Cloud-fundamentals

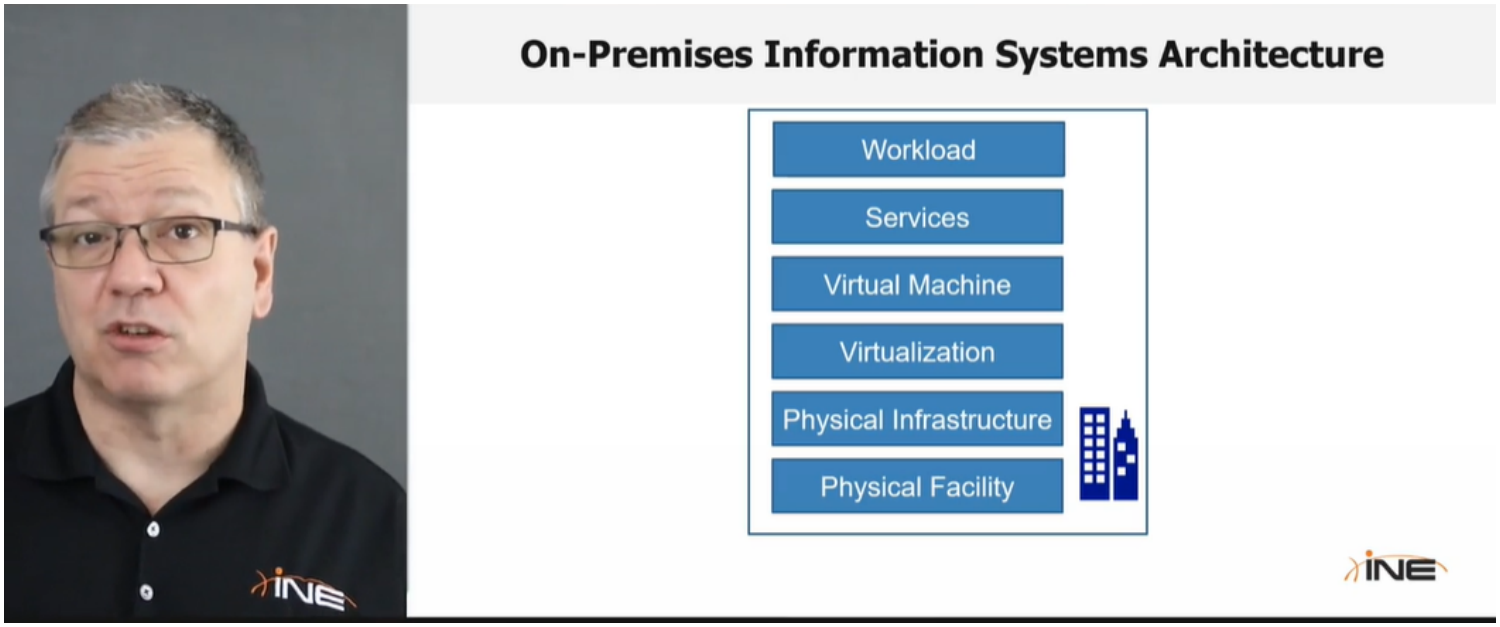
Module-1

What is the outcome of this course?

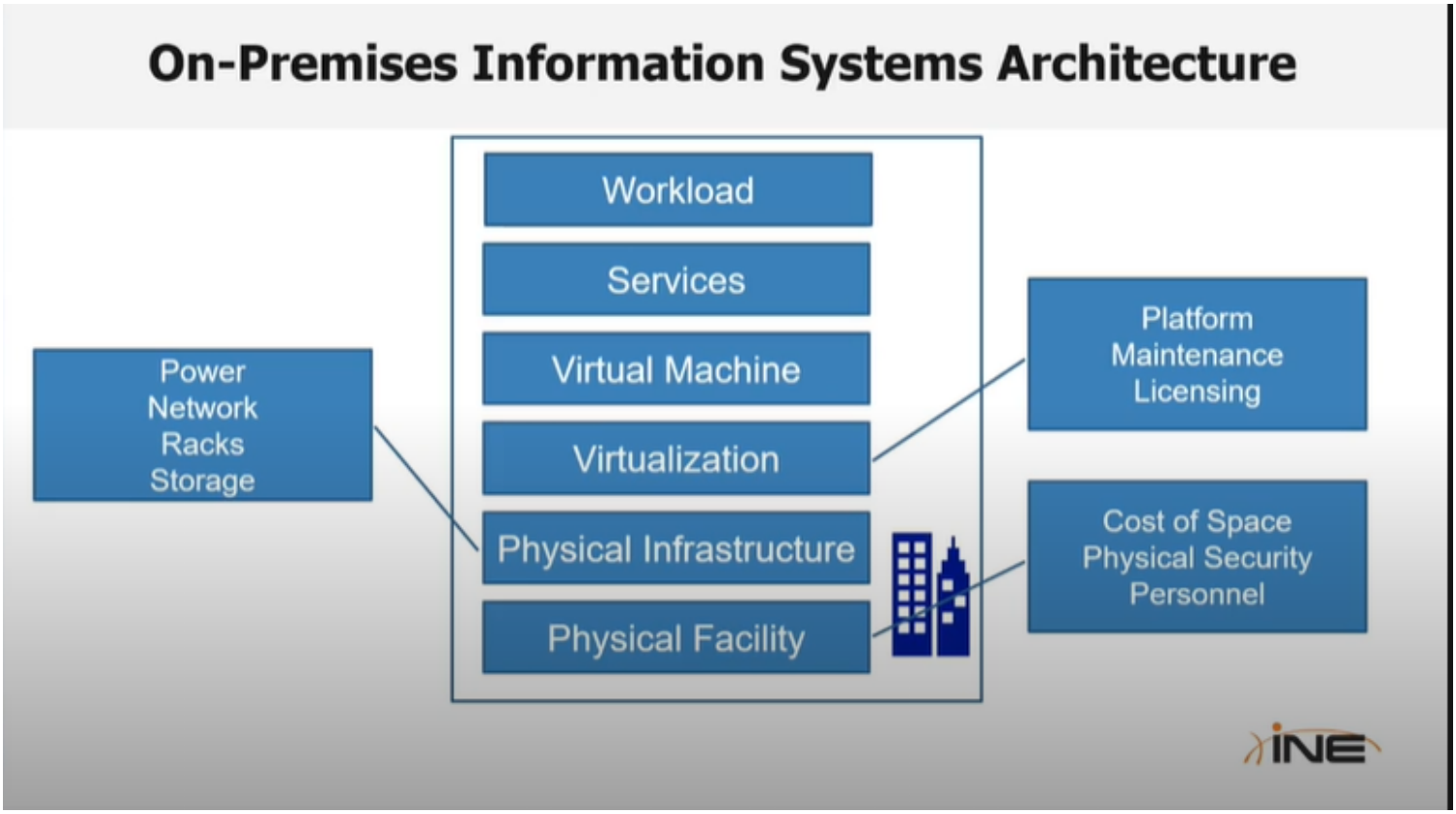
1) Learn to define what is the Cloud??
2) Services provided by the Cloud
3) Why Cloud for industries?
4) Major Cloud Service providers

What is the cloud?

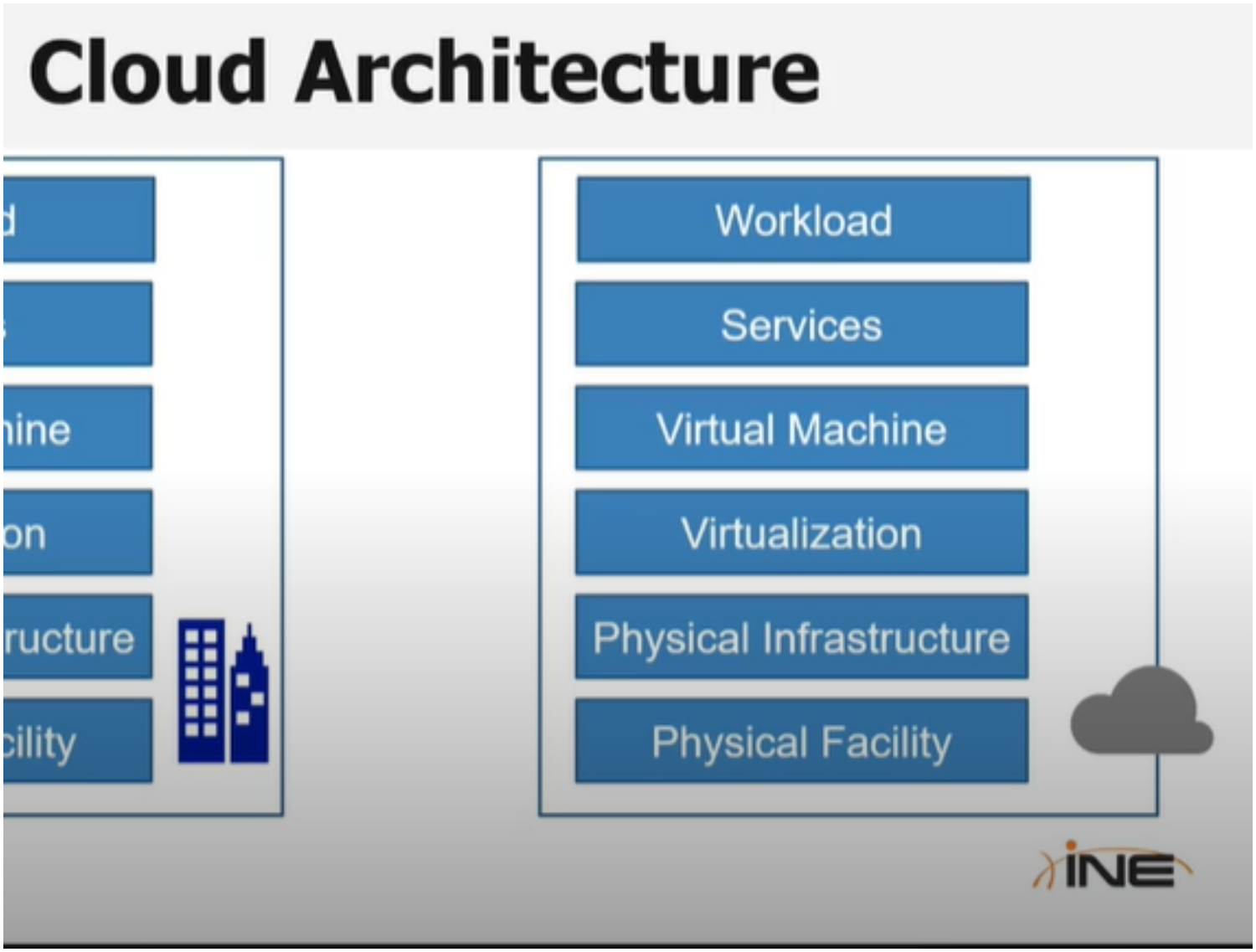
Cloud Architecture:
Types of Cloud Services
Accessing Cloud Services



Some hinderance to physical or on-premise data-centers:



Cloud Architecture:



The cloud provides good quality of the bottom three in the stack.
Good physical facility,security and IT infrastructure which most small to medium organizations can't afford.
Biggest reason why companies move towards cloud.

Types of cloud services

1)(Workload) Software as service :
This provides companies cloud based softwares as service eg:G-Suite,Microsoft 365 etc

2)Platform as a service (Just avail the entire services like server,databases):

When i use the entire platform provided by the cloud to manage services like hosting of websites and databases then it is Platform as a service.The cloud providers provides me web servers ,databases vm's etc and i can just provide the code to run.

3)Infrastructure as a service:
When i use the cloud to spin up virtual machines just for the infrastructure it provides then it is Infrastructure as service

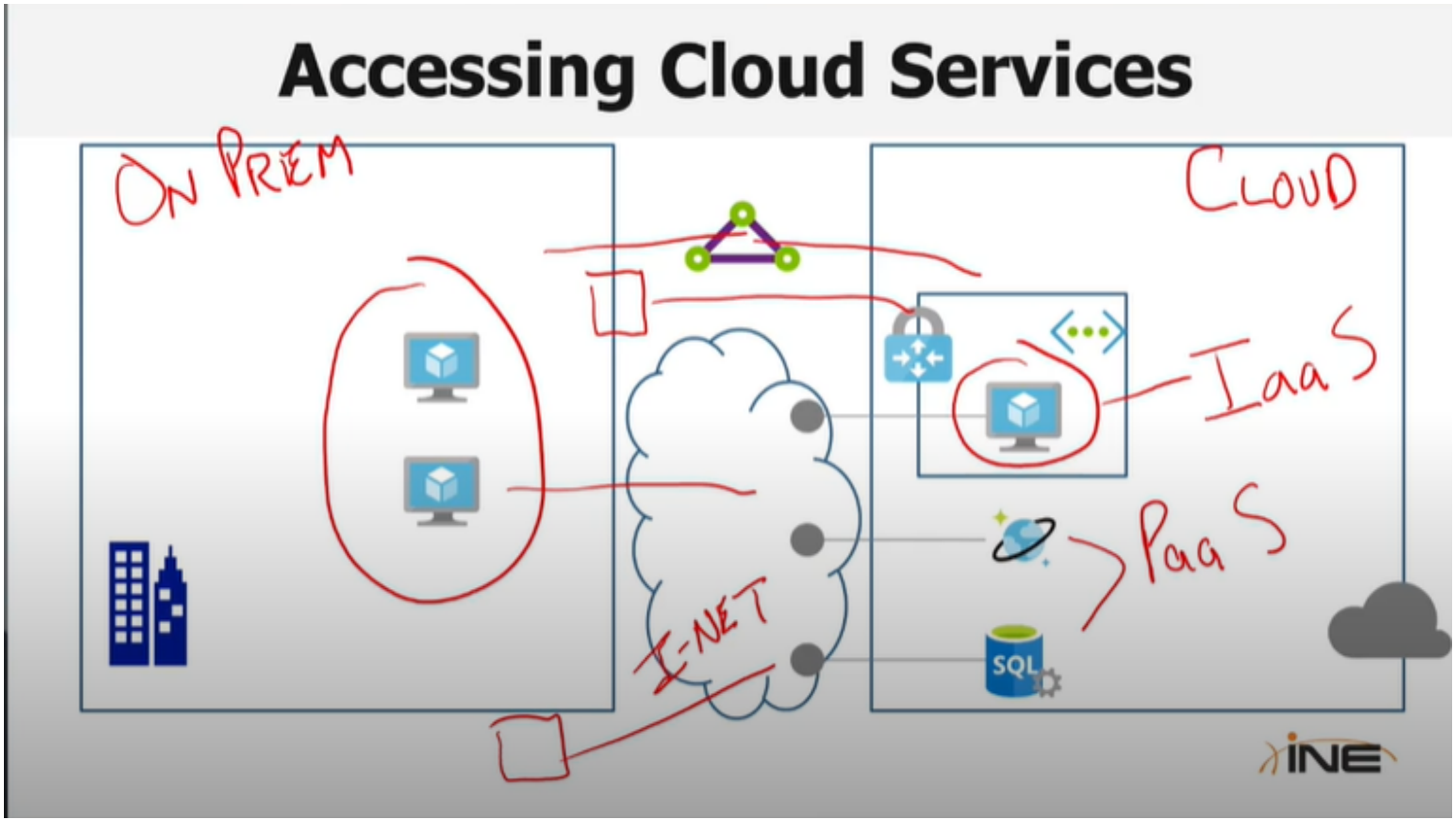
When i go from infrastructure as service to software as service- Ease of administration increases ie With G-Suite i can directly open up google docs and i am not worried on installing any dependencies in my machine

But the **Control i have** towards the services **decrease** when i move **from infrastructure to software**
ie When i have just a vm i am free to install softwares but when i go for Software as service most of the control lies with the cloud providers.

Accessing cloud services

1)Use Internet to access cloud services form on-premise
2)Use VPN from on-premise to connect to data-centers to access cloud services
3)Private connection to cloud data-centers

And many more ways



We can get a great VM with several virtual CPU GPU etc

WHo are cloud providers?

WHo are cloud-providers?

Amazon is the biggest cloud-provider
Microsoft at second and Google at third

AWS ---- first biggest specifically cloud based provider
175 products and services (a looooooot)

Azure ---- 169 services

Google Cloud-- 90 services

Tencent and Alibaba --- very large in China
Oracle and IBM

Digital Ocean

cloud management

We can manage cloud services in three ways:

1)Web application

2)Command line interface

3)REST API

4)SDK in some Programming Languages

For the command line interface management ,the cloud providers themself provides Cloud Shell which allows us to interact
with the services without installing any software or OS in our system.

In the CLI management we are also provided with options like the Bash shell or The Powershell.

cloud cost management

optimizing cost is the major thing to be learnt.

Most cloud providers provide Cost calculators to know about our use and set alerts,budgets etc.

Cloud providers have costs or billing in 2 categories:

1)Consumption based billing (we have to pay for how much we use. Basically difficult to compute the cost)

2)Capacity based billing (Pay for the storage you use)(database,web server etc)

The cost changes from providers to providers.
The cloud providers also have a weird feature like its free to upload resource to them but when you transfer them or
egress this into another machine you are charged.

Also sometimes some service from the cloud may be from 3rd parties and they come up with extra cost apart from the cloud cost.(Marketplace billing)

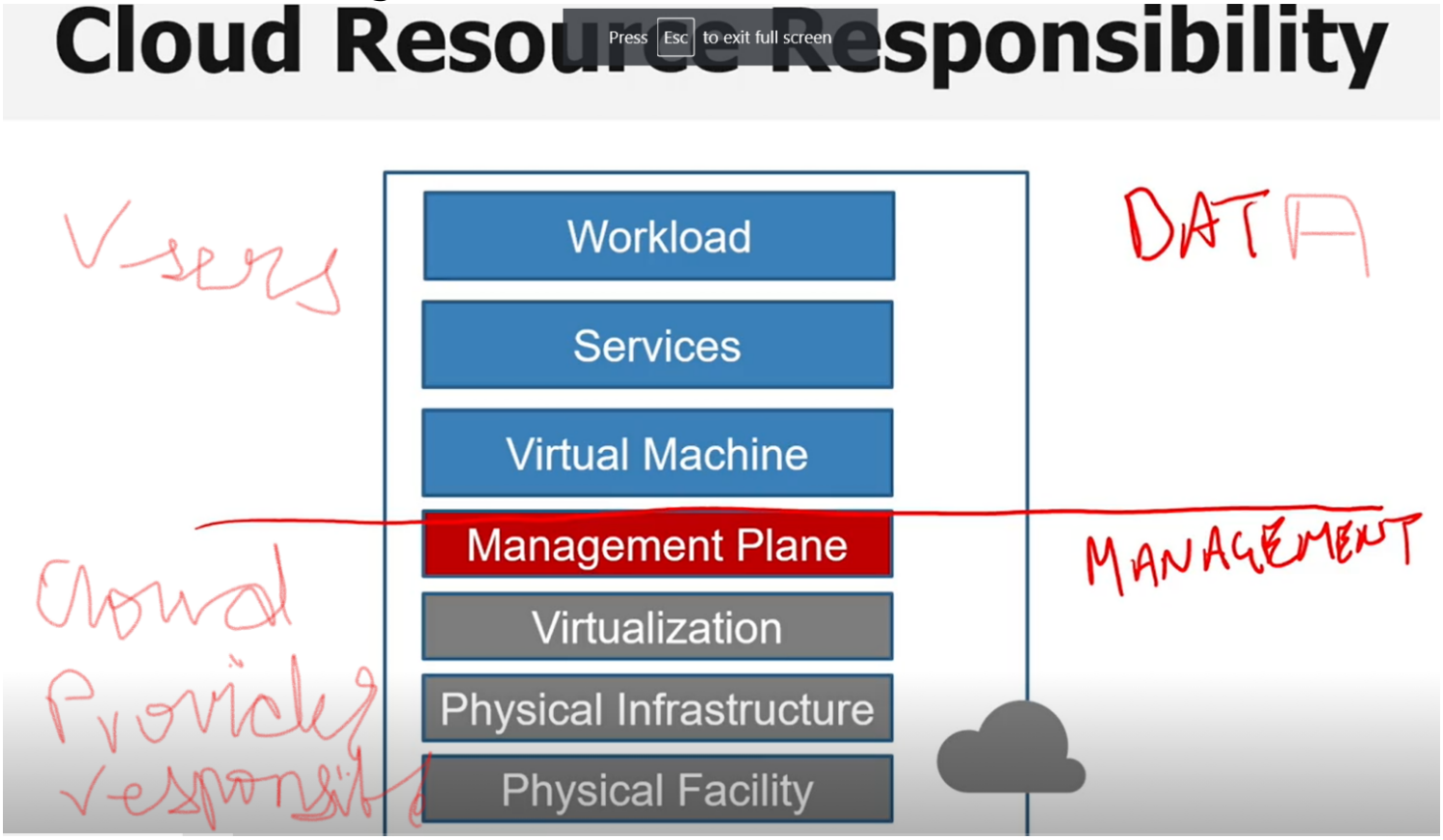
Example :May be some Linux distro is a premium one or some firewall which is owned by a 3rd party company.

Most of the cloud providers have calculators to find out the cost you will be paying for the services required.
There are lots of ways to optimize this so try to play around with it.

Ec2(Elastic Cloud Compute) is AWS service and this has things like VMs ,databases etc.

cloud support service

SLA- service level agreement



The user and cloud providers responsibility are called Management Plane and Data Plane respectively.

The management plane and data plane changes with respect to service we opt from the cloud.

Lets say we choose software as a service(G-suite) then the entire responsibility relies on the cloud providers as we cant do anything about something happenning to the software.)(Though we have some customizations)

Then if we choose platform as a service only the Workload we provide is our responsibilty and everything under that
1)Services(eg nginx server)
2)Virtual machine(eg linux instance to run web apps)

3)Physical infrastructure ,security etc everything is the cloud providers duty to maintain

The SLA provided by AWS for EC2 instance (vms ,databases etc) is 99 percent.

We can check the percent provided by the vendors as they have documentation for this.

Cloud Support

- AWS
  - Basic
  - Developer
  - Business
  - Enterprise
- Azure
  - Basic
  - Developer
  - Standard
  - Professional direct
- Google Cloud Platform
  - Basic
  - Developer
  - Production
  - Premium

The basic is the free one and other three are paid ones.
For each tier increase we get much more service from the vendor.

cloud infrastructure

Infrastructure as a service:

Getting machines to use our VMs,setting up network of machines,getting storage space are called infrastructure as a service.

The **virtualization,physical infrastructure, physical facility** are the responsibilities of the vendor .
And we use only these from the vendor nothing more.

Not only we can get a single VM instance but we can actually setup an entire network machines and also **easily** setup network configuration and rules for them.
These setting up of virtual networks in the cloud also comes under infrastructure as a service.

EC2/VM:

These instances comes up with something called Series and Sizes.

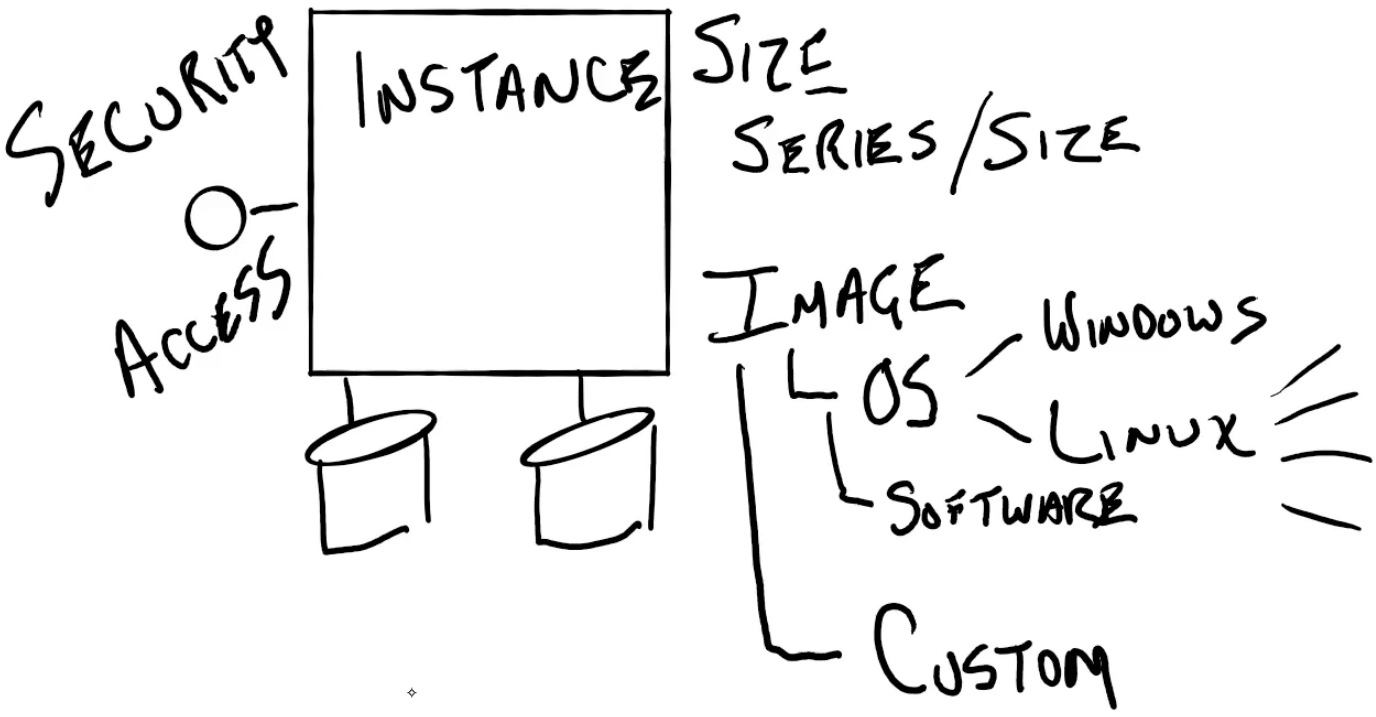
These series actually defines what are the features/specs provided for the instance we are gonna deploy.
The specs include the type of processor,amount of memory,storage capacity and much more.

The sizes in the series defines the amount of or number of cpus,RAM,HDD etc required.

The other choice we have is the IMAGE/OS that has to be deployed.

Images include

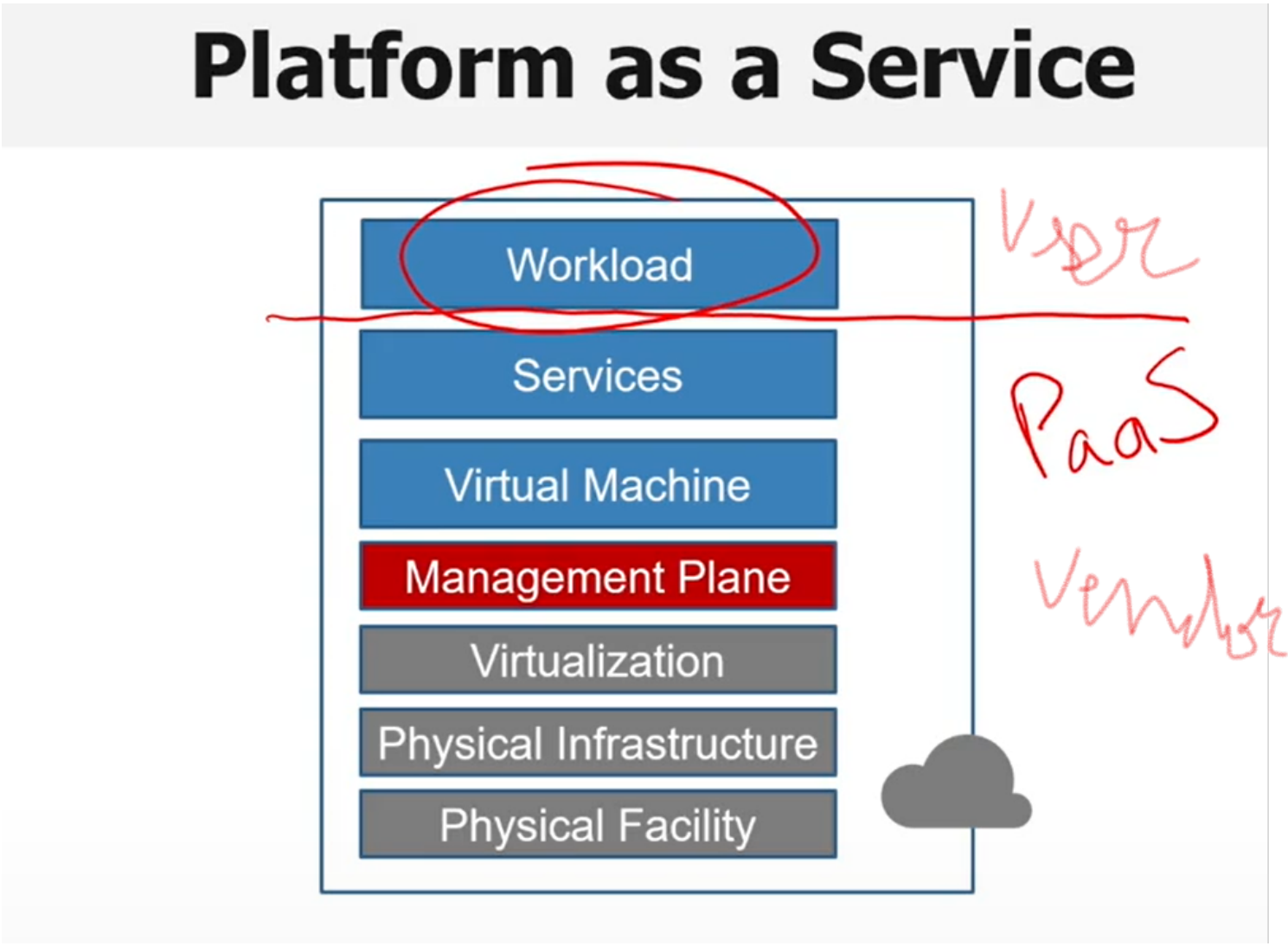
1)WIndows
2)Linux and its various distros
3)Images with some pre-installed softwares.
3)Custom Images



Cloud Storage

- AWS
  - S3 buckets
  - EFS
  - EBS
- Azure
  - Storage account
  - Managed disks
- Google Cloud
  - Storage buckets
  - Compute engine disks and images

platform as a service



Application hosting:

Containerized and Non-Containerized
Docker Lightsail
Kubernetes run
Fargate

Data HOsting:

Basically databases

Relational and Non-relational databases

Application HOstinG:

We can host webapps in any language in the cloud using the cloud platform.
In this case the vendor provides us server,vm etc and our only job is to write code.

AWS has a service called **lambda** which allows us to write functions which has to get executed and also mention some triggers to start its execution.

We can choose a HTTP API has a trigger and can write a simple Hello world function .
When we try to access this url (which is under api trigger option) we get the output or in other words our function gets executed.

Data HOsting:

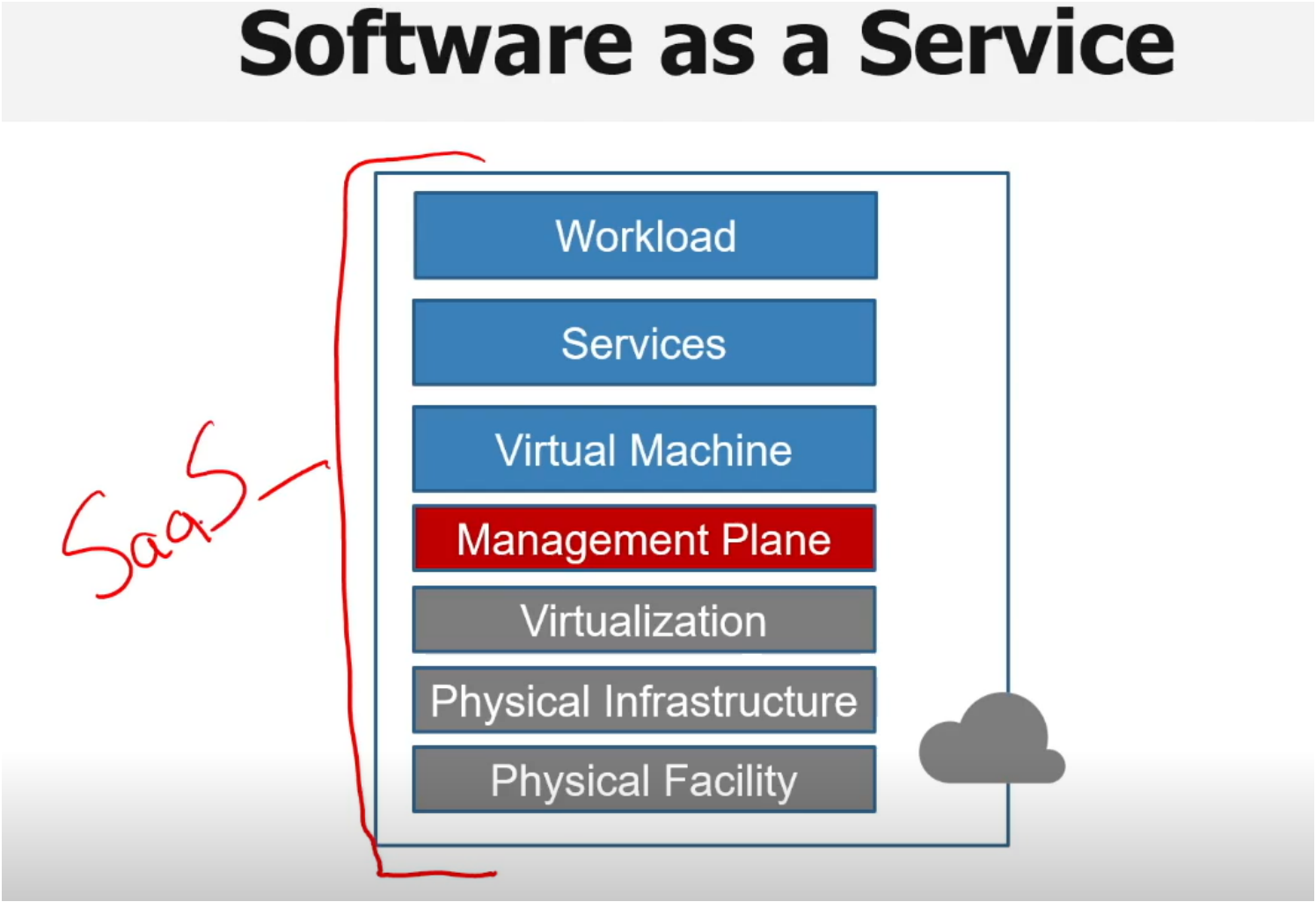
IN AWS RDS has relational databases.
We can create databases ,set credentials and much more. BUt this is a paid service unlike others.
ALso we can connect to these databases from our local machine and work in our comfort.

Cloud application service/Software as a service

Software as a service

Easy topic to understand!!!

Most of the time we are using Software as a service
Eg:G-Suite



Everything is provided by the vendor we just rent them.

SaaS Collaboration tools

Slack
Zoom
Microsoft teams

In SaaS we can also manage workloads independently.

module-2

Cloud management concepts

1)Shared responsibility model

2)CLoud monitoring

3)Access and Identity management

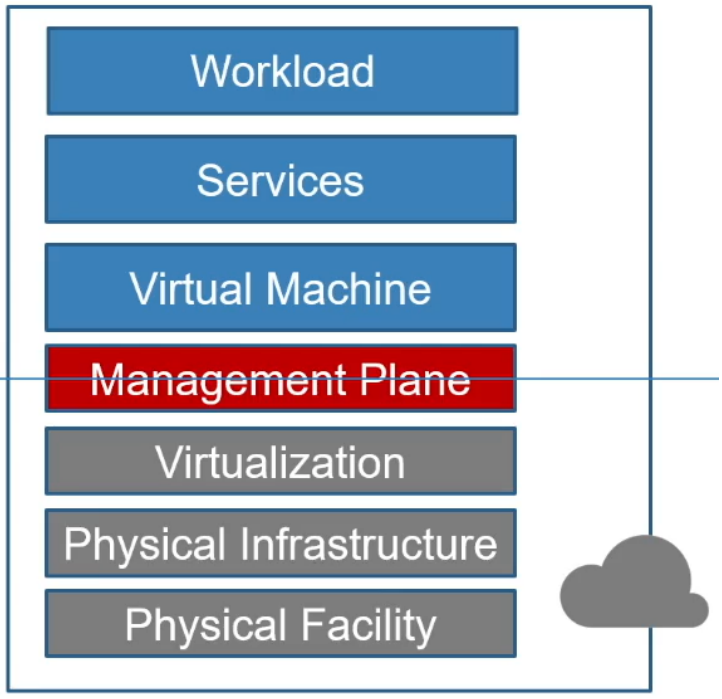
4)Provisioning and managing resources in the cloud

shared responsibility model

Management Responsibility

You are always responsible for managing your identities, and access to your subscription

The cloud provider is always responsible for managing and securing the facility, infrastructure, virtualization, and cloud management plane



This module talks on the responsibilities of the provider and the customer and the shared ones.
Also how these responsibilities change with the type of service we get like Iaas,Paas,Saas.

The managing of the resources must be given equal care in the cloud as on-premise as a user we still have responsibilities and duties to be performed in order for smooth functioning.

Standard Compliance is responsibility of both vendor and customer.

Learnt how to setup database server in RDS (AWS) and connect to it using MySQL workbench.

managing cloud resources

Daily management of course:

The complex management tools is the REST APIs which can be used to communicate with the cloud resources by building our own software on-premise.

Next we have CLI tools.
Next we have SDK in different languages.

Finally the trivial and easier one is the Web console.

Data plane in Iaas but not in Paas -- VIrtual machines,Services

monitoring and alerts

Very critical thing to do especially in the cloud as our application is in someone's data center.So monitoring becomes critical

Azure Monitor
AWS CloudWatch
Google Cloud Monitoring

Unified Monitoring:

These 3rd party monitoring tools can be integrated to work with cloud.

Nagios
Splunk
PRTG

The cloud providers also provide some monitoring tools.

Proactive Resource Management:
Simple words automating monitoring by triggering alerts.

cloud identity and access management

Cloud based identity
Access Management

Topics to be covered in depth .

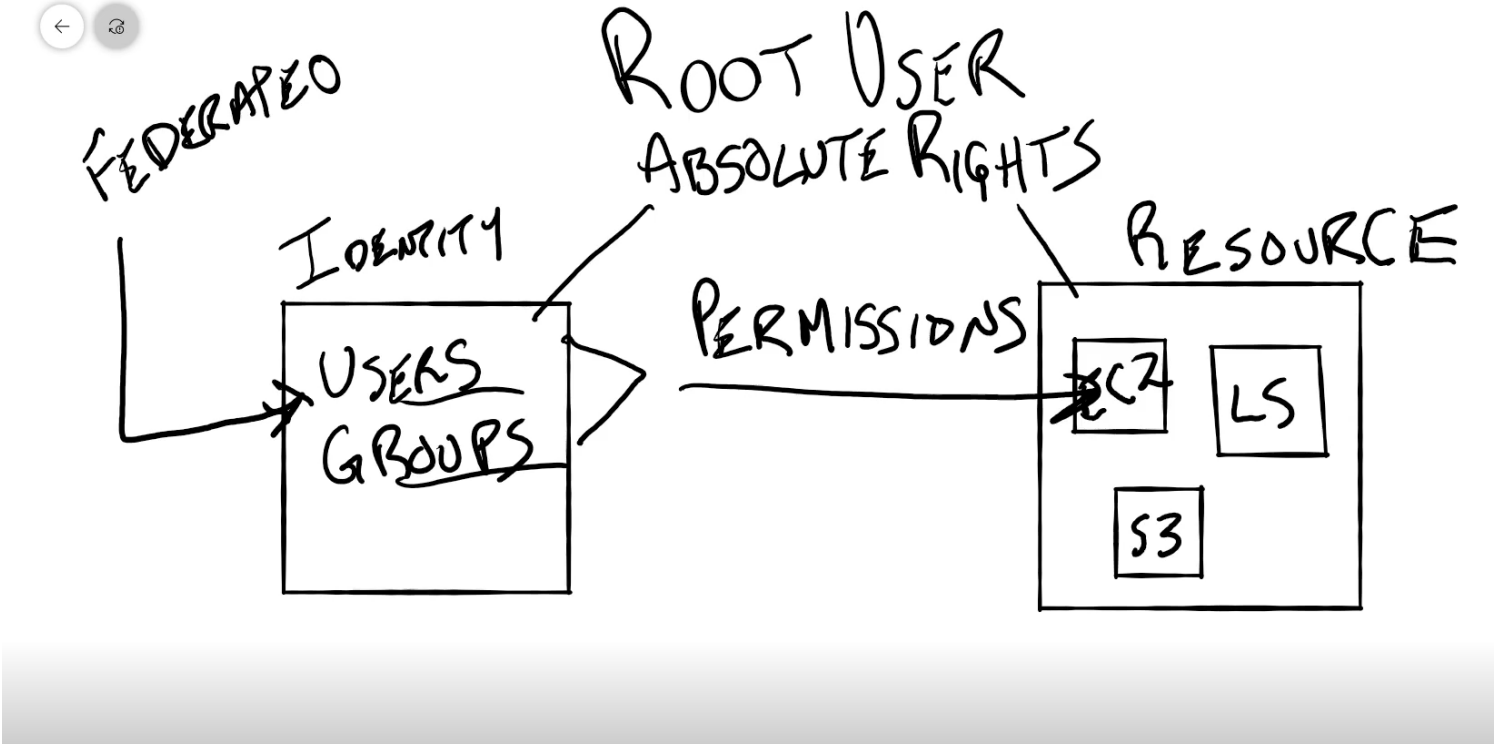
Whenever we create an account we have the root privileges.This is for every vendor.
With the root priv we have to very cautious.

Root user can create

1)Identity(users , groups)
2)Resources(ec2 ,rds etc)

Permission are assigned as

Policies in AWS and GCP
Roles in Azure



Azure

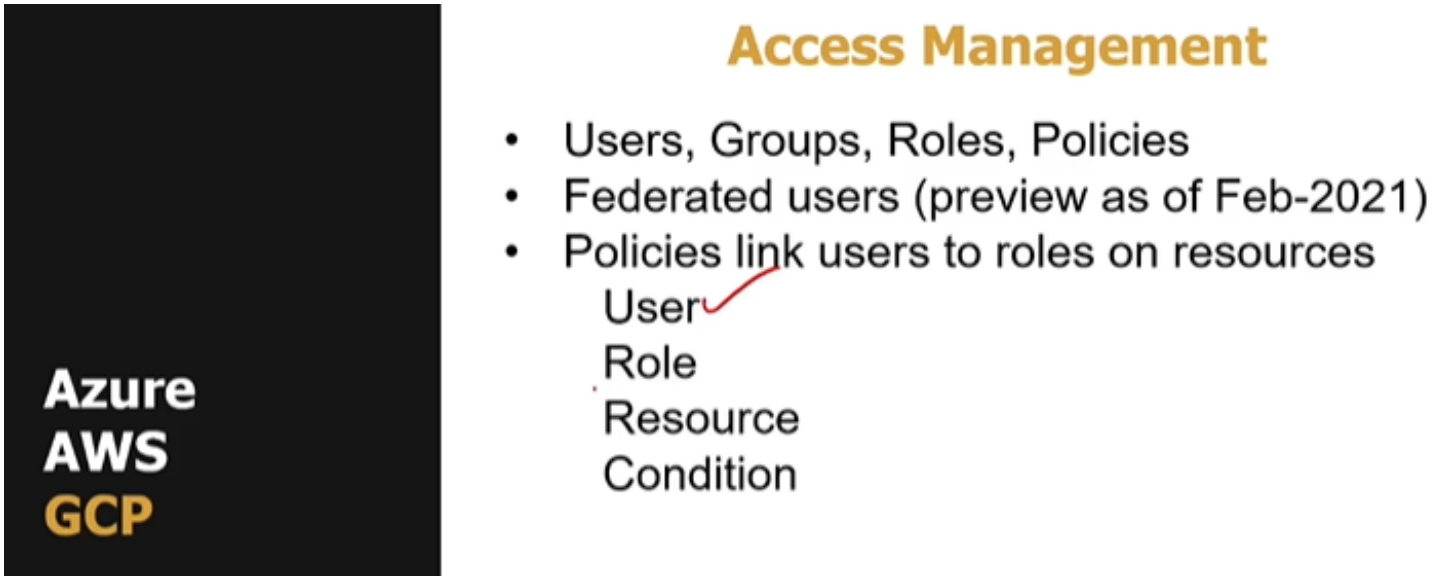
Access Management

- Users, Groups, Roles
- Federated users

Azure
AWS

Access Management

- Users, Groups, Permissions
- Federated users
- Policies grant permissions
  - Effect (allow/deny)
  - Action
  - Resources
  - Conditions



in AWS find IAM service to set policies , user, groups etc

Module-3

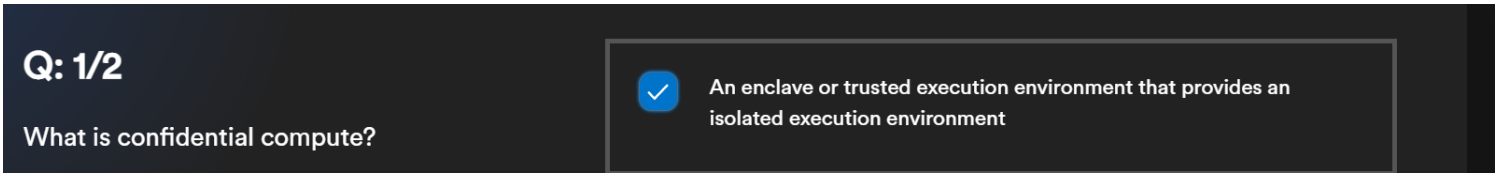
Security ,Compliance

Multi factor authentication is recommended by all the cloud providers.
When managing user identities the flow to be followed is identity->Group->Role->Resource

HSM(Hardware Security Modules) used to store certificates and sensitive keys in the cloud.

Five Rs
Revoke
Reset
Review
Remediate
Return

Many cloud providers give ambient protection(advertising kinda) to Ddos attacks.



Cloud security

Encryption in transit
Encryption at rest

Helps to secure resources in the cloud.

common cloud attacks

We will talk on

Targets
Attacks

Targets:

The targets depend on type of cloud service we will be opting namely Saas,Iaas,Paas.
Also can be classified as

1)Identities

2)Data

3)Services

Identities Targets:

1)The credentials we use to login to a Cloud based software (eg Microsoft 365)

2)The credentials we use to login to the Cloud console (Azure)

3)Data plane identities (If i run a mysql server which holds data of users then the credentials of mysql)

Data Targets:

1)S3 buckets

Services Targets:

1)Email service (Biggest Target)

2)Control Plane Services

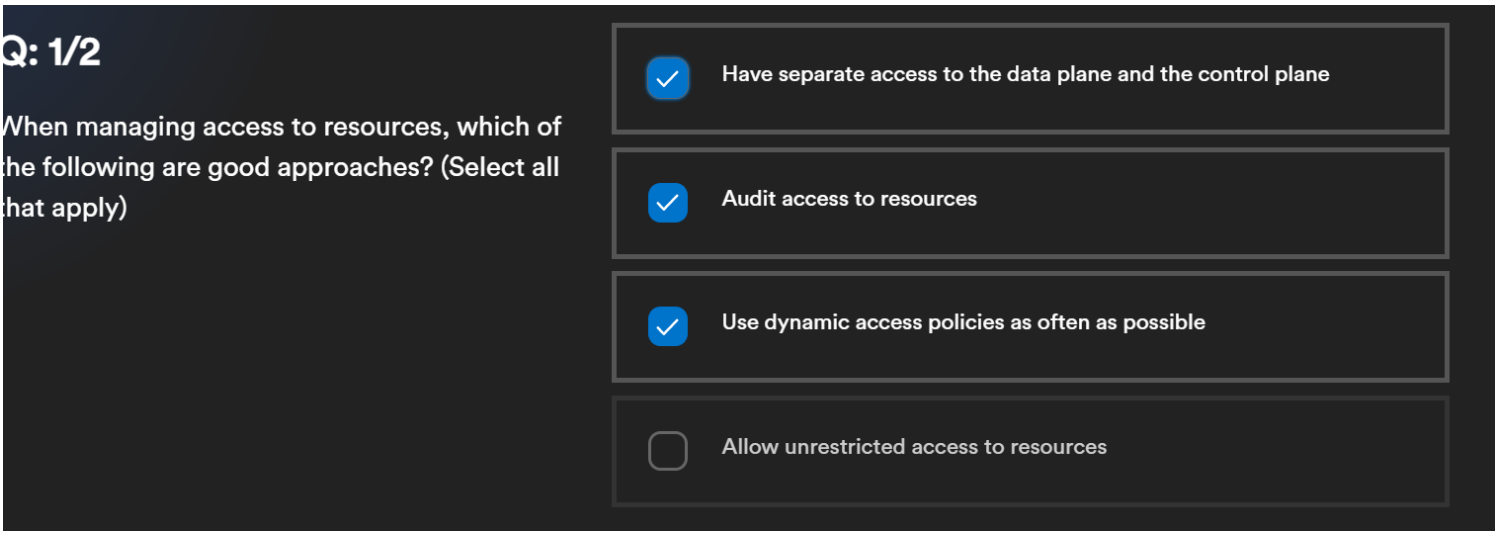
3)Ec2 instances (Compromise a cloud account setup Ec2 instance and use this for crypto mining)A common attack

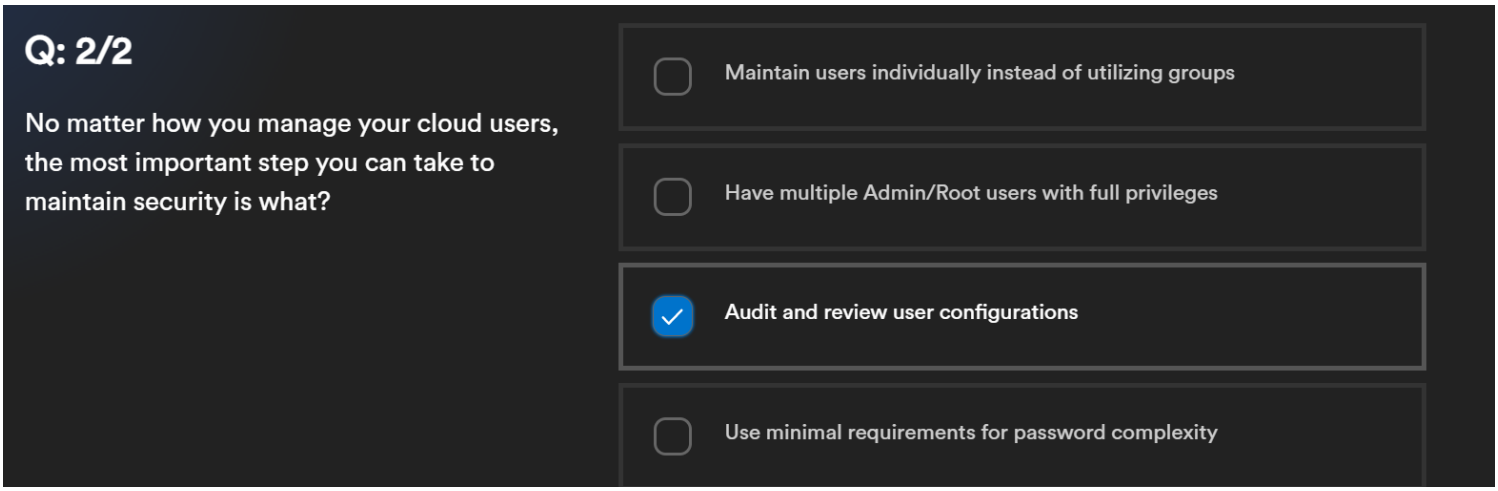
4)API services

Attack Methods:

Identity and Access Management

IAM in short





Dynamic Management:

Unique to cloud

A particular user can be given higher privileges or no privileges based on circumstances.

Identity manage:

min root users
organize into groups
dynamic management
audit and review user config

cloud is a data center of yours but physically residing somewhere else .....

Resource manage:

apply least privileges
dynamic access policies
audit resource access
separate control plane and data plane access

Control Plane ----- AWS console
Data Plane -------- Database you hosted in cloud

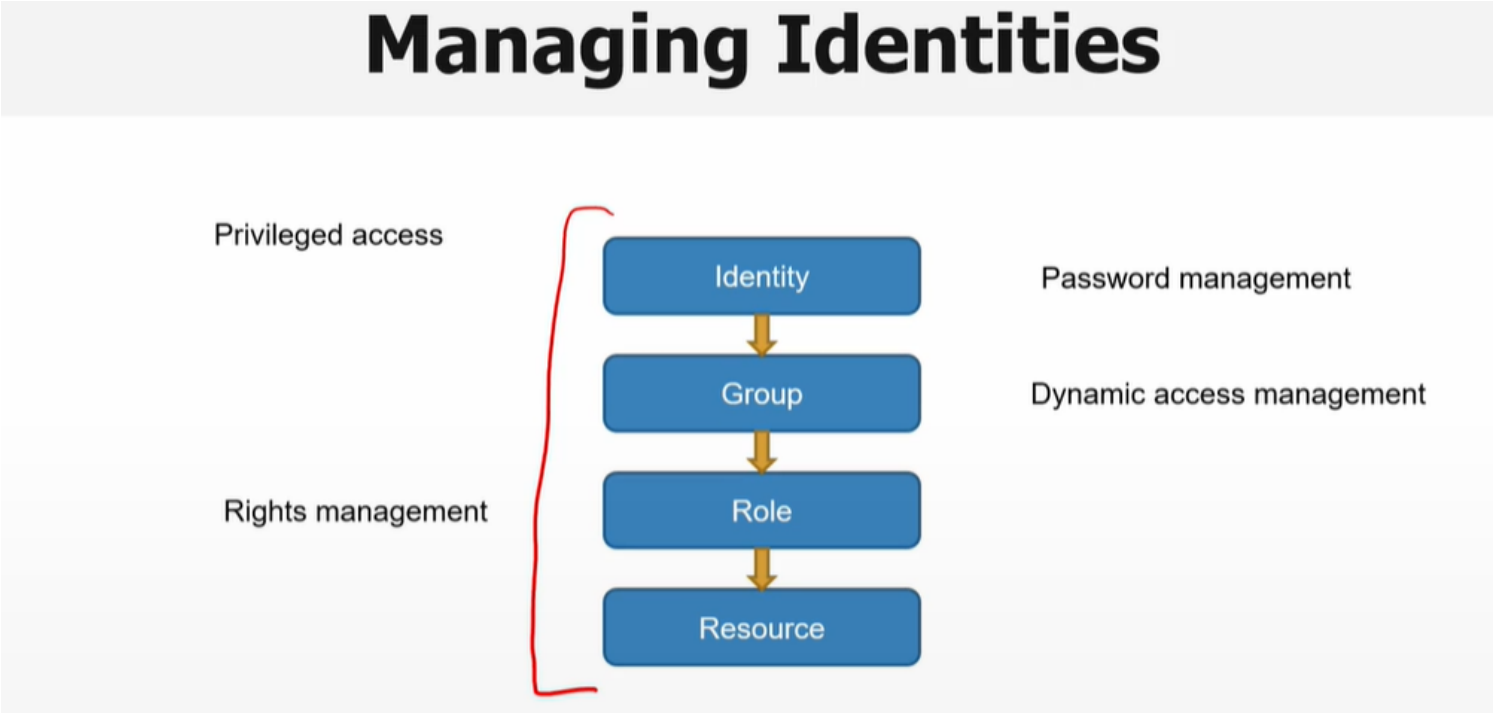
user uses two different creds to access control plane and data plane resources.

identity protection

account vulns
weak passwords
leaked creds
general threat

login vulns
ip address and address anomalies
password spraying
bruteforce

Managing identity



AWS	Azure	GCP
IAM Users IAM Roles IAM Policies	Azure AD Users Azure AD Service Principals Azure AD Managed Identities Roles	Google Account Service Account Role Policy

Identity Protection Services

AWS	Azure	GCP
CloudTrail Trusted Advisor	Identity Protection Azure AD Logs	Advanced Protection Program G-suite alert center Titan security keys

Multi-Factor Authentication

Identity Best Practices

- Apply password policy
- Implement conditional access
- Implement MFA
- Monitor
- Audit unused accounts