automation does is — it makes the IaC more orchestrated as it gives, as it liberates the private and public cloud models to have more control over the infrastructure.

In legacy environments forecasting demand is a full time job, but with cloud we can let the monitoring and automation tool to work for us and rapidly scale up and down the resources based on the need of the hour. Cloud automation helps in autoscaling. It is provided by any cloud provider. Sometimes to curb down costs, tracking and vigil of unused or extra resources can be handled by clearing. So Cloud computing helps in optimizing all these workload management by its auto scaling feature.

CI/CD is used in almost all organizations which practice DevOps or Agile methodologies. Cloud automation is the pioneer in serving the CI/CD processes. Connecting your source code with Git or SVN and pushing it to GitHb or BitBucket and managing code over there. Is all a handy thing over CI/CD.

3.7 What is Sonarqube?

Following are the key details about sonarqube:

- Helps to write cleaner code
- Helps in continuous code inspection
- Improves code reliability
- Increases application security

Following are the key details about sonarqube:

- It is a software testing tool which is used to improve the quality of the code and helps fix errors very early in the development
- It is a static analysis code. It goes through developers code and identifies errors
- It manages source code quality and consistency. It is an open source platform for continuous inspection of code quality
- It provides reports for various code quality issues for example code duplication. Also gives an analysis of Test Result
- Also gives information about code coverage
- Also gives information related to code complexity — whether it is simplified way or complex
- Describes design or architecture in simple or complex way
- Provides reports on Historical execution

3.7.1 Code Quality Checks Performed by Sonarqube

Some of the code quality checks performed by Sonarqube are as follows:

- Potential bugs
- Code defects to design inefficiencies
- Code duplication
- Lack of test coverage
- Excess complexity

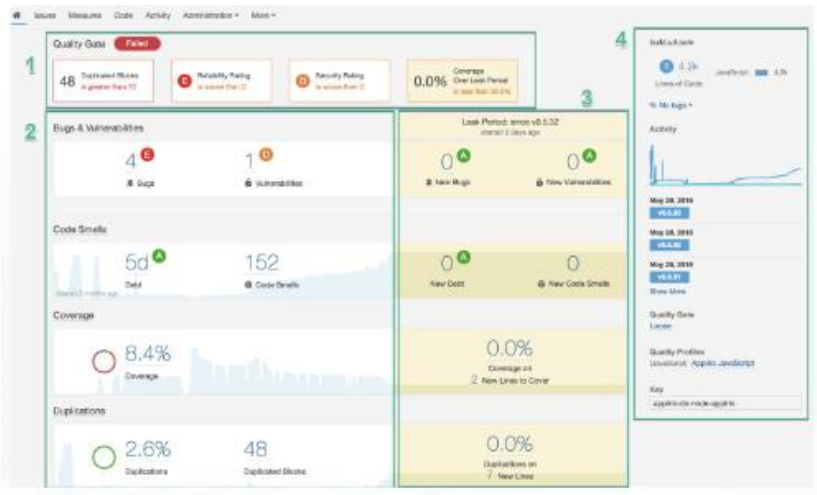
Some of the code quality checks performed by Sonarqube are as follows:

- Potential bugs
- Code defects to design inefficiencies
- Code duplication
- Lack of test coverage
- Excess complexity

3.7.2 Features of Sonarqube

Features of sonarqube are as follows:

- Can work with 25 different languages
- Can identify tricky issues
- Enhanced workflow
- Built in methodology



Some of the most important features of Sonarqube are as follows:

- **Can work with 25 different languages** — Java, DotNet, Cobol, Php, C++ to name a few.
- **Can identify tricky issues.** Some of which are as follows:
  - Detect bugs
  - Code smells
  - Security vulnerability

- Activate rules needed
- Execution path

- **Enhanced workflow:** Ensures better CI/CD, automated code analysis, get access through webhooks and API, integrate GitHub, and analyze breaches and decorate pull requests.
- **Built in methodology:** Discover memory leaks, good visualizer, enforce a quality gate, digs into issues, and plugins for IDEs.

3.8 Code Scanner

Following are the key details about code scanner:

- Code Scanners have a rapid walkthrough over the code
- Code Scanners can find errors which can lead to security bugs
- Code Scanners help in identifying common problem patterns
- Code Scanners alert developers with the above problems
- Code Scanners also provide suggestions to developers with the problems

Static code analysis tool for salesforce code to help improve the quality of the code. It does this by taking apex visualforce, lightning or a code and looks for patterns in it by identifying bugs, style and security issues, security vulnerabilities, quality issues and puts it into the tool. And it also helps you to build more rules.

3.8.1 Application of Code Scanner

Let's learn about application of code scanner.

- Reduces code complexity
- Aligns code with design
- Addresses security gaps

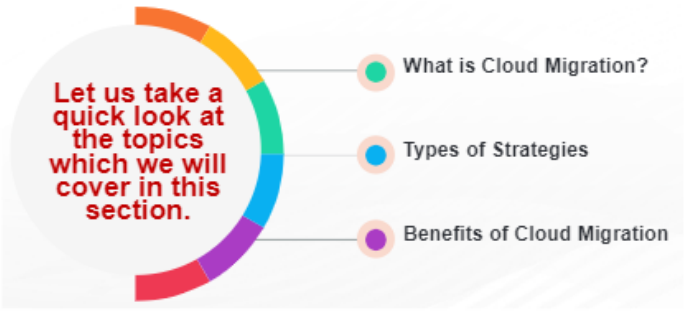
Let's learn about application of code scanner.

- Code Scanner helps you to apply best practices to your development workflow.
- Code Scanner helps your compliance with coding guidelines.
- Code Scanner helps you get various metrics and code replication checks.
- Code Scanner helps reduce bugs, security vulnerabilities, technical debt complexity going into production.

3.8.2 Organizational Improvement Using Code Scanner

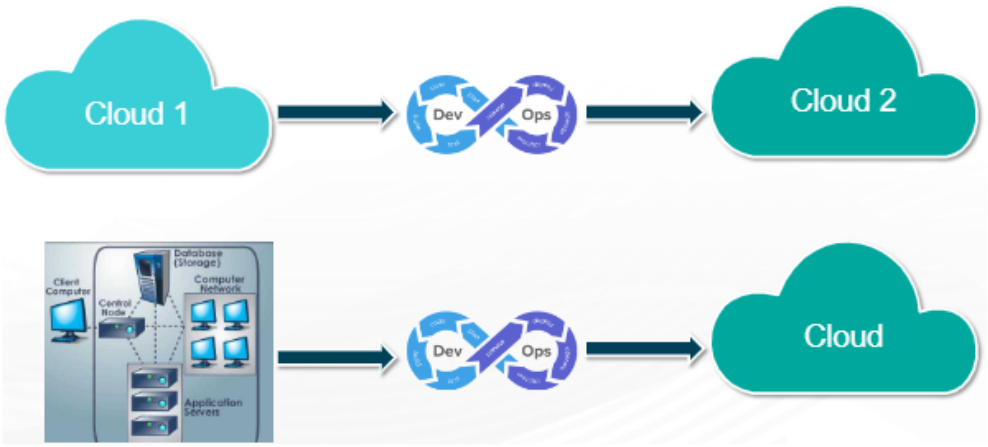
CodeScanner helps improve efficiency of your team. It helps to increase maintainability of your organization. Developers trying to maintain the code can get started quicker. CodeScanner helps to reduce total cost of ownership of your organization.

3.9 On Premise to Cloud Migration Strategies



Migration (go back into the history of human civilization) has always been a complex and politically debatable process. Similarly, cloud migration is also quite a complex process. So we will understand about this complex process in the upcoming slides.

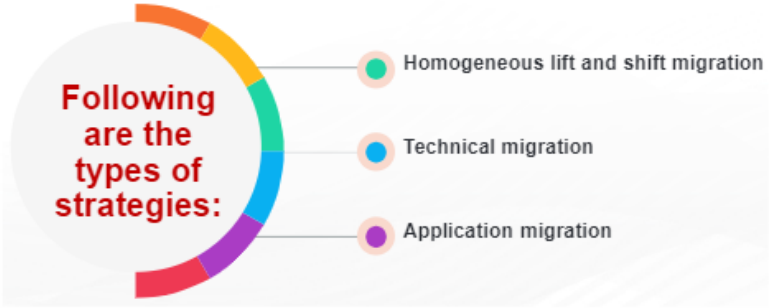
3.10 What is Cloud Migration?



Cloud computing is the process of transferring databases, applications, IT Processes from a Provisioned Data Store into a Cloud Cloud computing is also the process of transferring databases, applications, IT Processes from one Cloud into another Cloud

Suppose there is a company which was working on Premise Level Provisioning. Now, after realizing the current trend and also understanding the benefits of migrating to cloud and its services, they might move some or all of its data center into a cloud based infrastructure. It could be AWS or Azure or anything the company deems fit for its needs and requirements. This whole process is called Cloud Migration.

3.10.1 Types of Cloud Migration Strategies



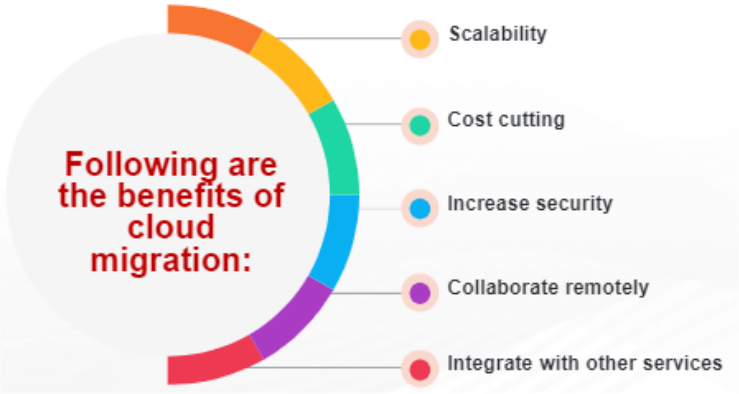
- **Homogeneous lift and shift migration:** This is almost like Copy Paste work. In simple terms an application will have its current hosting environment. What you do is lift the entire application from its current hosting environment and put it in the cloud environment exactly as it is. Generally, the three layers — Application, Database and OS get an exact copy from the current provisioned environment into the cloud. It is also referred as re-hosting, as it does not involve making extensive changes. This is cost effective, minimal disruption and also is a quick ROI.
- **Technical migration:** There is a certain level of upgrade in the Database and OS layer to meet certain transition level goals. This type of migration is adopted to sync with cloud native features such as scalability, automation, etc. It gives an edge in performance to organizations. Also helps organizations to plan the next stage in their transformation.
- **Application migration:** Here the application layer is also transformed along with DB and OS. It is further divided into:

  a. New system implementation

  b. System conversion

  c. Landscape transformation

3.10.2 Benefits of Cloud Migration



Scalability means that you can easily upscale or downscale IT and other requirements as per business needs. Sometimes in traditional provisioning, the data centers are rarely used to their full potential but the maintainability of the same still incurs adequate costs. So Scalability helps to decide how much to use and when to use

Moving to Cloud reduces operational costs. This happens because you pay for whatever you use. You do not have to pay for just procuring something by default whether it is being used or not.

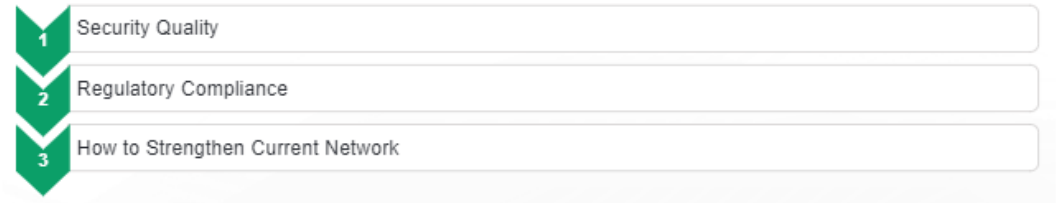
Cloud Service providers handle cloud operations of security issues via inbuilt security capabilities and auto updates.

Cloud computing allows organizations to collaborate with various tools, software, access to various database and other provisioning environments from anywhere. This makes it easier to work even from a remote location

Integration with other services becomes seamless when you work in Cloud. It is because of the integration features available in Cloud

3.11 Network Security Enablement from On-Premises to Cloud

Security pivotal points with respect to transitioning to cloud consist of the following:



Security Quality: This discussion of cloud is more secure or On Premise is more secure has a lot of varied opinion. But then in defense of the cloud, we can say it is more secure because the data isn't physically there in office for hackers or employees who have an ill intention to misuse for whatever reasons. So cloud can lessen the odds of a data breach.

On top of this cloud-based data isn't as susceptible to external reasons like robbers and acts of nature like fire, earthquake, etc., and get destroyed because data centers usually have advanced fire/temperature gauging systems, among other security features.

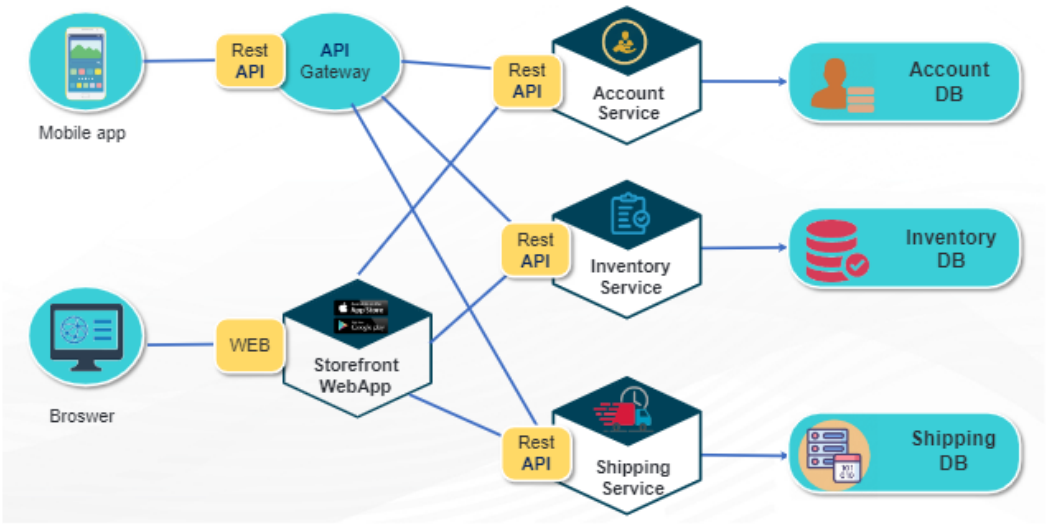
cloud systems learn our network and grows with us, over time it can become more secure than on-premise security.

Regulatory Compliance: Companies who opt for cloud based services must comply with data security regulations. But the cloud providers do their security provisioning with utmost due diligence and instances of data breach is 95% not possible unless some violation is done from the companies end. So educating company employees with Cloud Cyber Security best practices to follow and implement is highly important.

How to Strengthen Current Network:

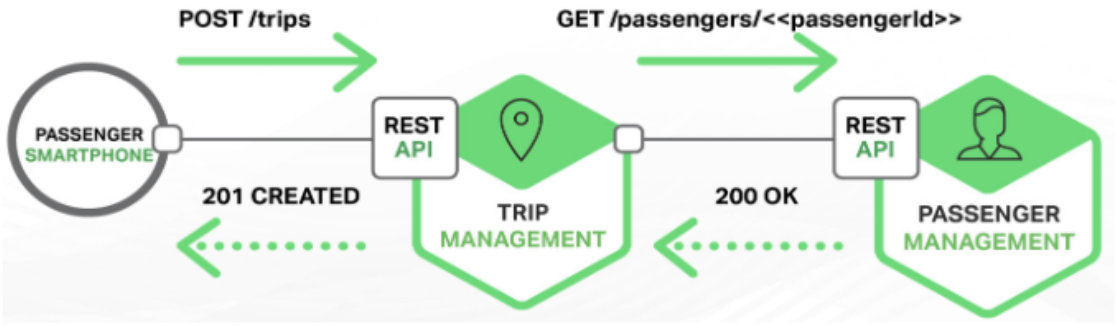
- Control Employee' Internet usage monitor the same
- A strict password policy is a must
- Cyber security awareness, education and implementation
- Go for a reputed and secure cloud service provider

3.12 What are Microservices?



Microservices are nothing but an architectural approach. This approach is to create a cloud based applications. Each application is built over a group of services. Each service has its own processes and they interact through APIs.

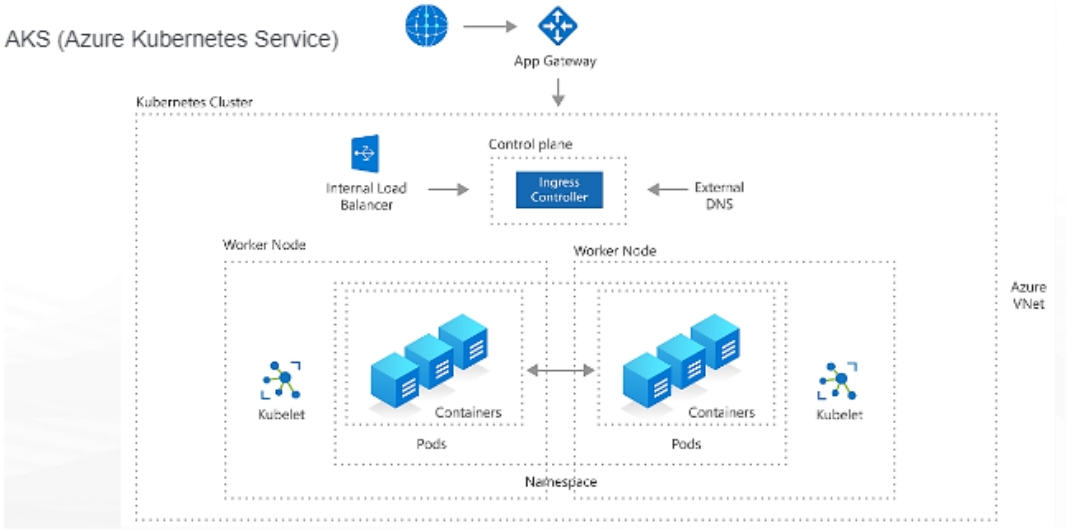
3.12.1 How Microservices Work?



MicroServices break down the service oriented architecture strategy. It breaks down the functional services into further granular form. And collecting all these granules forms the basic of operation of MicroServices.

- When multiple microservices are collected together, they combine to form larger macroservices. These large macroservices provide greater ability to quickly update the code of a single function/method. A microservice predominantly tries to attend or address even mitigate a single concern. For example, data search, login functionality, or a web service function.
- Microservices act as self healers. A lot of tools, one of which is Kubernetes also help Microservices to act as self healers. And human intervention is not necessary. It occurs behind the scene and is apparently transparent to the user as well.

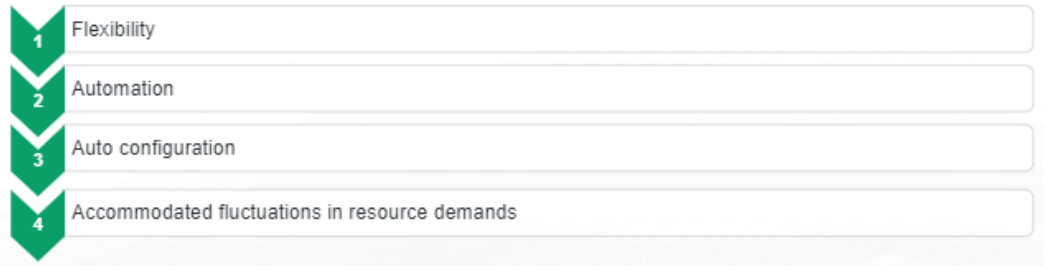
3.12.2 Azure Kubernetes Service (AKS)



Kubernetes System is an open source. Azure Kubernetes Service is based on this open system. It is a managed container orchestration service.

3.12.2.1 Benefits of AKS

Following are the benefits of AKS:

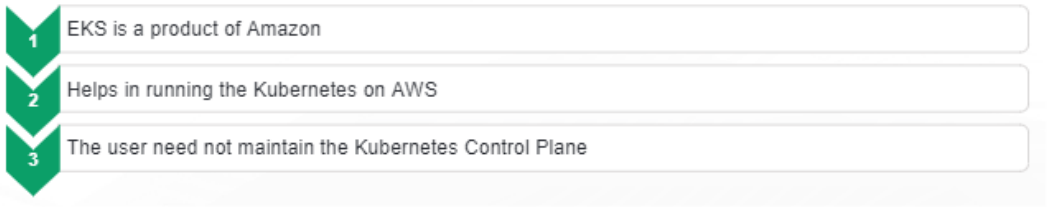


The benefits of AKS are as follows:

- Flexibility
- Automation
- Auto configuration
- Accommodates Fluctuations in resource demands

3.12.3 Elastic Kubernetes Service (EKS)

Following are the key details about EKS:

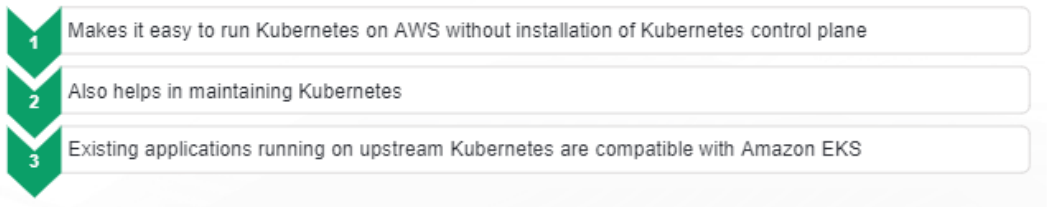


EKS is also a managed service. It makes Kubernetes easier to run on AWS. It is an open source system. Organizations can do deployment and management of containerized applications. For example PaaS (Platforms as a Service). There is an abstraction layer created on top of a host or a group of hosts. Development teams or developers can let Kubernetes manage a host of functions such as:

- Load balancing
- Monitoring and controlling resources consumption by team or application
- Limiting resource consumption
- Leveraging additional resources from new hosts added to a cluster

3.12.3.1 Benefits of EKS

Benefits of EKS are as follows:



Using EKS, complicated and cumbersome steps are done for us. For example, creation of Kubernetes master cluster. Configuring service discovery, Kubernetes primitives, and networking. Existing tools work better with EKS and does not involve too many modifications.

EKS can be integrated with various AWS services. Makes it easy for organizations to scale and secure applications. That too seamlessly.

There is AWS Fargate — it is a compute engine without a server for containers. If you use Fargate, then there's no need to provision and manage servers. Organizations can specify and pay for resources per application. Fargate has a feature of application isolation by design and it also improves security.

What did you Grasp?

1. What is a Kubernetes volume?
   - **A) The software within an OS that controls capacity allocation for nodes**
   - **B) A directory for the data accessible to containers in a pod**
   - **C) Layering software that puts apps into compartments for easier deployment**
   - **D) Code that enables two software programs to communicate**

In a nutshell

In this module, you have learned:

1. What is Provisioning on Cloud
2. Types of Cloud Provisioning
3. Life-Cycle of Provisioning on Cloud
4. On Premise to Cloud Migration Strategies
5. Network Security Enablement from On-Premises to Cloud
6. Microservices Management in Cloud

