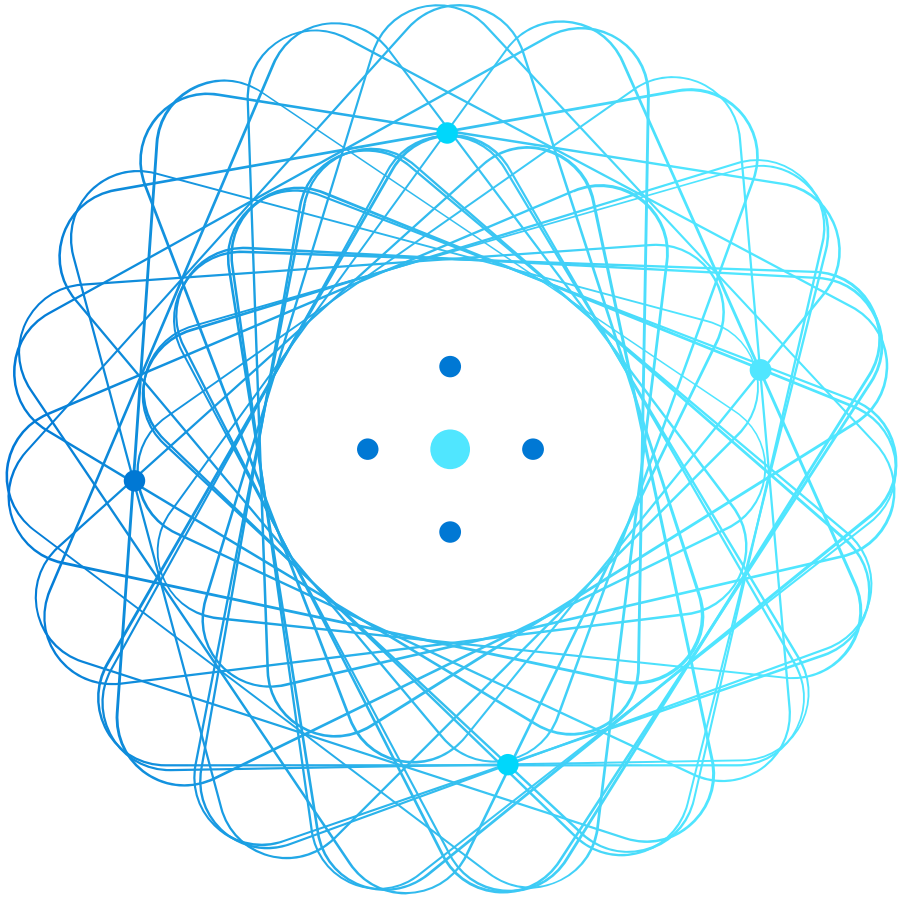
Cloud Computing

Jason Wong
Trainocate Malaysia



Who am I

Google Cloud Platform Certified Trainer

Microsoft CERTIFIED Trainer

CISCO CERTIFIED CCSI INSTRUCTOR

redhat CERTIFIED TRAINING PARTNER

NetApp

IBM MASTER INSTRUCTOR

Agenda

What is Cloud Computing?
How did we get to Cloud Computing? What is Next?
Cloud Models
Benefits of Cloud Computing
Introduction to Cloud Services
Cloud Providers Regions and availability Zones

What is Cloud Computing?

On-demand self-service

No human intervention needed to get resources

Broad network access

Access from anywhere

Resource pooling

Provider shares resources to customers

Rapid elasticity

Get more resources quickly as needed

Measured service

Pay only for what you consume

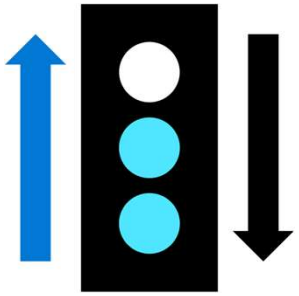
Microsoft Azure Google Cloud amazon web services SOFTLAYER an IBM Company

History of the Cloud

- The roots of cloud computing lie in centralized computing of the 1950s and 1960s.
- Widespread Internet access permitted organizations to offer services over the Internet rather than locally.

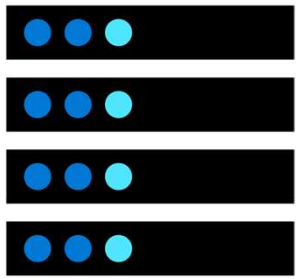
- Examples and key dates:
- **Salesforce.com - 1999**
- **Amazon Web Services - 2002**
- **Google Apps - 2006**

What is Cloud Computing?



Networking

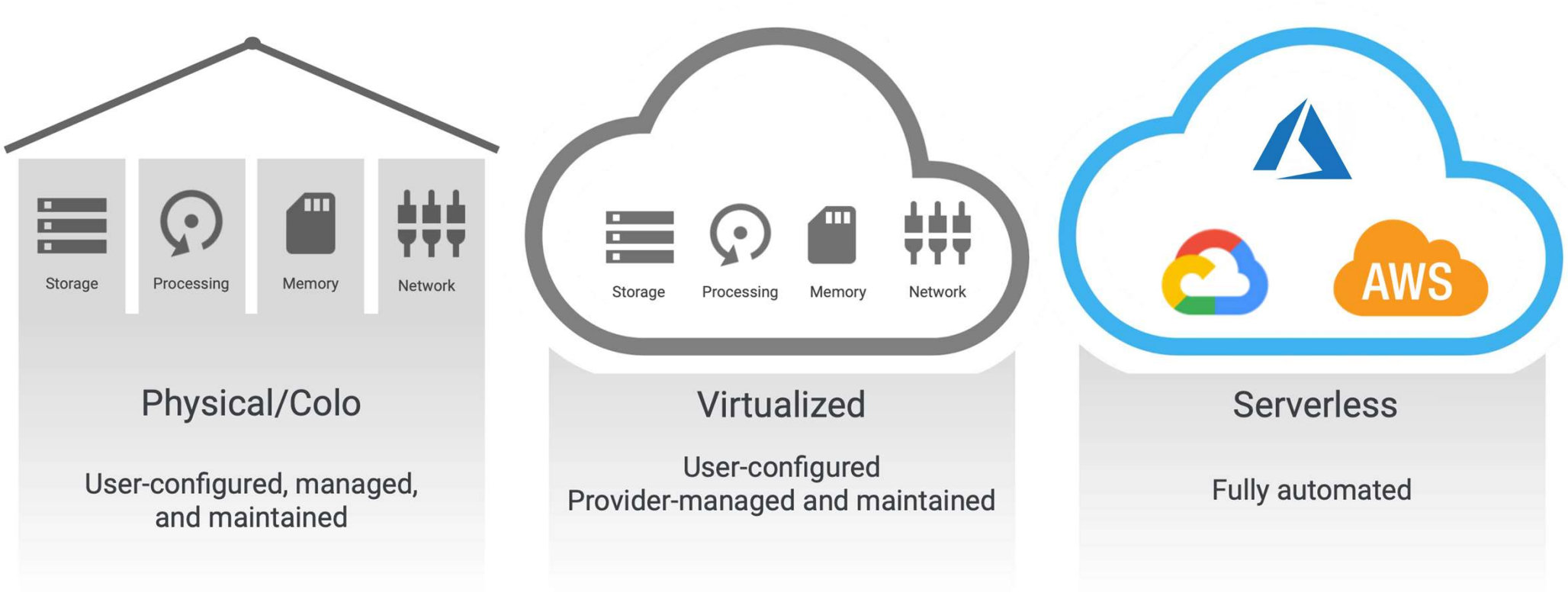
Storage



Compute

Analytics

How did we get to Cloud Computing? What is Next?



Every company is a data company

Cloud Benefits

- High availability
- Fault tolerance
- Scalability
- Elasticity
- Global reach
- Customer latency capabilities
- Agility
- Predictive cost considerations
- Disaster recovery
- Security

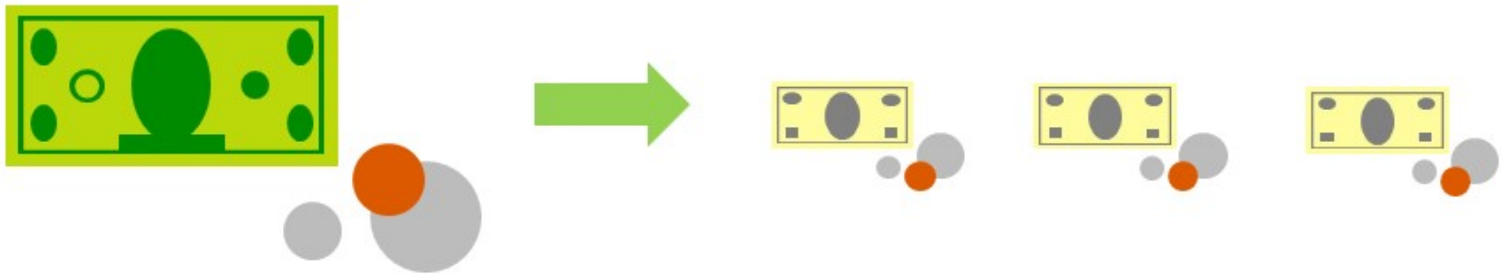
Compare CapEx vs. OpEx

Capital Expenditure (CapEx)

- The up-front spending of money on physical infrastructure.
- Costs from CapEx have a value that reduces over time.

Operational Expenditure (OpEx)

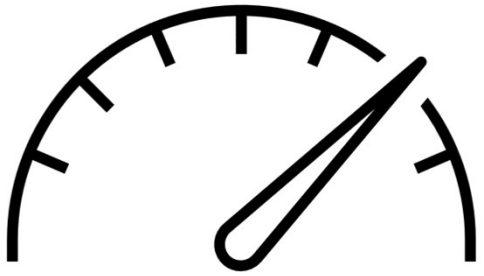
- Spend on products and services as needed, pay-as-you-go
- Get billed immediately



Consumption-based model

- Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use. Whatever they use is what they pay for.

- Better cost prediction
- Prices for individual resources and services are provided
- Billing is based on actual usage

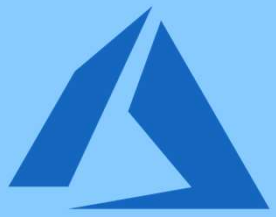


Private

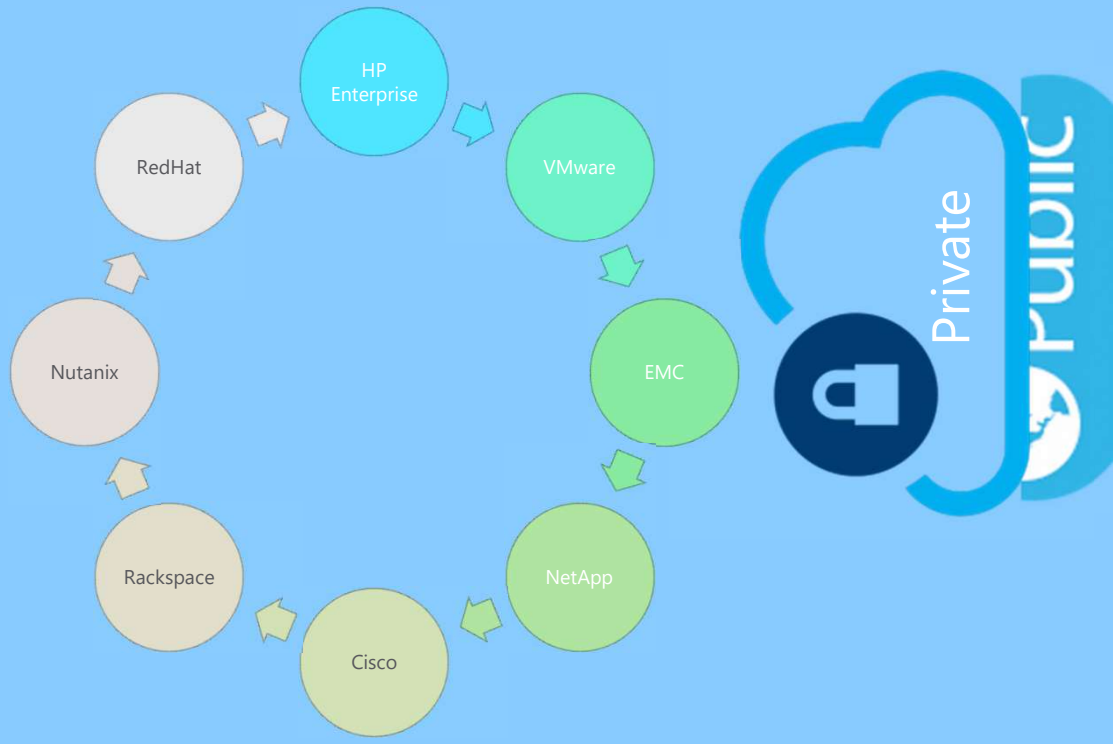
TYPE OF Cloud Computing

- Owned by cloud services or hosting provider.
- Provides resources and services to multiple organizations and users.
- Accessed via secure network connection (typically over the internet).

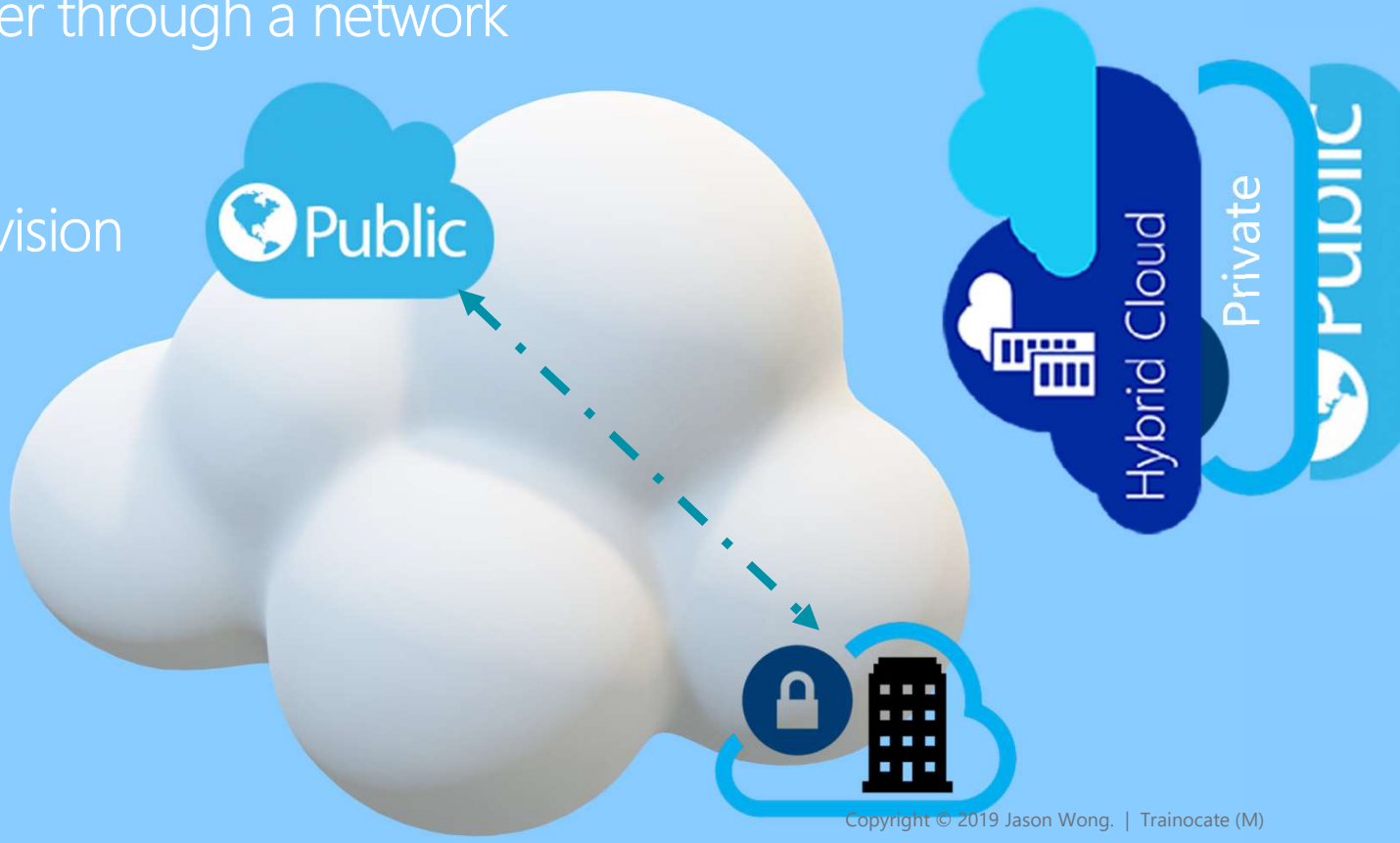
Google Cloud



- Organizations create a cloud environment in their datacenter.
- Internet or private internal network.
- Organization is responsible for operating the services they provide.
- Does not provide access to users outside of the organization.
- Computing services and infra are hosted privately.
- Uses software-defined Networking and Virtualization



Combines Public and Private clouds or on-prem
Fit into appropriate location.
Connect multiple computer through a network
Consolidate IT resources
Workload portability
Scale out and quickly provision new resources
Single management
Orchestration



- **Multitenant platform**
- **Shared cloud environment**

- **Pros:**

✓ Openness and Impartiality
✓ Flexibility and Scalability,
✓ Secure, Compliance,
✓ Controlled level of privacy and configuration

- **Cons:**

× Hardware maintenance
× Remote access may be limited
× Increased IT staff
× Maintenance and capital costs

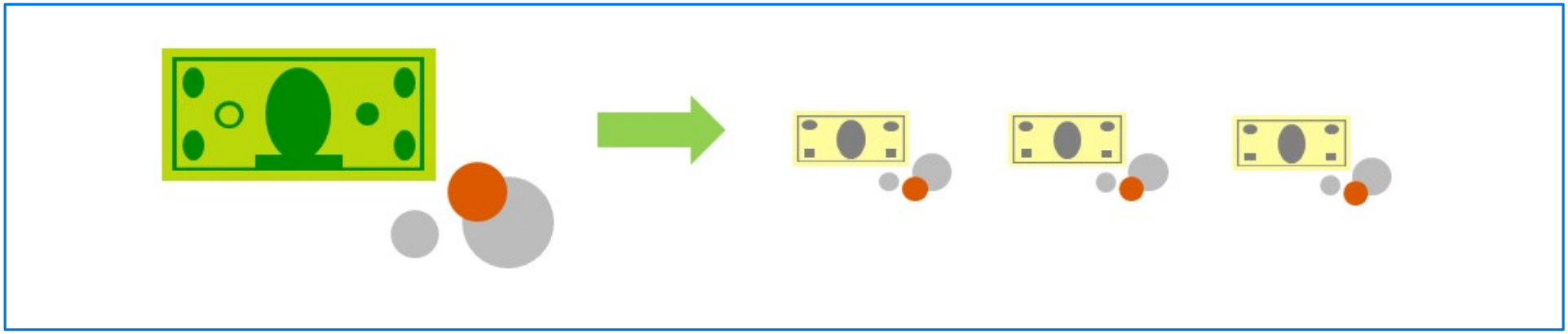
Compare CapEx vs. OpEx

Capital expenditure (CapEx)

- The upfront spending of money on physical infrastructure.
- Costs from CapEx have a value that reduces over time.

Operational expenditure (OpEx)

- Spend on products and services as needed, pay-as-you-go.
- Get billed immediately.



Consumption-based model

Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use.

- **Better cost prediction.**
- **Prices for individual resources and services are provided.**
- **Billing is based on actual usage.**

In summary....

Public Cloud	• No capital expenditures to scale up. • Applications can be quickly provisioned and deprovisioned. • Organizations pay only for what they use.
Private Cloud	• Hardware must be purchased for start-up and maintenance. • Organizations have complete control over resources and security. • Organizations are responsible for hardware maintenance and updates.
Hybrid Cloud	• Provides the most flexibility. • Organizations determine where to run their applications. • Organizations control security, compliance, or legal requirements.
Community Cloud	• Non-profit • Similar to Private cloud but shared environment among organization or community • Achieve common needs among organization

Cloud Services

- What is Infrastructure-as-a-Service (IaaS) ?

✓ Fully customizable environment

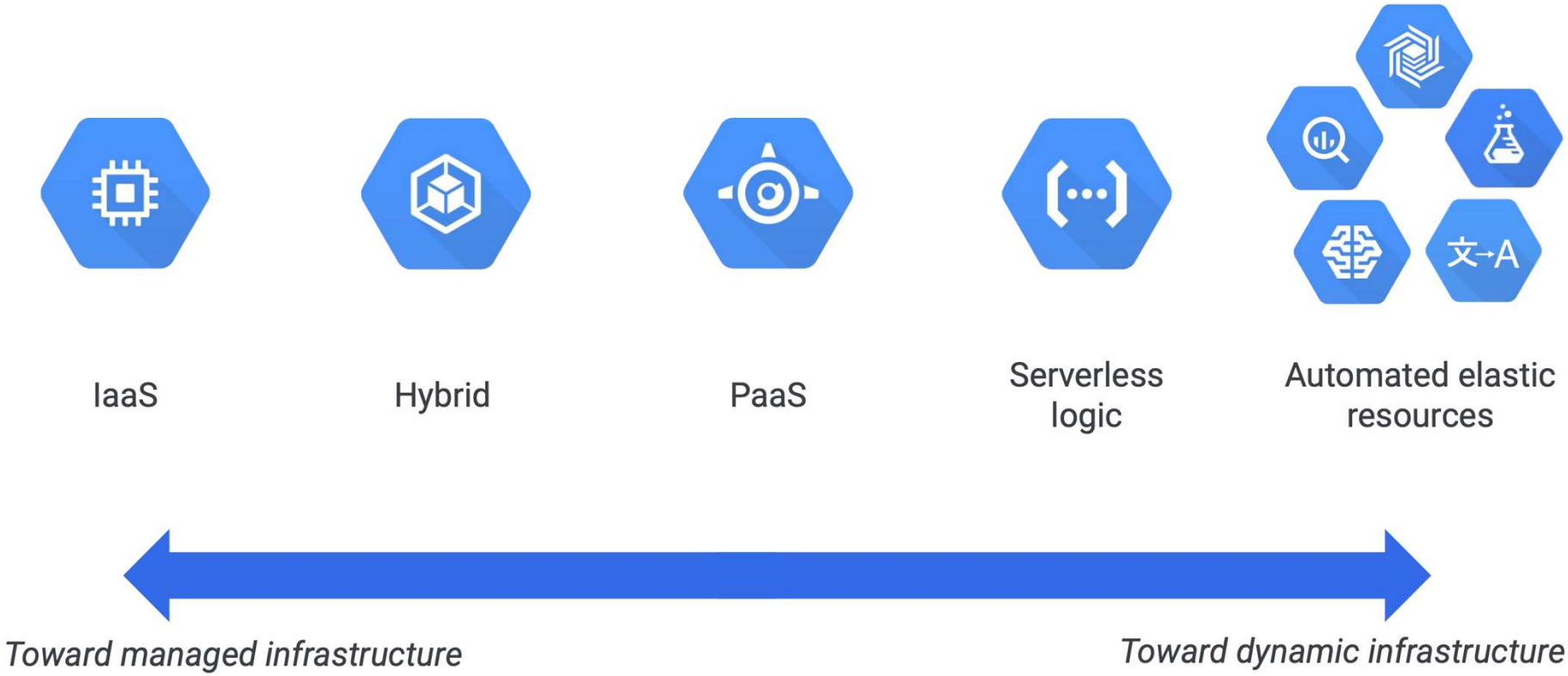
- What is Platform-as-a-Service (PaaS) ?

✓ Fully automated environment for Developers

- Software-as-a-Service (SaaS) , Database-as-a-Service (DBaaS), Monitoring-as-a-Service (MaaS)

✓ Fully automated environment for any applications

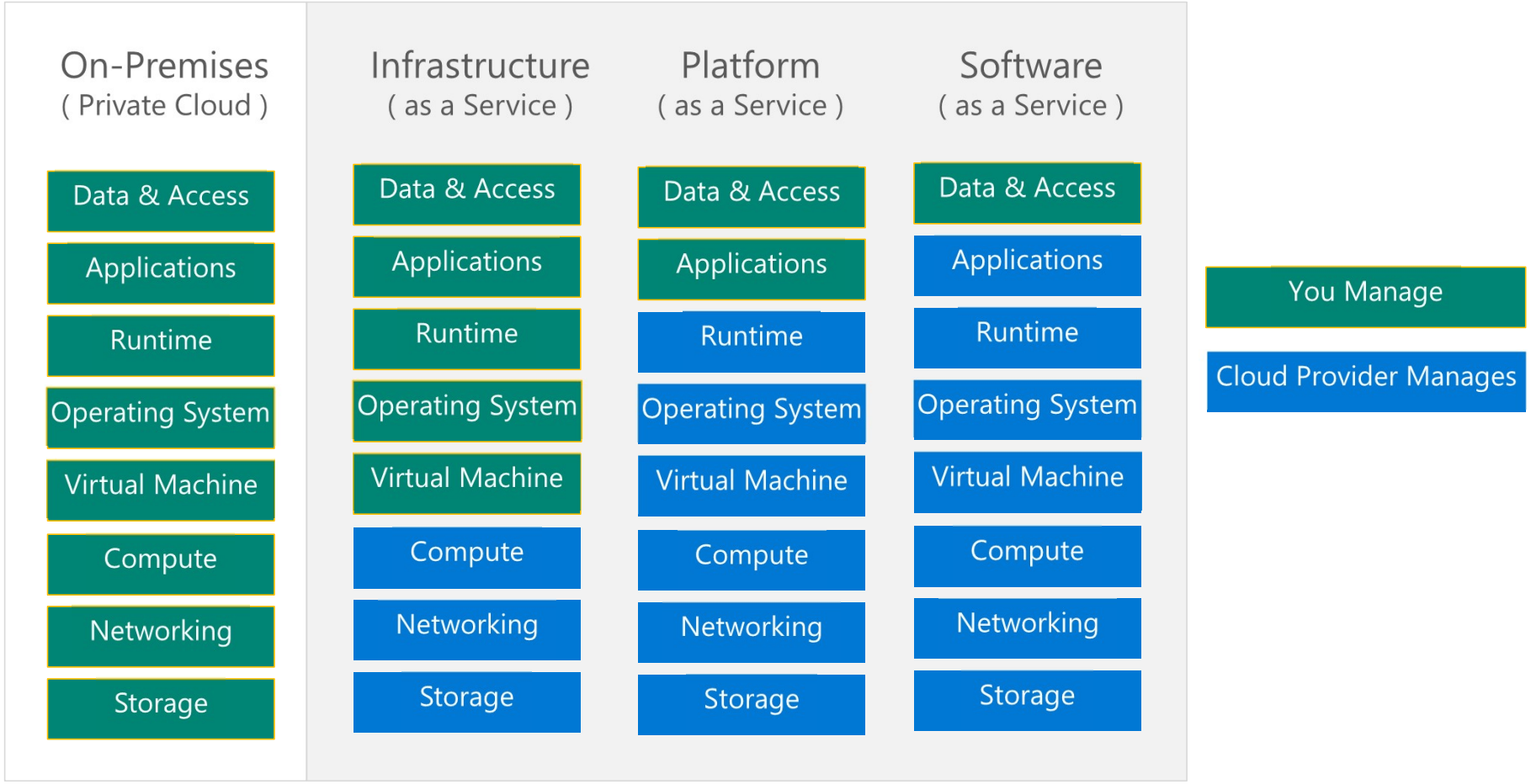
Cloud Services



Cloud service comparison

IaaS	PaaS	SaaS
The most flexible cloud service.	Focus on application development.	Pay-as-you-go pricing model.
You configure and manage the hardware for your application.	Platform management is handled by the cloud provider.	Users pay for the software they use on a subscription model.

Shared responsibility model



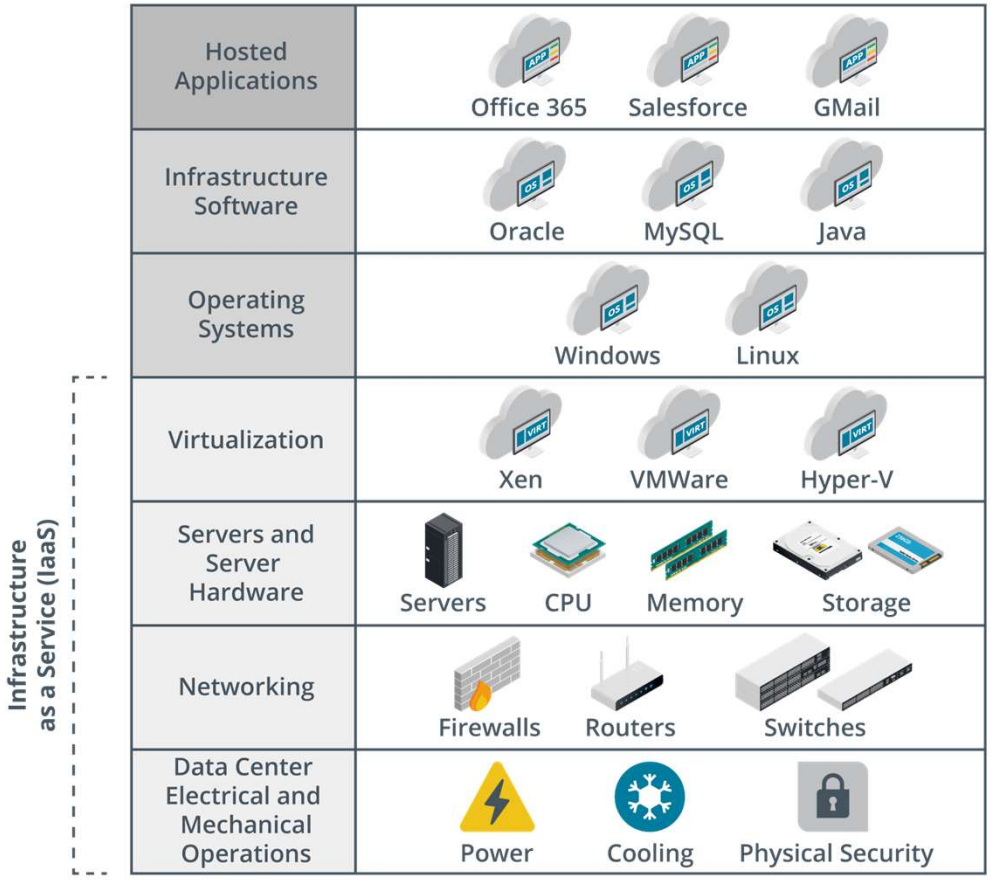
Infrastructure as a Service (IaaS)

- Cloud service provider retains responsibility for hardware support.
- Consumers are responsible for the management of virtual machines that are hosted on the CSP hardware infrastructure.
- Businesses can deploy exactly the number of servers they need.
- May realize a reduction in capital expenditures for hardware and licenses.

- Costing: Highest among all. Pay per resource allocation. May run 24/7
- Target audience: IT administrators

Infrastructure as a Service Examples

- AWS EC2
- Google GCE
- Azure VM
- Rackspace
- Digital Ocean



Platform as a Service (PaaS)

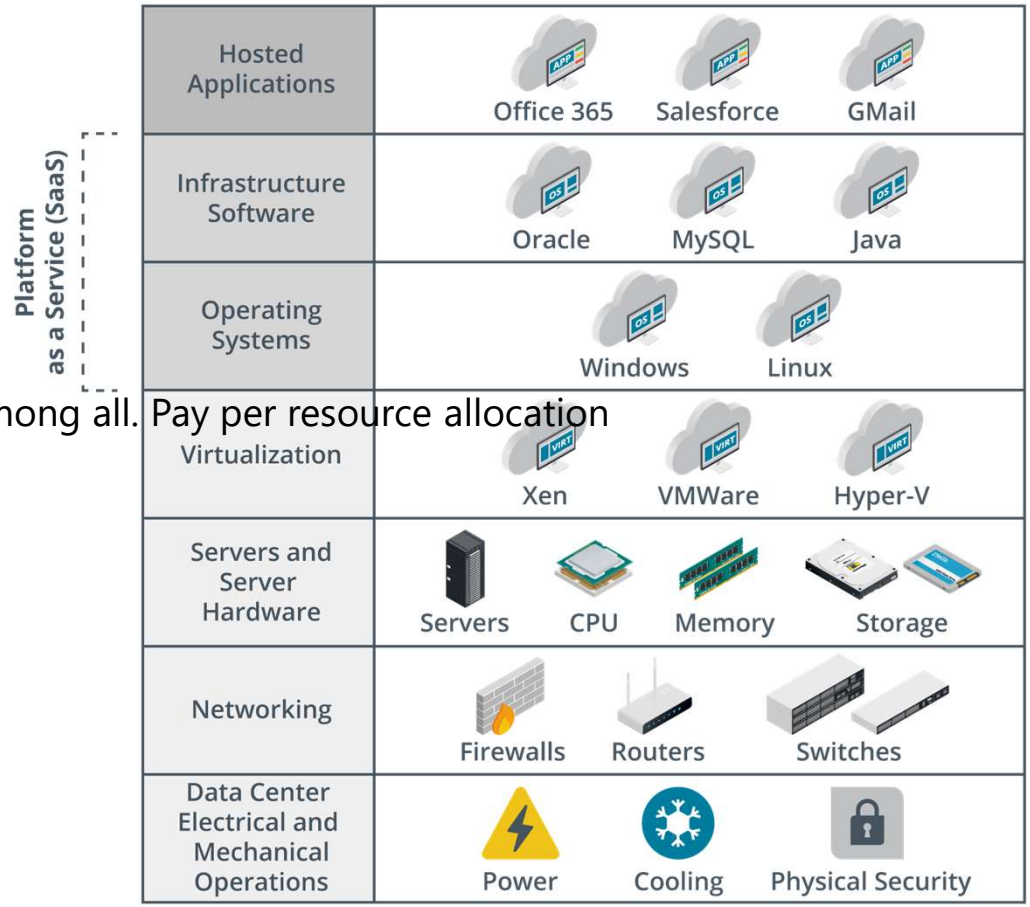
- Cloud service provider retains responsibility for the hardware and operating system and provides platform maintenance.
- Customer uses the platform for business operations.
- Typically used to provide development and database platforms to the organization's developers and database administrators.

- Costing: Lower than IaaS. Pay per resource Utilization. May run 24/7
- Target audience: Developers, Database Administrators (DBAs)

Platform as a Service Examples

- Google App Engine
- Google Run
- Azure App Service, Azure Functions
- AWS Cloud 9
- AWS Elastic Beanstalk
- Salesforce Heroku

• Costing: Highest among all. Pay per resource allocation



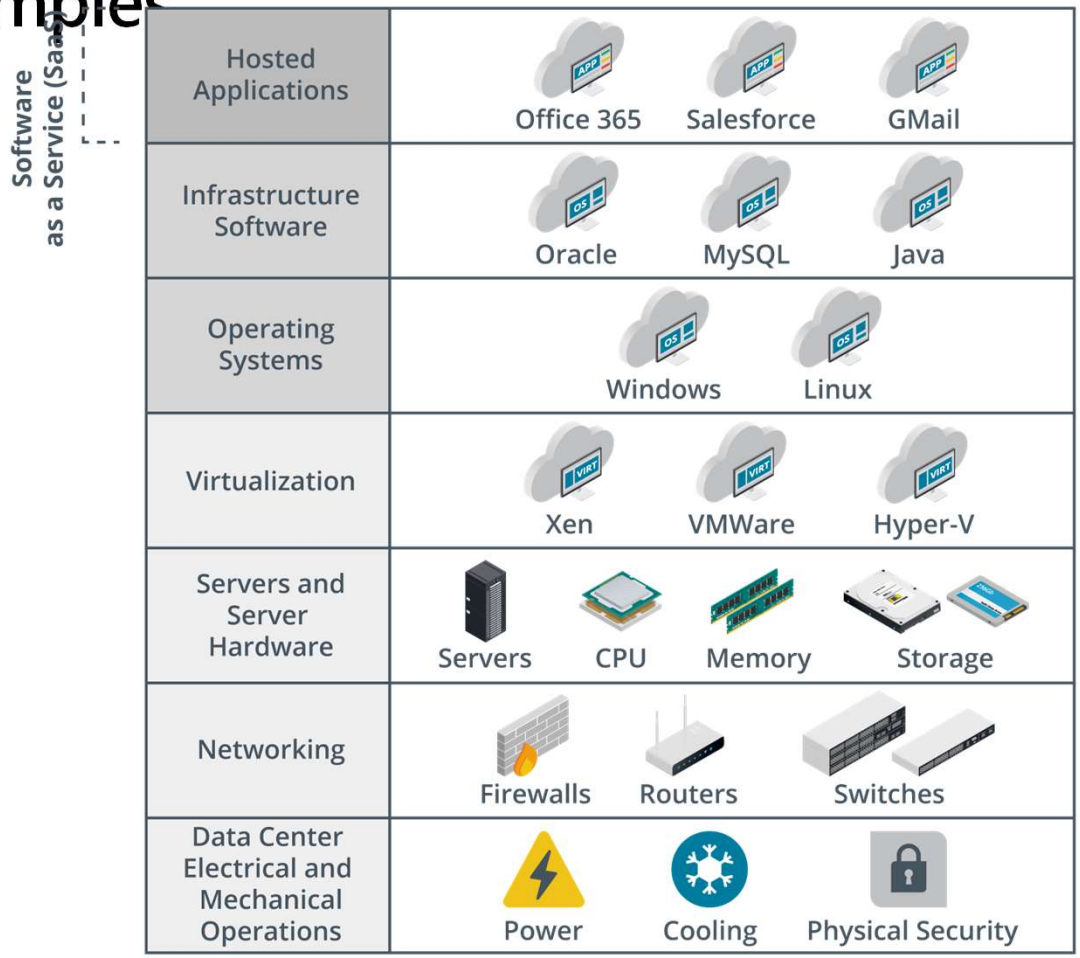
Software as a Service (SaaS)

- Consumer has direct use of software across a network.
- Cloud service provider retains responsibility for the underlying hardware, operating system, and patches.
- Usually licensed via subscription.
- Very high adoption rate.

- Costing: Cheapest among all. Pay per resource Utilization. Don't expect 24/7
- Target audience: End users

Software as a Service Examples

- AWS SaaS Factory
- Dropbox
- Google Kubernetes Engine Autopilot
- Google Onlooker
- Microsoft Office 365
- Netflix
- Redhat Insights
- WebEx

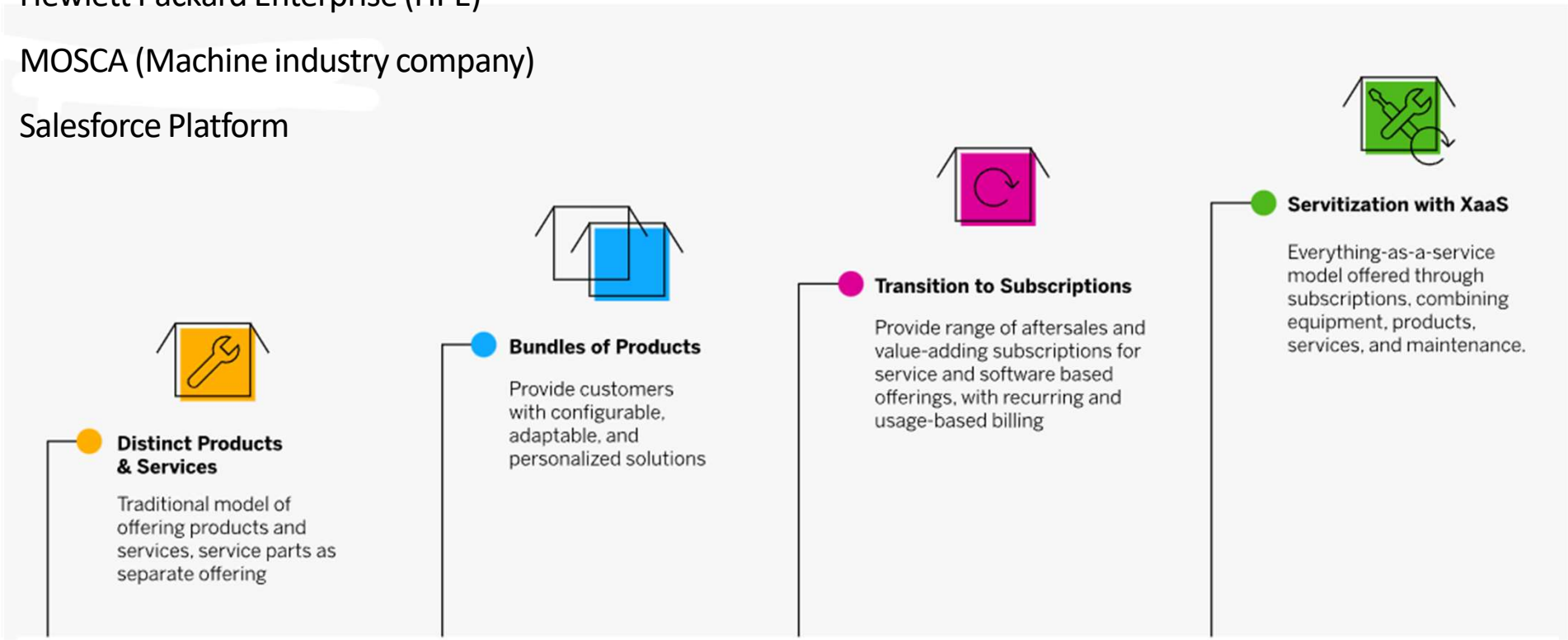


Anything as a Service (XaaS) Or Everything-as-a-Service

- Include SaaS, PaaS and IaaS
- Catch-all phrase for any technology solutions that are moved to the cloud or that exhibit the same pay-as-you-go subscription model as the three primary cloud service models.
- Delivery of various services, applications, and resources over the internet

Anything as a Service Examples

- Apache Stratos
- Hewlett Packard Enterprise (HPE)
- MOSCA (Machine industry company)
- Salesforce Platform



Reviews

Five cloud characteristics

On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measure services

Four service models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Anything as a Service (XaaS)

Reviews (continued)

Four cloud deployment models

- Private cloud
- Public cloud
- Community cloud
- Hybrid

Shared responsibility model

- Cloud service provider secures the hosting data centers
- Consumer secures the data within the cloud

Activity

Q1. Which statement describe On-demand self-service?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q1. Which statement describe On-demand self-service?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q2. Which statement describe Resource pooling?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q2. Which statement describe Resource pooling?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q3. Which statement describe Rapid Elasticity?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q3. Which statement describe Rapid Elasticity?

A. Metering of resources is monitored, controlled and billable.

B. Consumers can provision resources as needed and automatically

C. The cloud service provider pools resources in a multitenant model and adjusts resources allocation on consumer's needs

D. Services are available across the network from commonly available clients

E. Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual

Activity

Q4. Which are the primary cloud service models ? [Choose two]

A. Software-as-a-Service

B. Private cloud

C. Public cloud

D. Anything-as-a-Service

E. Platform-as-a-Service

Activity

Q4. Which are the primary cloud service models ? [Choose two]

A. Software-as-a-Service

B. Private cloud

C. Public cloud

D. Anything-as-a-Service

E. Platform-as-a-Service

Activity

Q5. What are the responsibilities in shared security model ? [Choose two]

A. Customers are responsible for network security

B. Customers are responsible for data security

C. Customers are responsible for data center security

D. Cloud Service Providers are responsible for network security

E. Cloud Service Providers are responsible for data security

Activity

Q5. What are the responsibilities in shared security model ? [Choose two]

A. Customers are responsible for network security

B. Customers are responsible for data security

C. Customers are responsible for data center security

D. Cloud Service Providers are responsible for network security

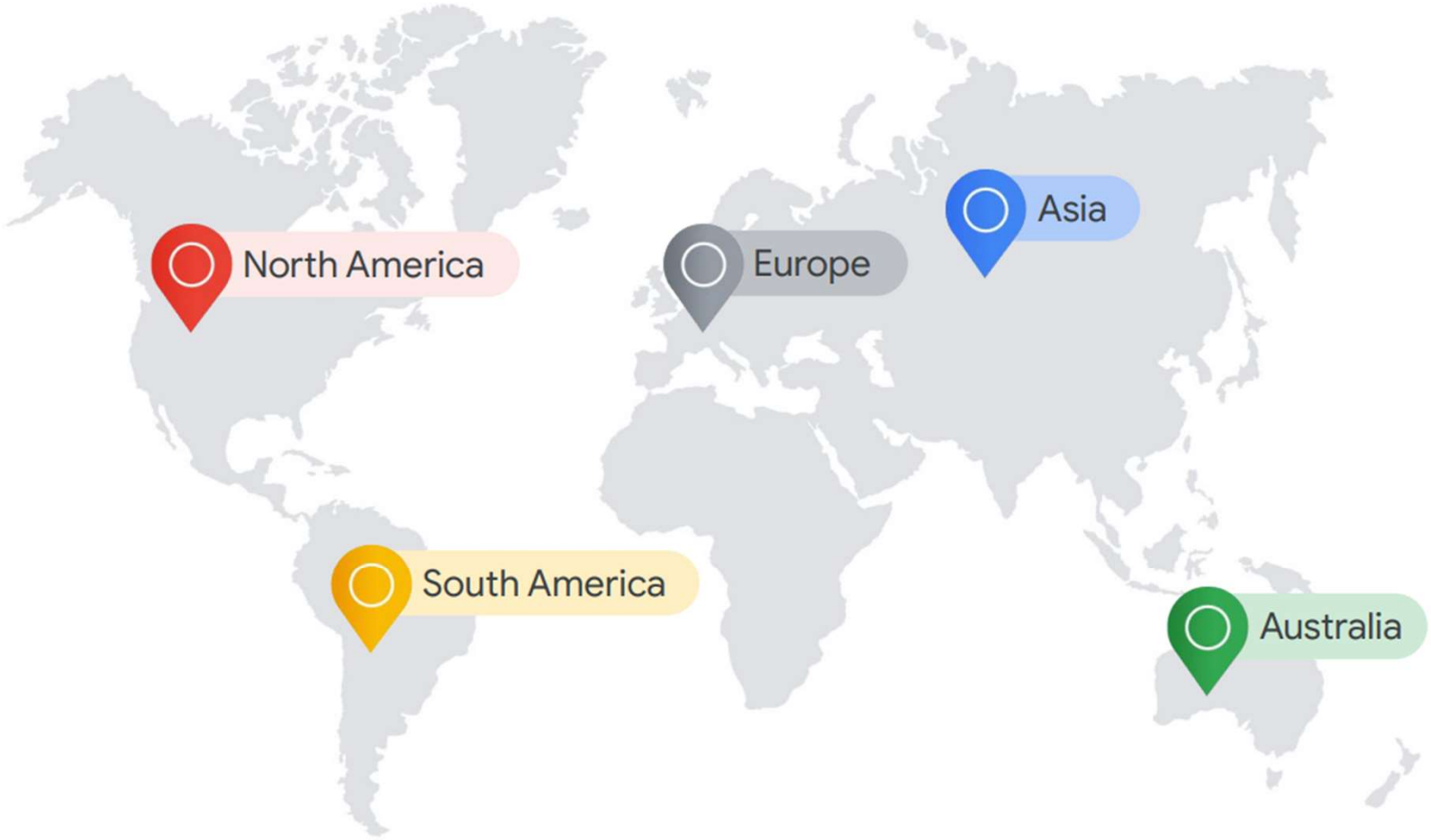
E. Cloud Service Providers are responsible for data security

Continue or Break?

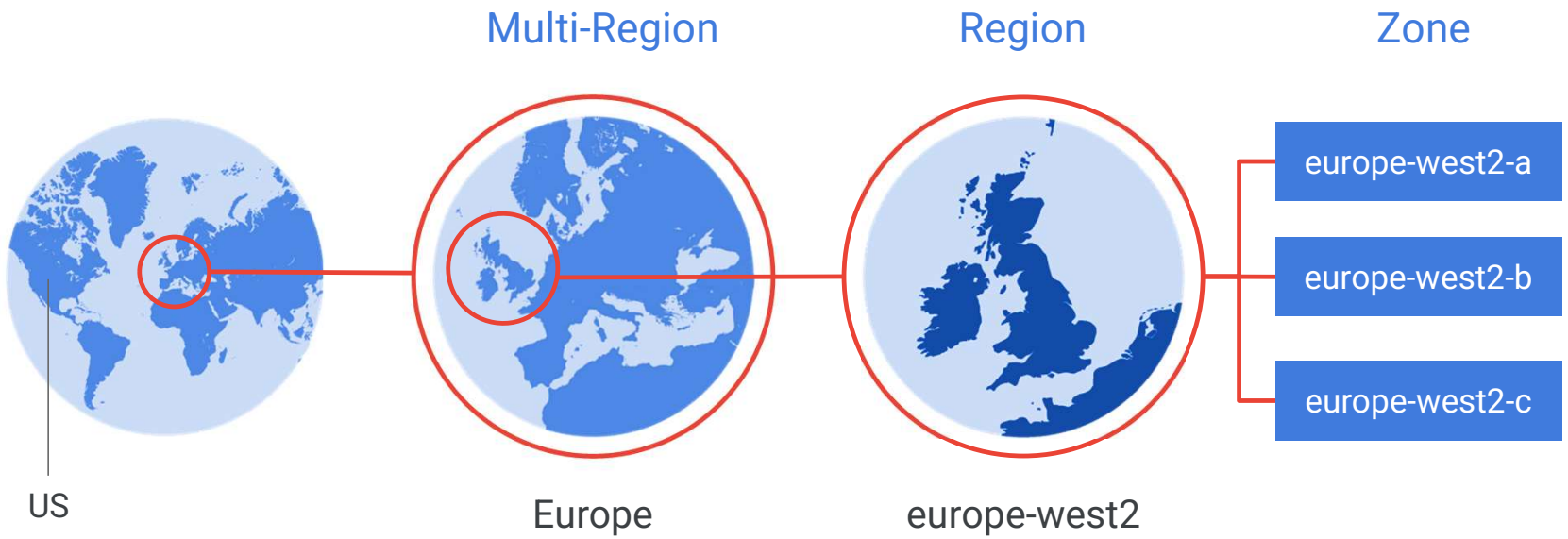
Cloud Provider Infrastructures

Cloud are designed for high throughput

Infrastructure locations



Geographic locations contain regions and zones



Azure Regions and Zones

Azure offers more global regions than any other cloud provider with 60-plus regions representing over 140 countries

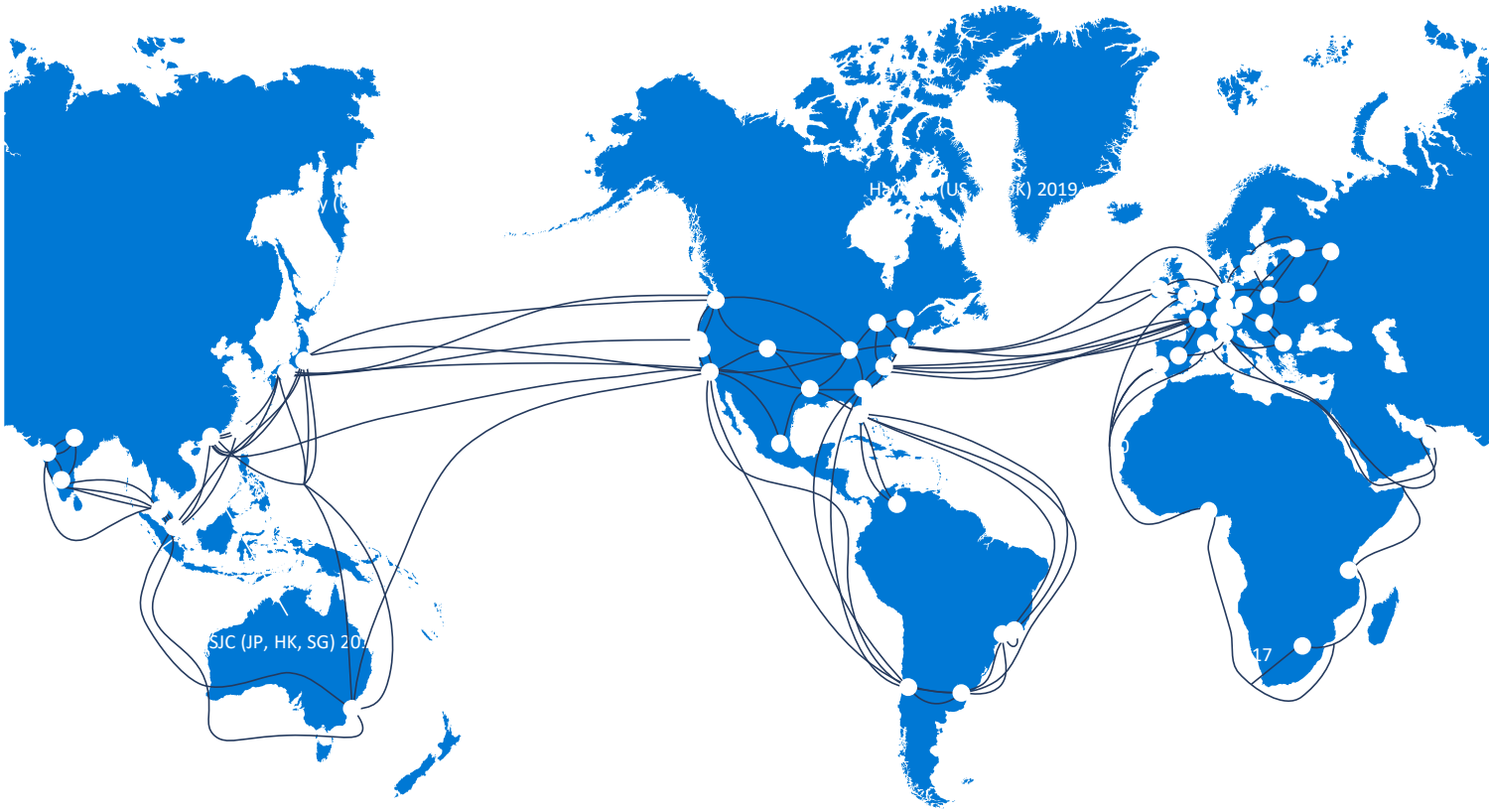
- **Regions are made up of one or more datacenters in close proximity.**
- **They provide flexibility and scale to reduce customer latency.**
- **Regions preserve data residency with a comprehensive compliance offering.**

Google Cloud Platform

24-29 Regions
134 points of presence and
13 subsea cable investments
around the globe

Edge points of presence

Network



Google is committed to environmental responsibility

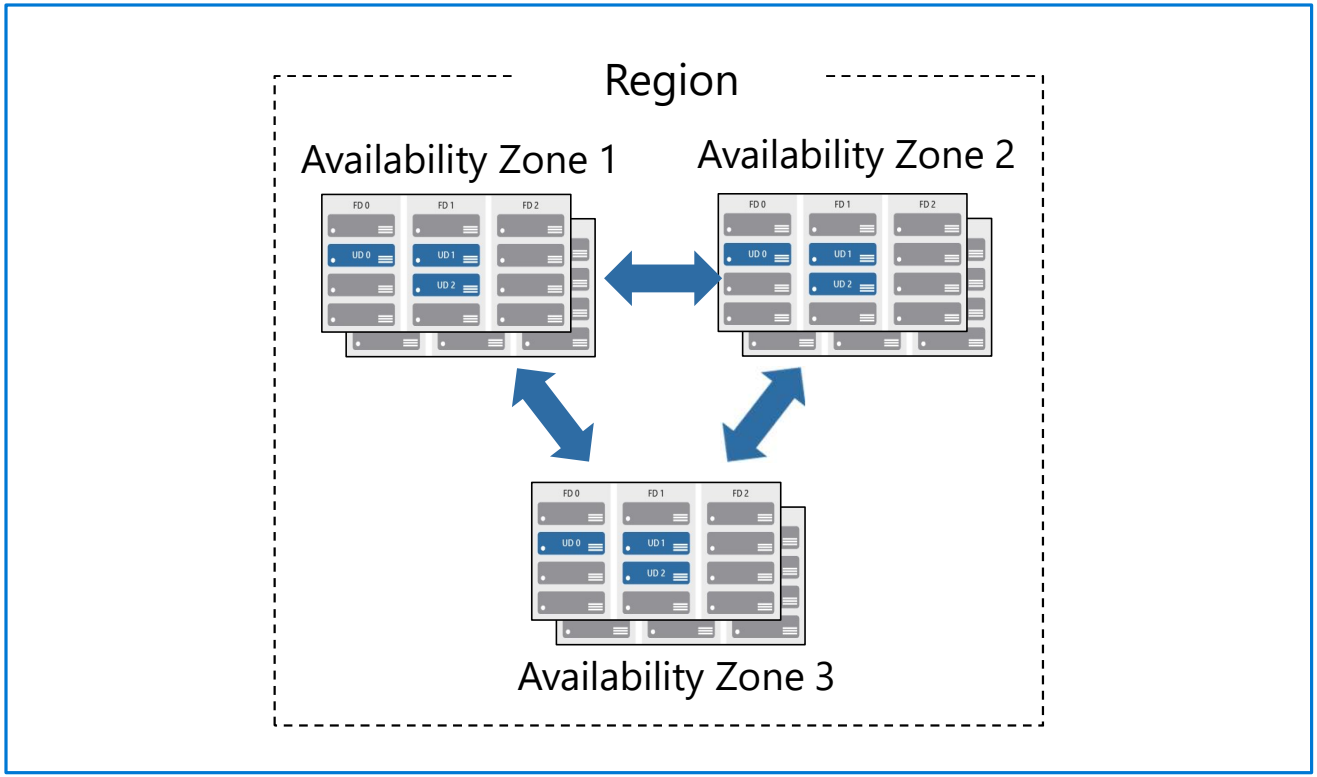
100% carbon neutral since 2007

One of the world's largest corporate purchasers of renewable energy

First data centers to achieve ISO 14001 certification

Availability zones

- Provide protection against downtime due to datacenter failure.
- Physically separate datacenters within the same region.
- Each datacenter is equipped with independent power, cooling, and networking.
- Connected through private fiber-optic networks.



Azure Region pairs / GCP Multi-Regions

- At least 300 miles of separation between region pairs.
- Automatic replication for some services.
- Prioritized region recovery in the event of outage.
- Updates are rolled out sequentially to minimize downtime.

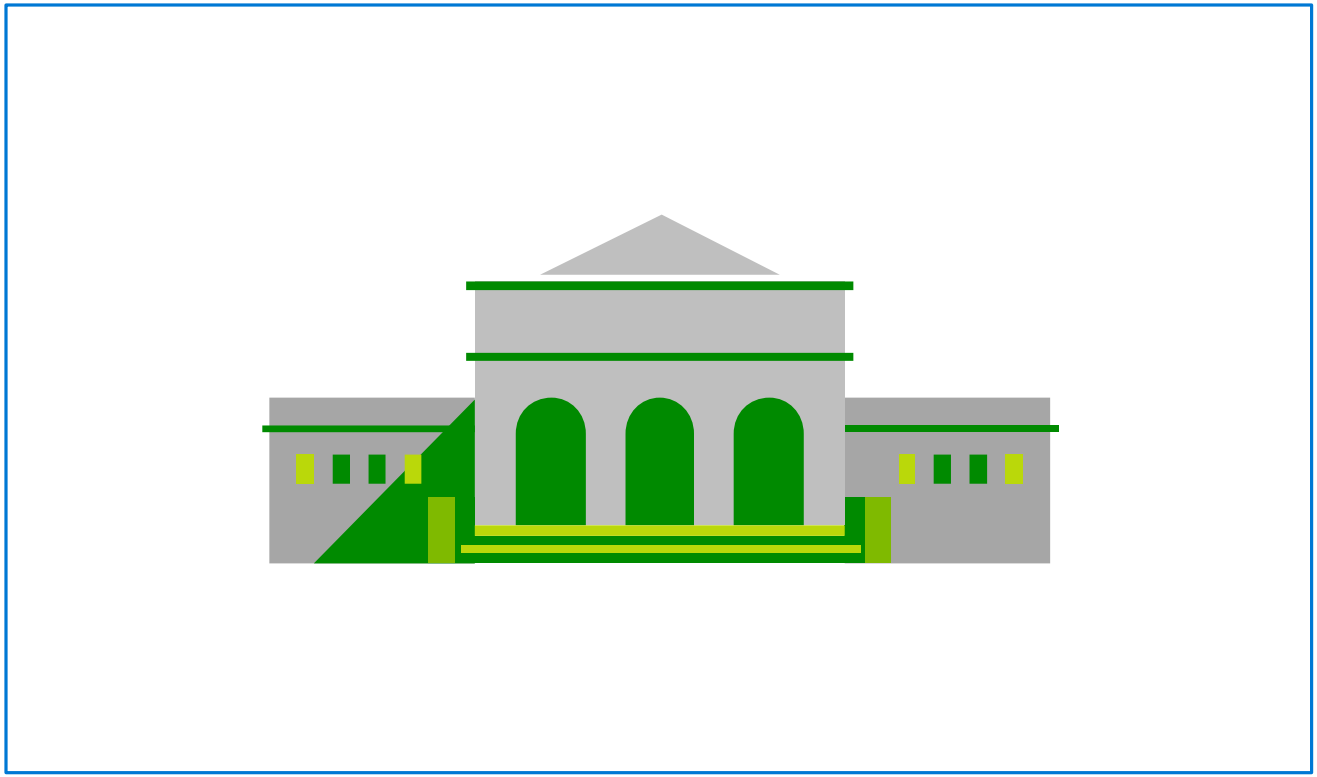
Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US

Azure sovereign regions (US government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.

Azure government:

- Separate instance of Azure.
- Physically isolated from non-US government deployments.
- Accessible only to screened, authorized personnel.



Azure sovereign regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet.
- All data stays within China to ensure compliance.

AWS (China) Accounts

A set of credentials that are distinct and separate from AWS global accounts

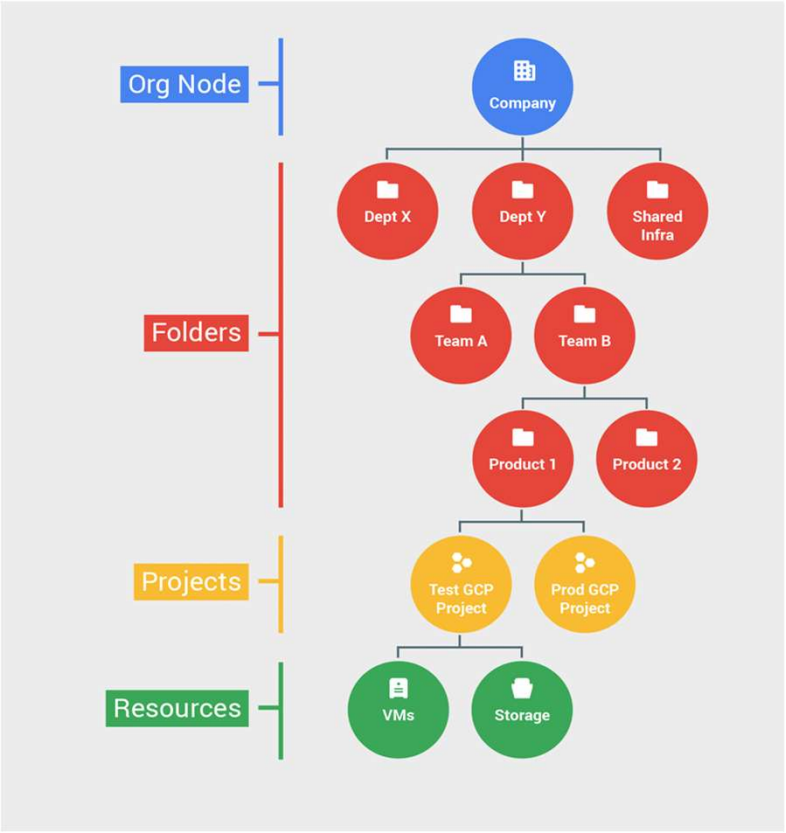
Azure China features:

- Physically separated instance of Amazon web services operated by Sinnet (in Beijing) or NWCD (Ningxia region).
- All data stays within China to ensure compliance.

Getting Started with GCP/Azure

Resource hierarchy levels define trust boundaries

- Group your resources according to your organization structure.
- Levels of the hierarchy provide trust boundaries and resource isolation.



Sign up Accounts

- Company Account
- Free/Personal account
- Free student account
- Microsoft Learn sandbox
- Google Skills Boost
- AWS Skills Guild

Personal Free Accounts

Google Cloud Platform (GCP)

Free Tier: All Google Cloud customers can use select Google Cloud products—like Compute Engine, Cloud Storage, and BigQuery—free of charge, within specified monthly usage limits.

Azure

Free monthly amounts of 25+ popular services for 12 months (new Azure customers only)

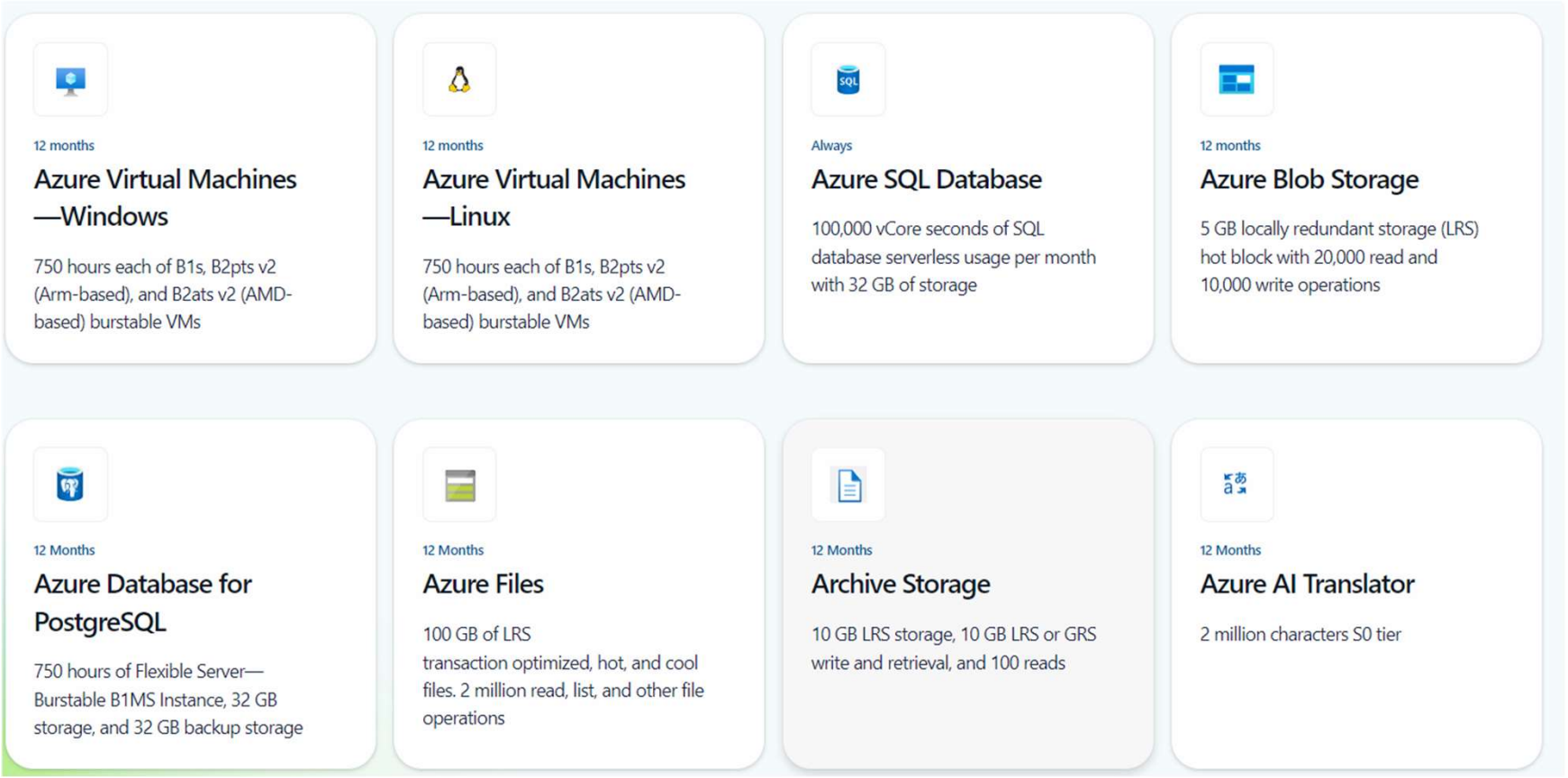
Free monthly amounts of 55+ always-free services

Access to full catalog of services up to free amounts and USD200 credit

Spending protection—credit card won't be charged*

No upfront commitment—cancel anytime

Free Products/Services in Azure



Free Products/Services in GCP

Compute Engine

Scalable, high-performance virtual machines.

1 e2-micro instance per month

Cloud Storage

Best-in-class performance, reliability, and pricing for all your storage needs.

5 GB-months Standard Storage

BigQuery

Fully managed, petabyte scale, analytics data warehouse.

1 TB queries per month

Google Kubernetes Engine

One-click container orchestration via Kubernetes clusters, managed by Google.

One Autopilot or Zonal cluster per month

Cloud Run

A fully managed environment to run stateless containers, build apps, or host and deploy websites.

2 million requests per month

Cloud Build

Fast, consistent, reliable builds on Google Cloud.

120 build-minutes per day

Operations (formerly Stackdriver)

Monitoring, logging, and diagnostics for applications on Google Cloud.

Monthly allotments for logging and monitoring

Firestore

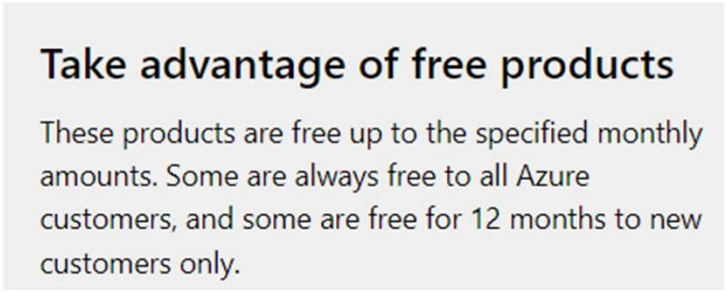
NoSQL document database that simplifies storing, syncing, and querying data for apps.

1 GB storage

Azure for Students

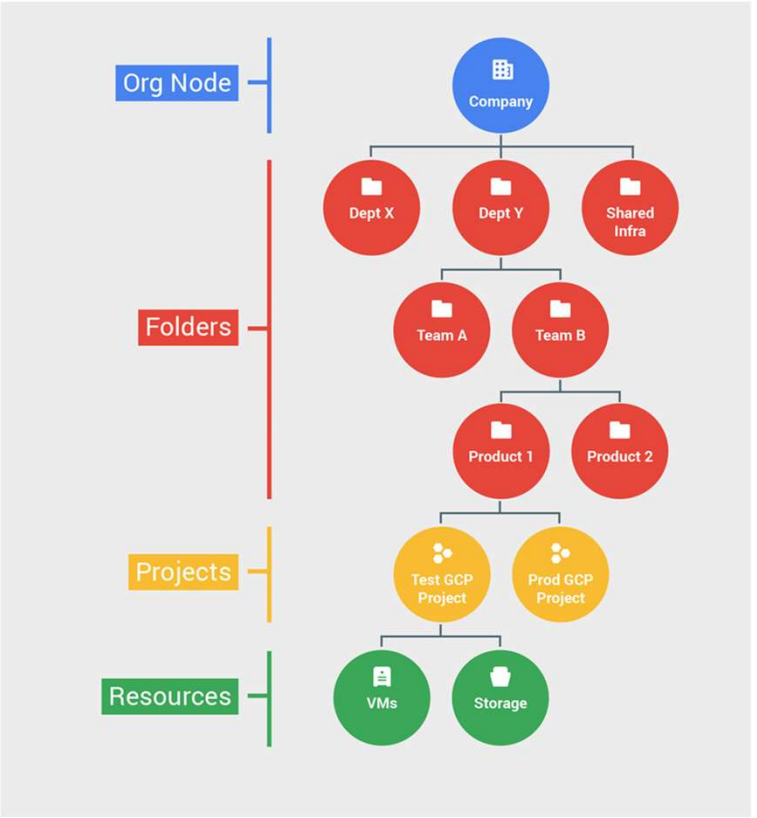
- Start with $100 credit
- No credit card required
- Free Services similarly offered in Personal Account

https://azure.microsoft.com/en-us/free/students



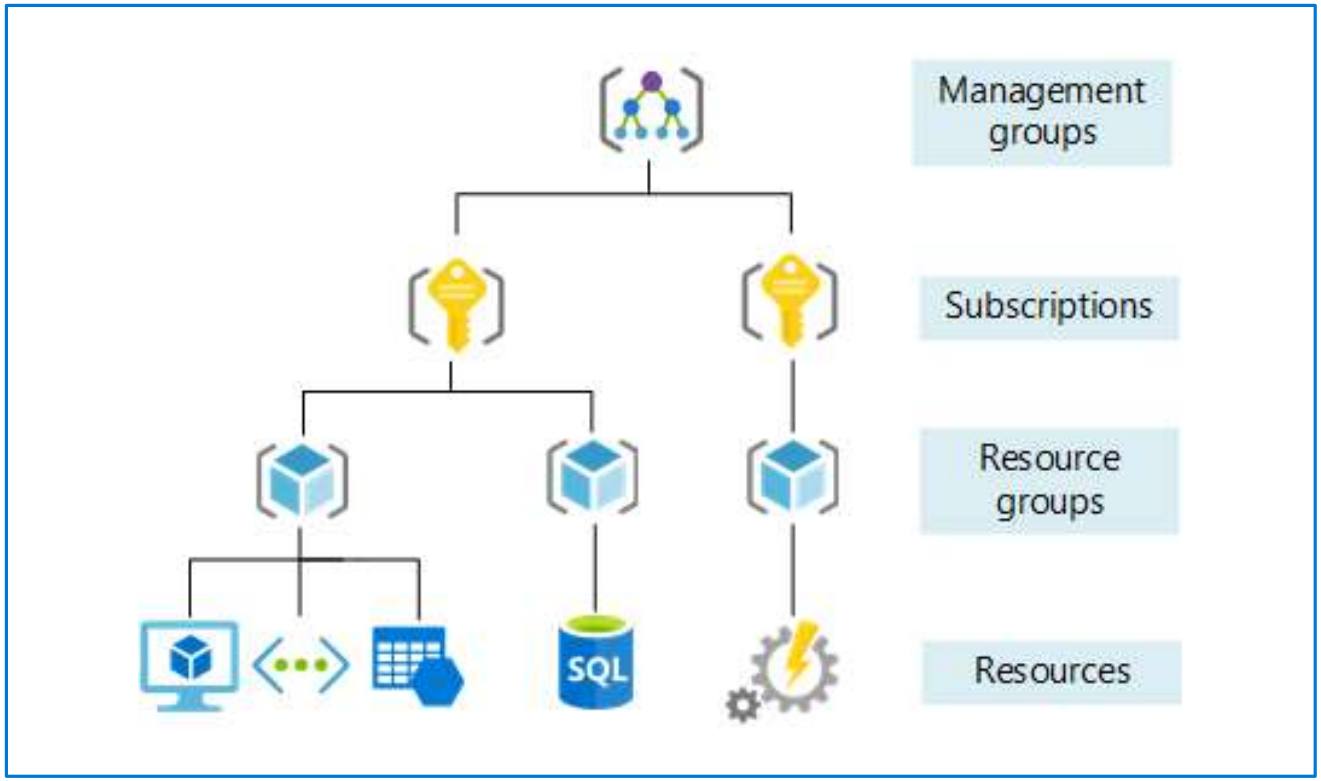
Resource Management

- Group resources according to organization structure
- Levels of hierarchy provide trust boundaries and resource isolation



Management groups

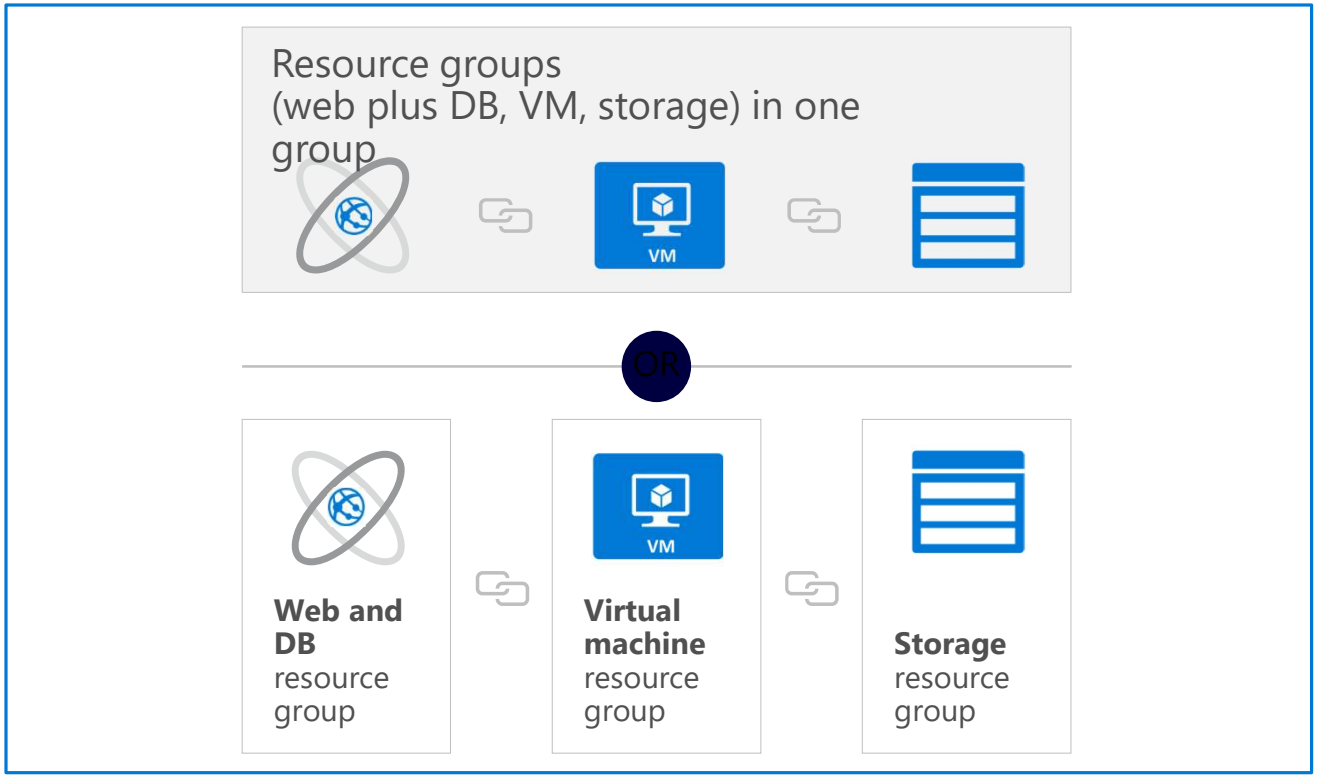
- Management groups can include multiple Azure subscriptions.
- Subscriptions inherit conditions applied to the management group.
- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth.



Resource groups

A **resource group** is a container you use to manage and aggregate resources in a single unit.

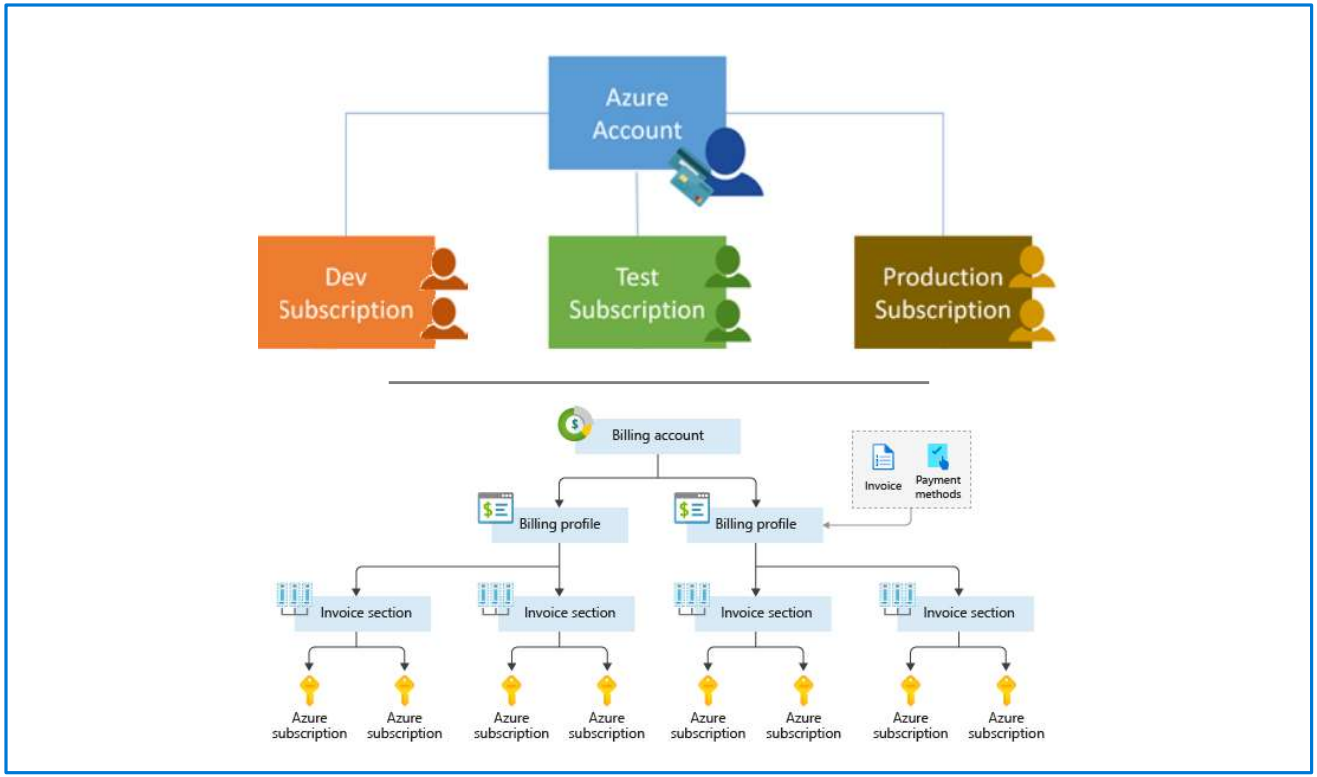
- Resources can exist in only one resource group.
- Resources can exist in different regions.
- Resources can be moved to different resource groups.
- Applications can utilize multiple resource groups.



Azure subscriptions

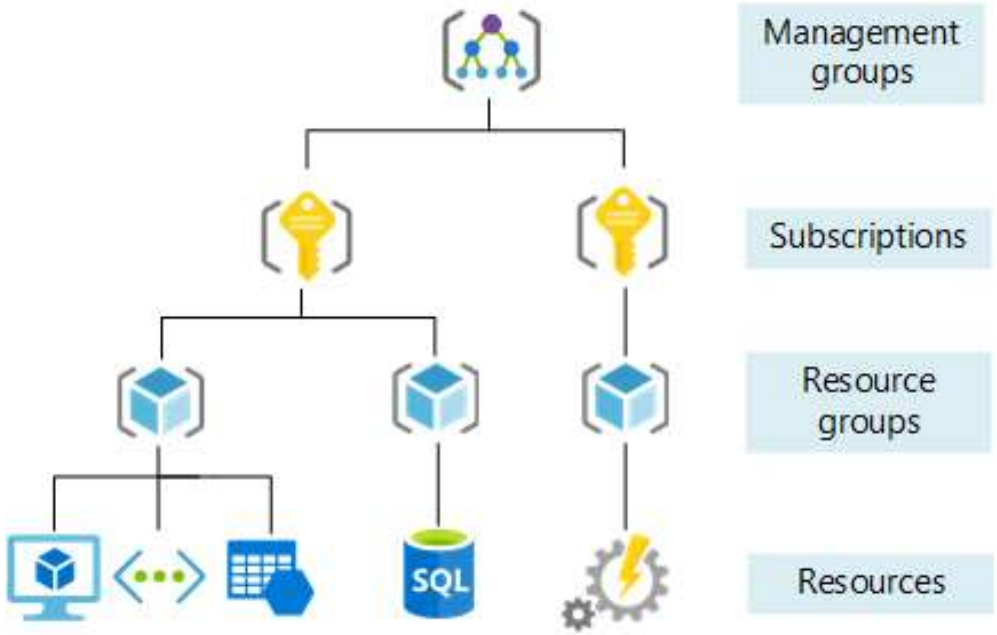
An Azure subscription provides you with authenticated and authorized access to Azure accounts.

- **Billing boundary: Generate separate billing reports and invoices for each subscription.**
- **Access control boundary: Manage and control access to the resources that users can provision with specific subscriptions.**



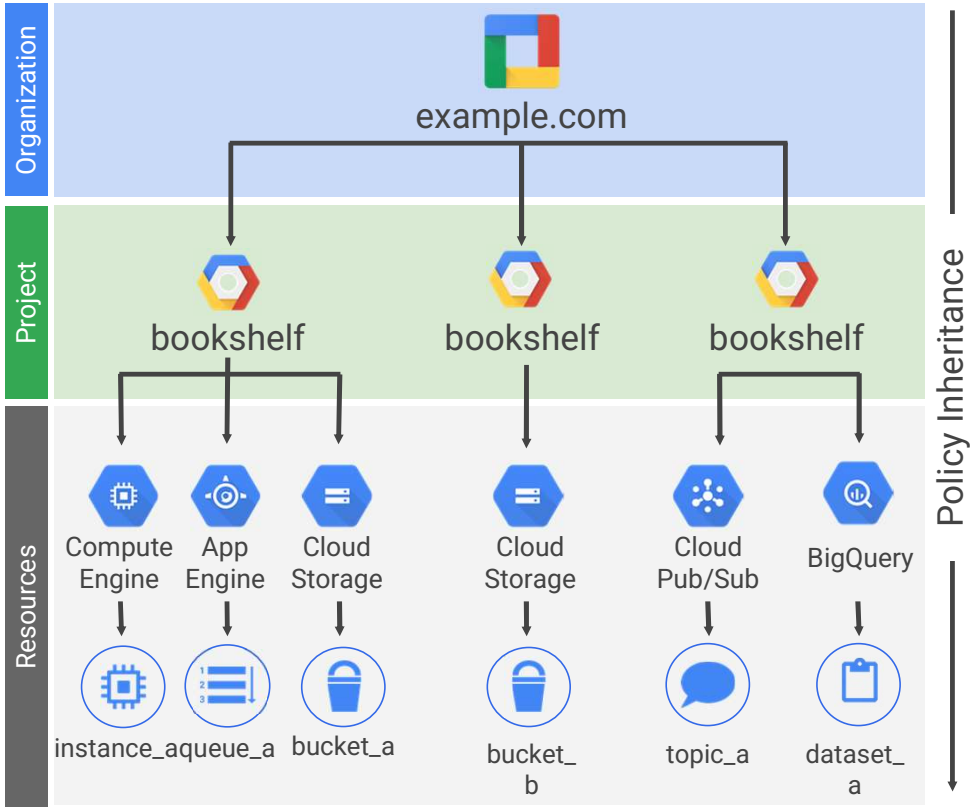
Google Project or Azure Subscription

- Track resource and quota usage.
- Billing boundary.
- Access control boundary:
  - Manage permissions and credentials.
- Enable services and APIs.



An example IAM resource hierarchy

- A policy is set on a resource.
  - Each policy contains a set of roles and role members.
- Resources inherit policies from parent.
  - Resource policies are a union of parent and resource.
- A less restrictive parent policy overrides a more restrictive child policy.



What can you use to manage your administrative users?

Gmail accounts and Google Groups

G Suite / Workspace

Cloud Identity

On-prem Active Directory

Azure Active Directory

Microsoft Entra ID

SalesForce

Amazone Workspaces

Office 365

Vmware Workspace ONE

Compute services

Compute Services

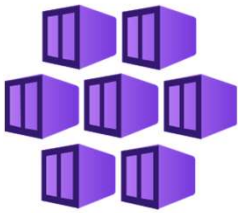
- is an on-demand service that provides computing resources such as disks, processors, memory, networking, and operating systems.
- Processors : vCPU
- Memory
- Ephemeral or Persistent Disks: Standard HDD, SSD, Ultra-SSD
  Snapshots or Dynamically increase disk size
- Virtual Network Interfaces (vNIC)
- OS : Linux / Windows and etc
- Can be part of IaaS, PaaS, SaaS or Serverless

Azure Compute services

Virtual Machines

App Services

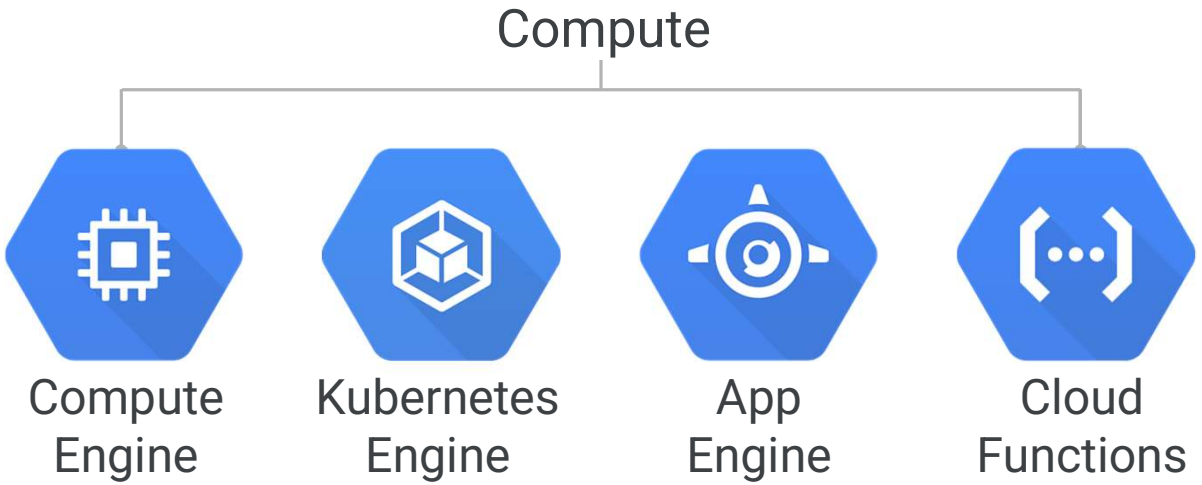
Container Instances



Azure Kubernetes Services (AKS)

Azure Virtual Desktop

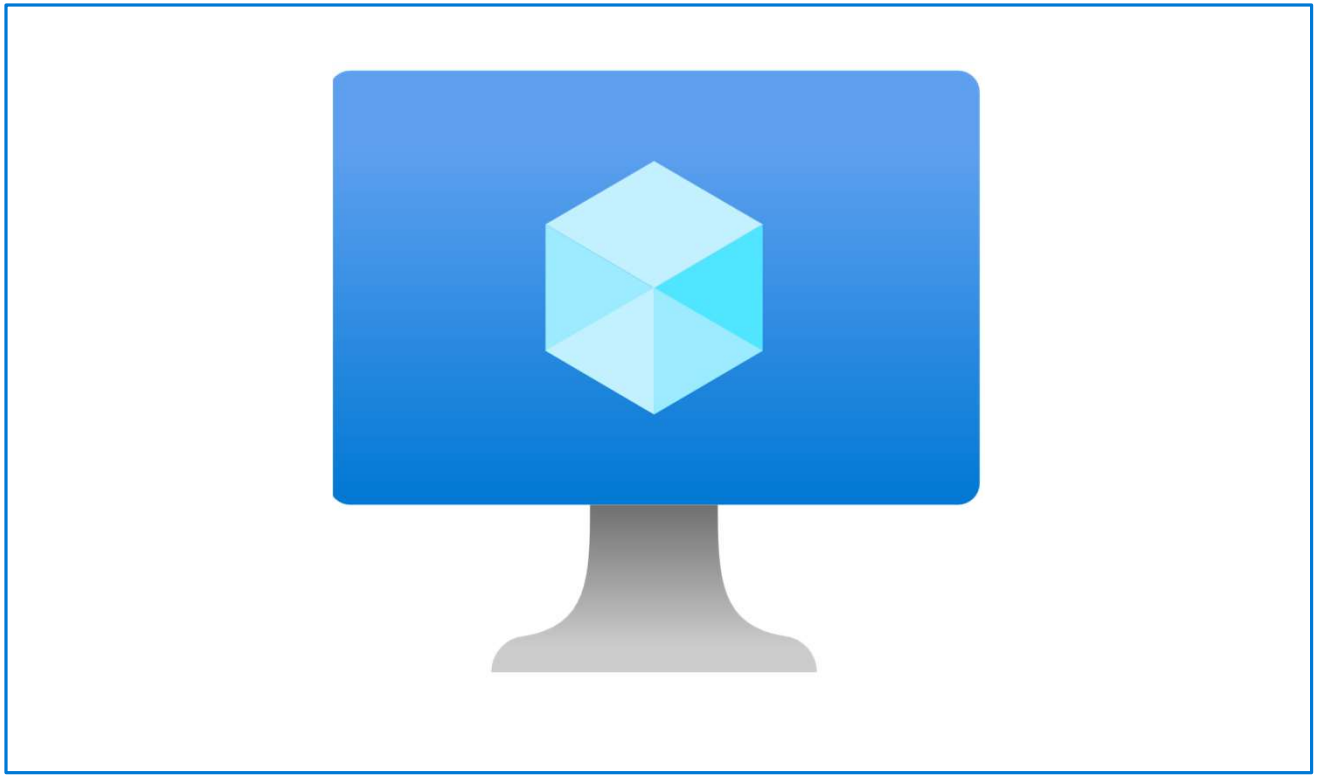
GCP Compute services



Virtual machines (aka instances)

virtual machines (VMs) are software emulations of physical computers.

- **Includes virtual processor, memory, storage, and networking.**
- **IaaS offering that provides total control and customization.**



Scale up or scale out with Compute services

Use big VMs for memory- and compute-intensive applications

Use Autoscaling for resilient, scalable applications

Compute services offers customer friendly pricing

- Per-second billing, sustained use discounts, committed use discounts

  Reserved Instances discount (1 or 3 years)
- Preemptible / SPOT instances
- High throughput to storage at no extra cost
- Custom machine types: Only pay for the hardware you need

Compute services as PaaS

Azure

Azure Container Instances: A PaaS offering that runs a container or pod of containers in Azure.

Azure Container Apps: A PaaS offering, like container instances, that can load balance and scale.

Azure Kubernetes Service: Container Orchestration based on k8s

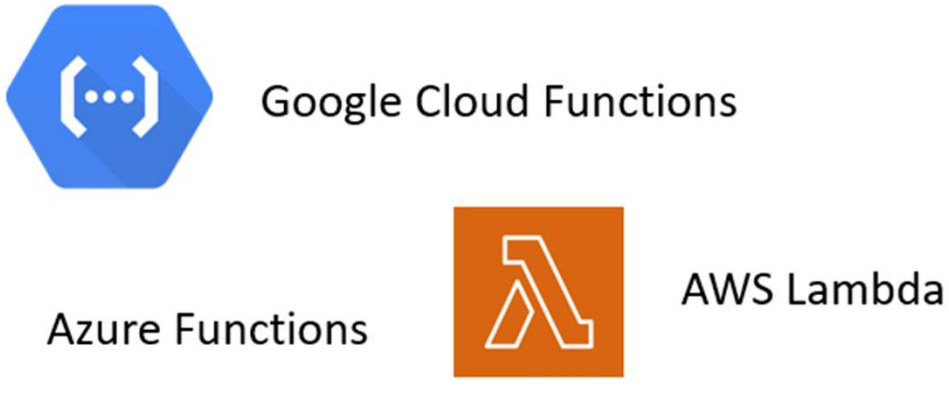
Google Cloud

Google Kubernetes Engine: Container Orchestration based on k8s

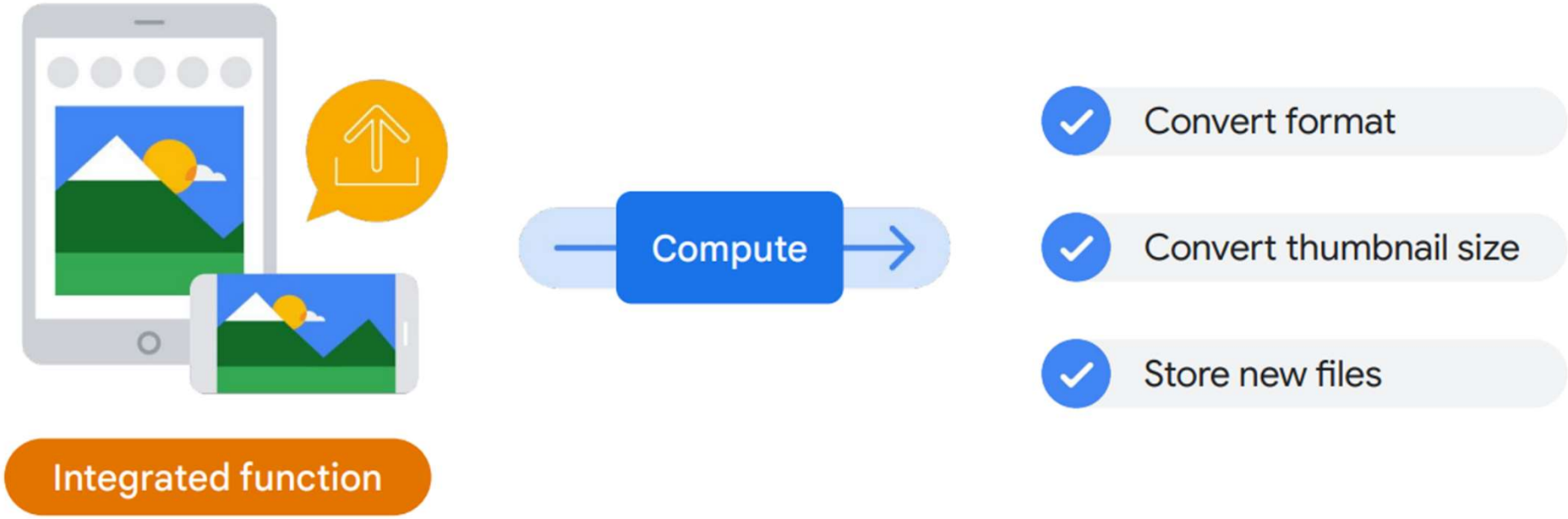
Google Cloud Run: fully managed platform that enables you to run your code directly on top of Google's scalable infrastructure

Function as a Service (FaaS)

- PaaS offering that supports serverless compute operations
- Event-based code runs when called / triggered . Without requiring user/admin intervention
- Supports modern programming languages: Node.js, Python, Go, PHP, Java, .Net, Ruby
- Seamless integration with Queueing platform: SNS/SQS, Pub/Sub, Azure Event hub ,Kafka
- Seamless integration with Storage services : Azure Blob, Google Cloud Storage, AWS S3



Function as a Service (FaaS) – Case Use



App Services / App Engines

- Optimized for dynamic web applications
- PaaS offering with enterprise-grade, performance, security, and compliance requirements
- Fully managed platform to build, deploy, and scale web apps and APIs quickly
- Works with .NET, Node.js, Java, Python or PHP

Azure App Service

Google App Engines

AWS Elastic Beanstalk

Salesforce Heroku

Networking services

Networking Capabilities

- **Networking Foundation** : provide core connectivity for resources
- **Load Balancing and Content Delivery** : allow for management, distribution, and optimization of your applications and workloads
- **Hybrid Connectivity** : provide secure communication to and from your resources in cloud provider network to on-premises network - VPN Gateway, Direct physical fiber connections, Virtual WAN, and Peering Service.
- **Network Security** : protect your web applications and IaaS services from DDoS attacks and malicious actors

Networking Foundation

- Provide core connectivity for your resources in virtual private cloud network
- VPC-network or vNET is the fundamental building block for private network in cloud provider data centers

✓ Communication between Cloud resources (between VM and VM | between VM and Storage resource | between Storage and Kubernetes containers)

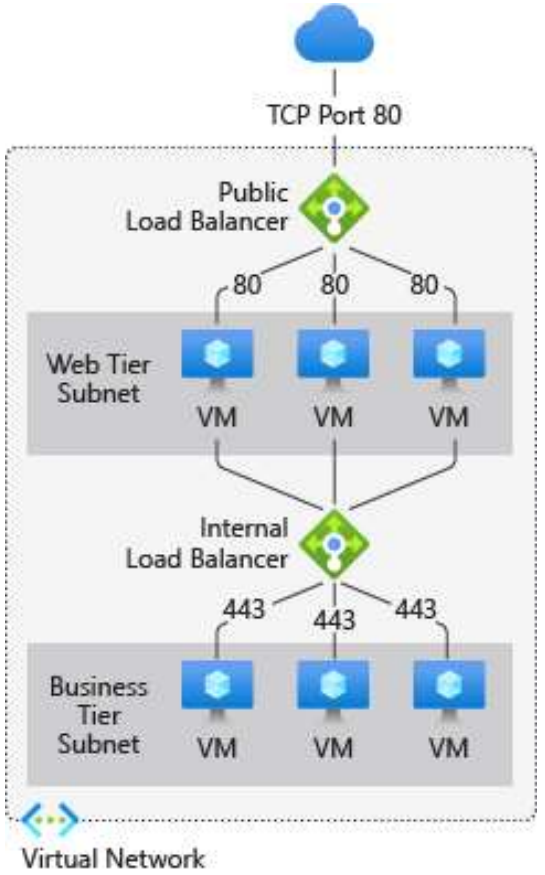
✓ Communication between network (VPC Peering or VPC Sharing)

✓ Communication to the Internet

✓ Communication with on-prem networks (Hybrid)

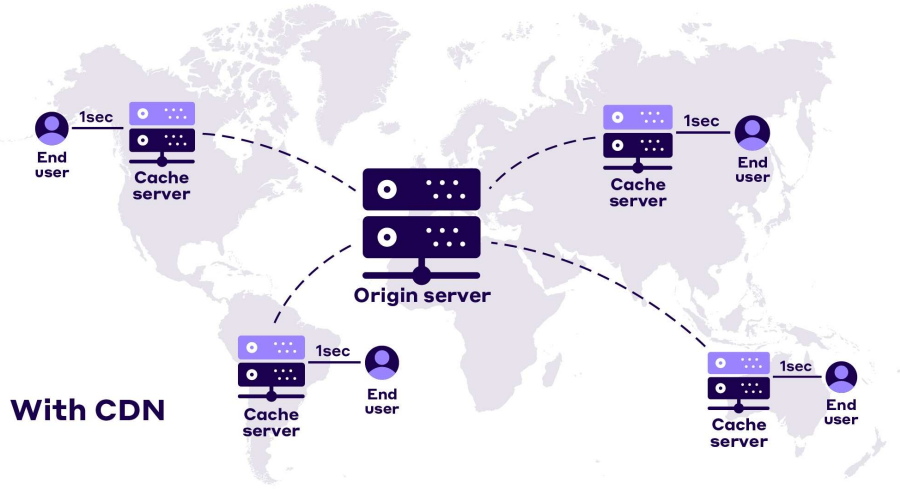
Load Balancing

- Provides high-performance, low-latency Layer 4 load-balancing for all UDP and TCP protocols.
- Enables traffic management to your web application requirements (URL MAP, Route-based rules)
- Type: Internal | Regional | Global



Content Delivery Network (CDN)

- is a globally distributed network of servers that can efficiently deliver web content to consumers.
- Bring user data closer to them
- Protect apps, websites from cyberthreats



Hybrid Connectivity

- VPN : create encrypted cross-premises connections to virtual private cloud networks or create encrypted connections between VPC/VNET, or cross-cloud connections

✓ Site-to-Site VPN

✓ Point-to-Site

- Physical dedicated fiber connection between virtual private cloud networks and customer on-prem networks,

✓ Google Cloud Interconnect, Azure ExpressRoute, AWS Direct Connect

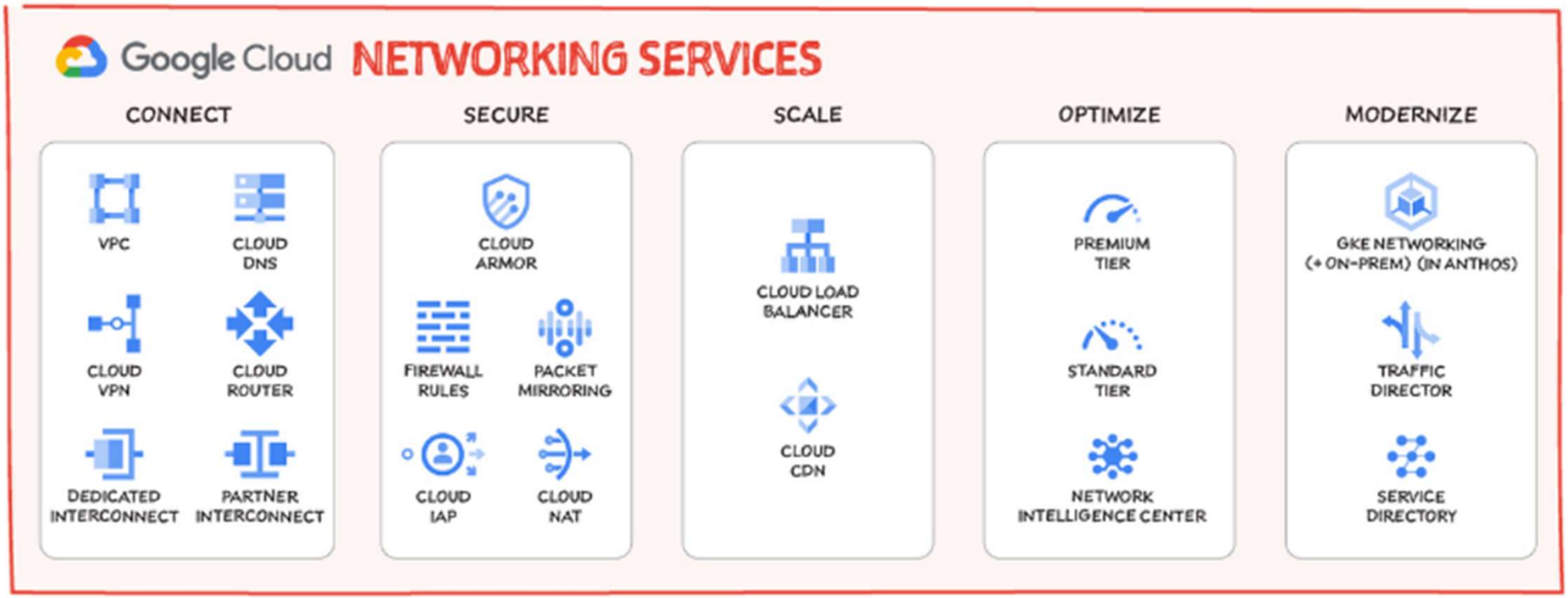
Network Security

- Firewall Rules or Policies : Allow / Deny network traffic according to ip-ranges, protocols, port numbers
- Security Groups : Allow / Deny network traffic according to applications / network-tags
- DDoS-protection: Mitigation techniques against Distributed Denial of Service attacks
- Network Virtual Appliances: IDS, Network Inspection Engines, Forensic Software,
- Port Mirroring : Create redundant copies of resources traffic to be monitor
- VPN : Virtual Private Network enables secure, using only private IP connect to on-prem networks
- Web Application Firewall (WAF) : provides protection to your web applications from common web exploits and vulnerabilities such as SQL injection, and cross site scripting.

DNS service

- 100% uptime, fully managed service
- Create managed zones, then add, edit, delete DNS records
- Programmatically manage zones and records using RESTful API or command-line interface
- Permission control thru IAM
- Fully integrated with resources monitoring and logging
- Fully customized domain names, records management

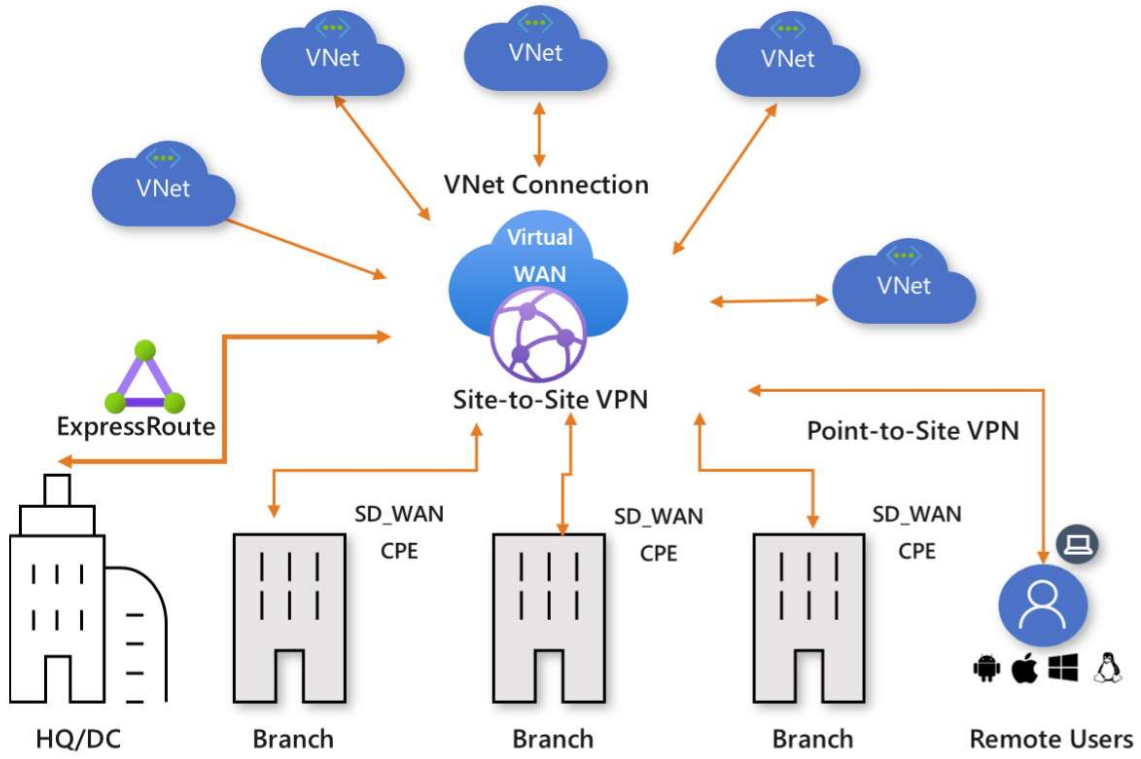
Google Networking services



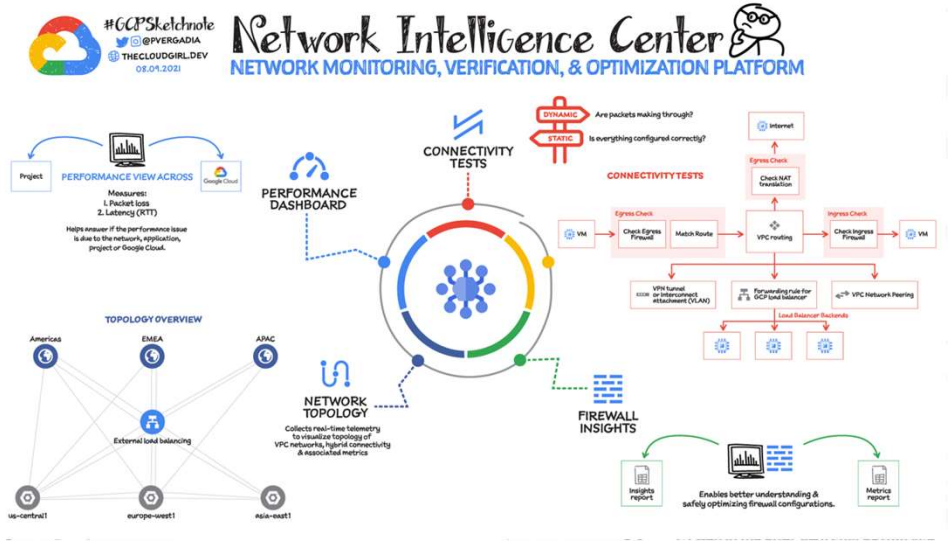
Azure Virtual WAN

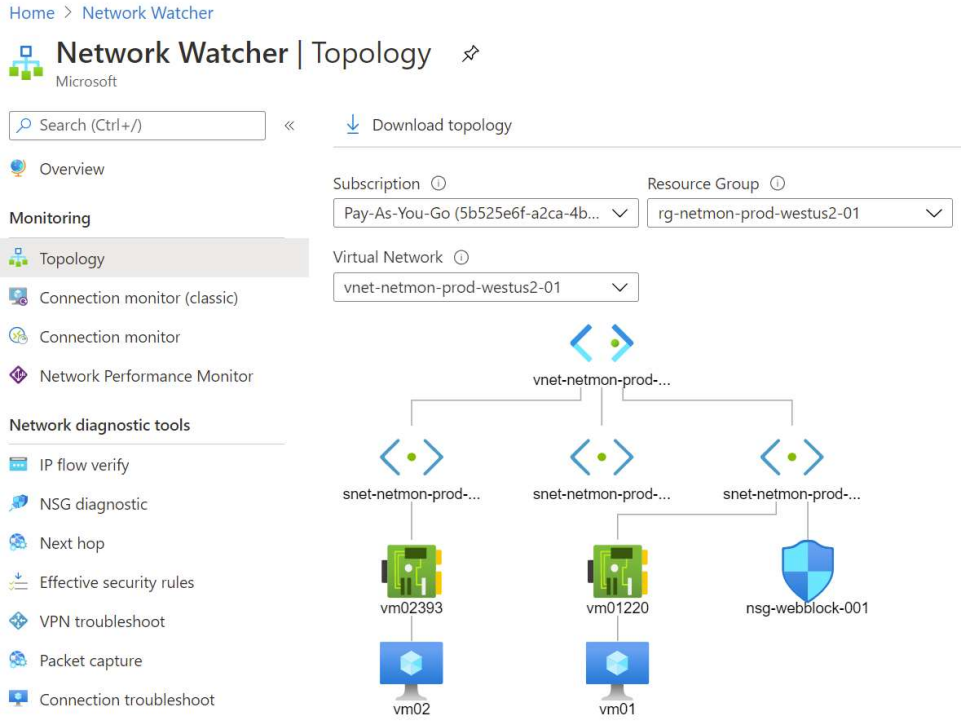
Single operational interface mana

- Branch connectivity
- Site-to-site VPN
- Remote user VPN
- ExpressRoute
- Intra-cloud connectivity
- VPN ExpressRoute inter-connectivity
- Routing, Firewall, encryption



Network Monitoring services





Continue or Break?

Storage in the Cloud

Storage in the cloud

A service that you can use to store files, messages, tables, and other types of information

Durable, secure, scalable, managed, accessible

Storage for virtual machines, unstructured data and structured data

Two tiers: Standard (HDD magnetic drives) and Premium (SSD)

Azure storage services

Azure Blob: Optimized for storing massive amounts of unstructured data, such as text or binary data.

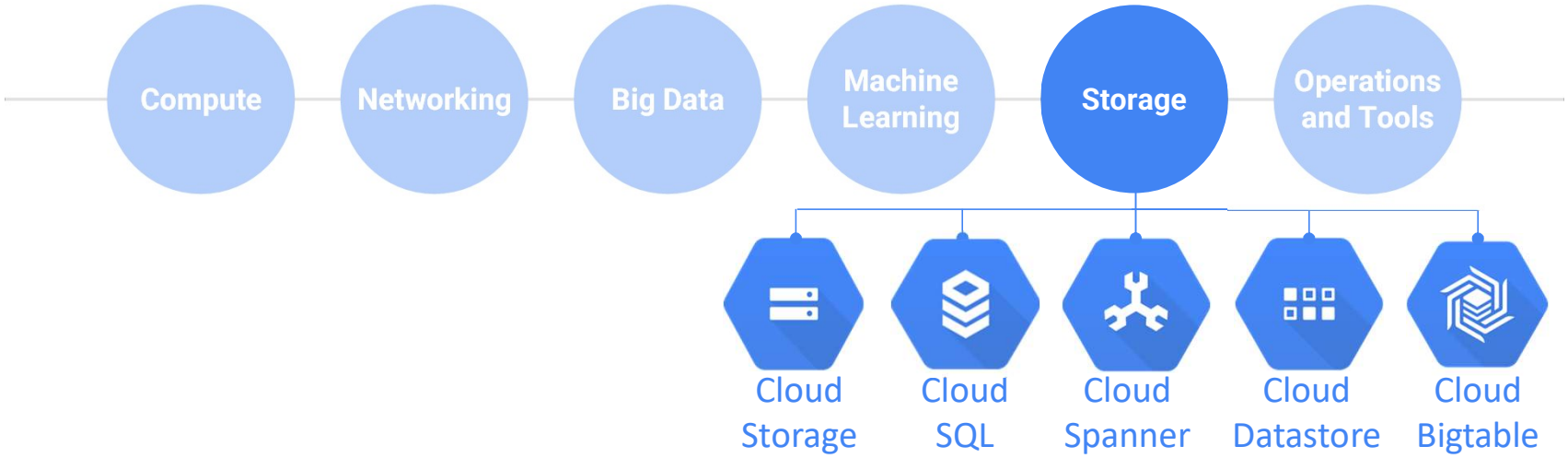
Azure Disk: Provides disks for virtual machines, applications, and other services to access and use.

Azure Queue: Message storage service that provides storage and retrieval for large amounts of messages, each up to 64 KB.

Azure Files: Sets up a highly available network file share that can be accessed by using the Server Message Block protocol.

Azure Tables: Provides a key/attribute option for structured nonrelational data storage with a schema-less design.

Google Cloud Platform



Storage access tiers

Hot	Cool	Cold	Archive
Optimized for storing data that is accessed frequently.	Optimized for storing data that is infrequently accessed and stored for at least 30 days.	Optimized for storing data that is infrequently accessed and stored for at least 90 days.	Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements.

File management options

Command line utility

- Copy blobs or files to or from your storage account.
- One-direction synchronization.
- AzCopy or gsutil

Graphical user interface

- Compatible with Windows, MacOS, and Linux.
- Easily click and drag or perform other tasks
- Azure Storage Explorer
- Google Cloud Storage Browser

File Synchronizer

- Synchronizes cloud and on-premises files in a bidirectional manner.
- Cloud tiering keeps frequently accessed files local, while freeing up space.
- Example: Azure File Sync, Resilio Connect, Linux rsync

Azure Storage Accounts Replication Strategies

Data Replication Options	Description
Locally redundant storage (LRS)	Data is replicated three times within a single facility in a single region
Zone-redundant storage (ZRS)	Data is replicated across multiple Availability Zones within one region
Geo-redundant storage (GRS)	Data is replicated three times within the primary region and replicated three times to the regions pair.
Read access geo-redundant storage (RA-GRS)	Data is replicated three times within the primary region and replicated with read-access to the region pair
Geo-zone-redundant storage (GZRS)	Data is replicated across three Availability Zones and replicated to the region pair
Read-access Geo-zone-redundant storage (RA-GZRS)	Data is replicated across three Availability Zones and replicated with read-access to the region pair

Azure Storage Account Kinds

Storage account type	Supported services	Supported tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
Storage (general purpose v1)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
StorageV2 (general purpose v2)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, GZRS RA-GZRS
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
File Storage	Files only	Premium	LRS, ZRS (limited regions)

All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest

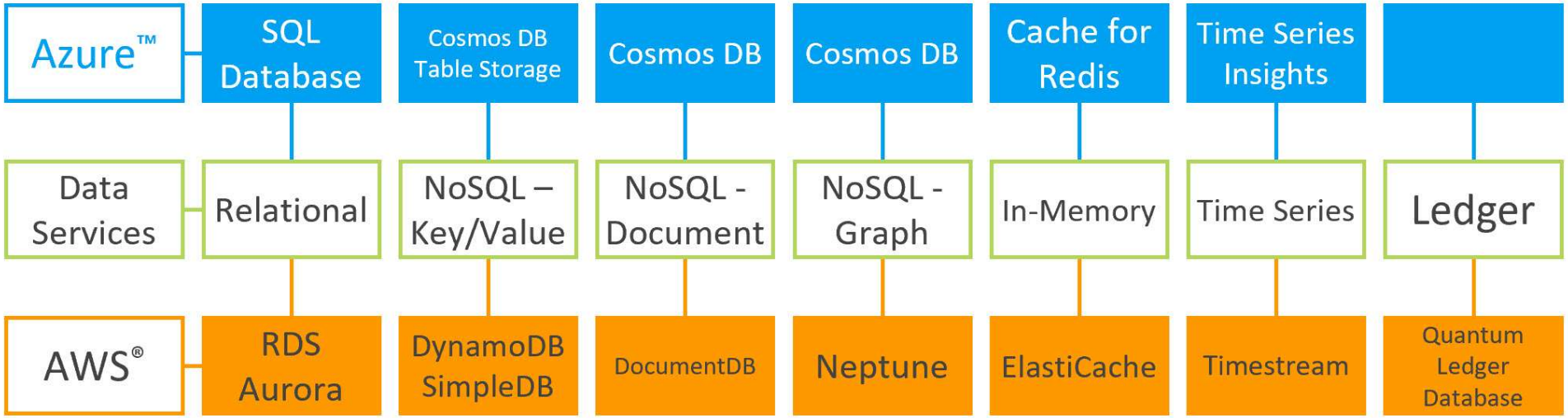
Database in the cloud

- A RDBMS (**relational database** management system)
- **NoSQL database** non-relational databases that store data in a non-tabular format, rather than in rule-based, relational tables like relational databases do.
- **In-Memory database** read and write data records straight in / out of physical memory
- A **time series database** (TSDB) is a database optimized for time-stamped or time series data. Typically used with IoT, Drones, small gadgets
- A **ledger database** is somewhat more modern and commonly refers to a type of database that uses cryptographic techniques, including blockchain, to secure data.

Google Database Systems

	Cloud Datastore	Cloud Bigtable	Cloud Storage	Cloud SQL	Cloud Spanner	BigQuery
Type	NoSQL document	NoSQL wide column	Blobstore	Relational SQL for OLTP	Relational SQL for OLTP	Relational SQL for OLAP
Transactions	Yes	Single-row	No	Yes	Yes	No
Complex queries	No	No	No	Yes	Yes	Yes
Capacity	Terabytes+	Petabytes+	Petabytes+	Up to ~10 TB	Petabytes	Petabytes+
Unit size	1 MB/entity	~10 MB/cell ~100 MB/row	5 TB/object	Determined by DB engine	10,240 MiB/ row	10 MB/row

Azure and AWS Database Systems

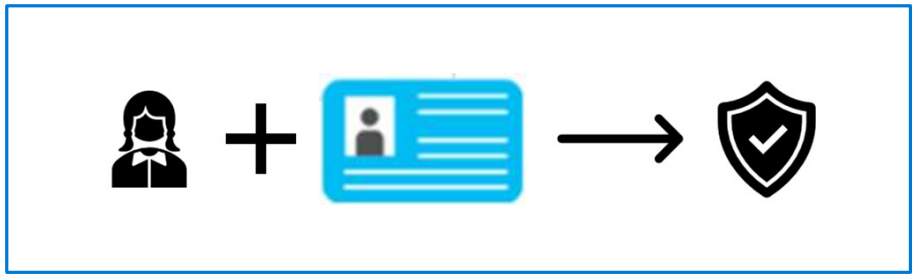


Security in the Cloud

Compare authentication and authorization

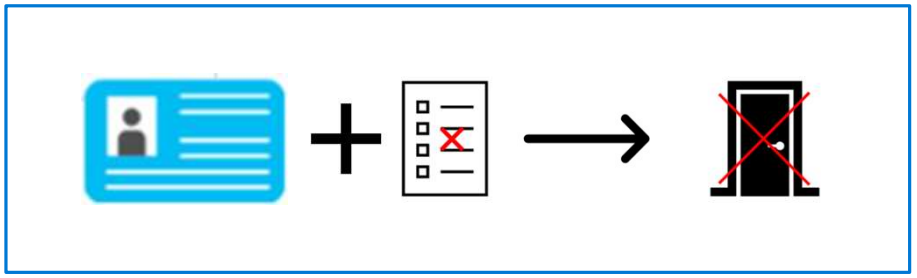
Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.



Authorization

- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.



Multifactor authentication

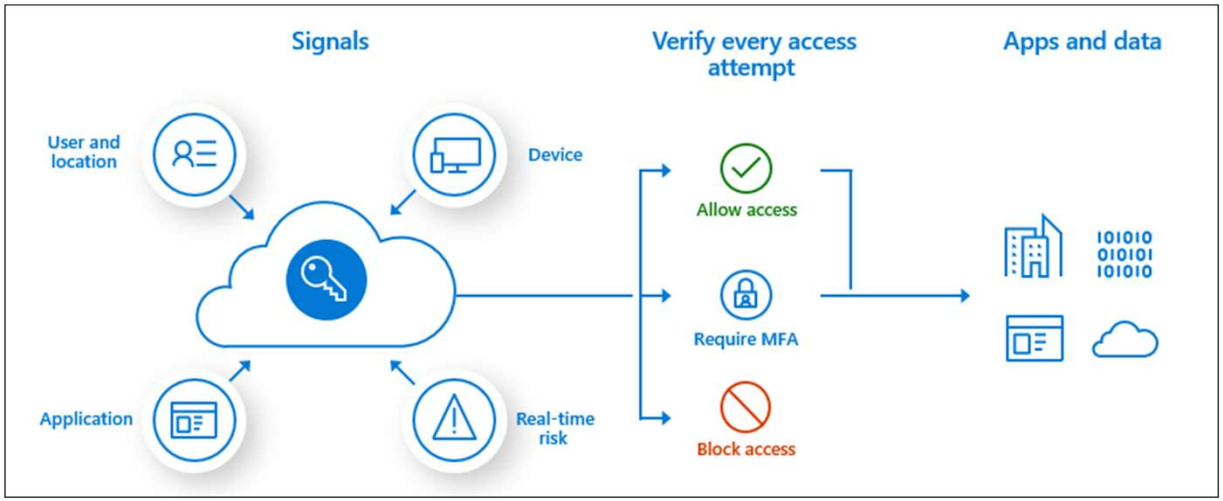
Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

Conditional Access

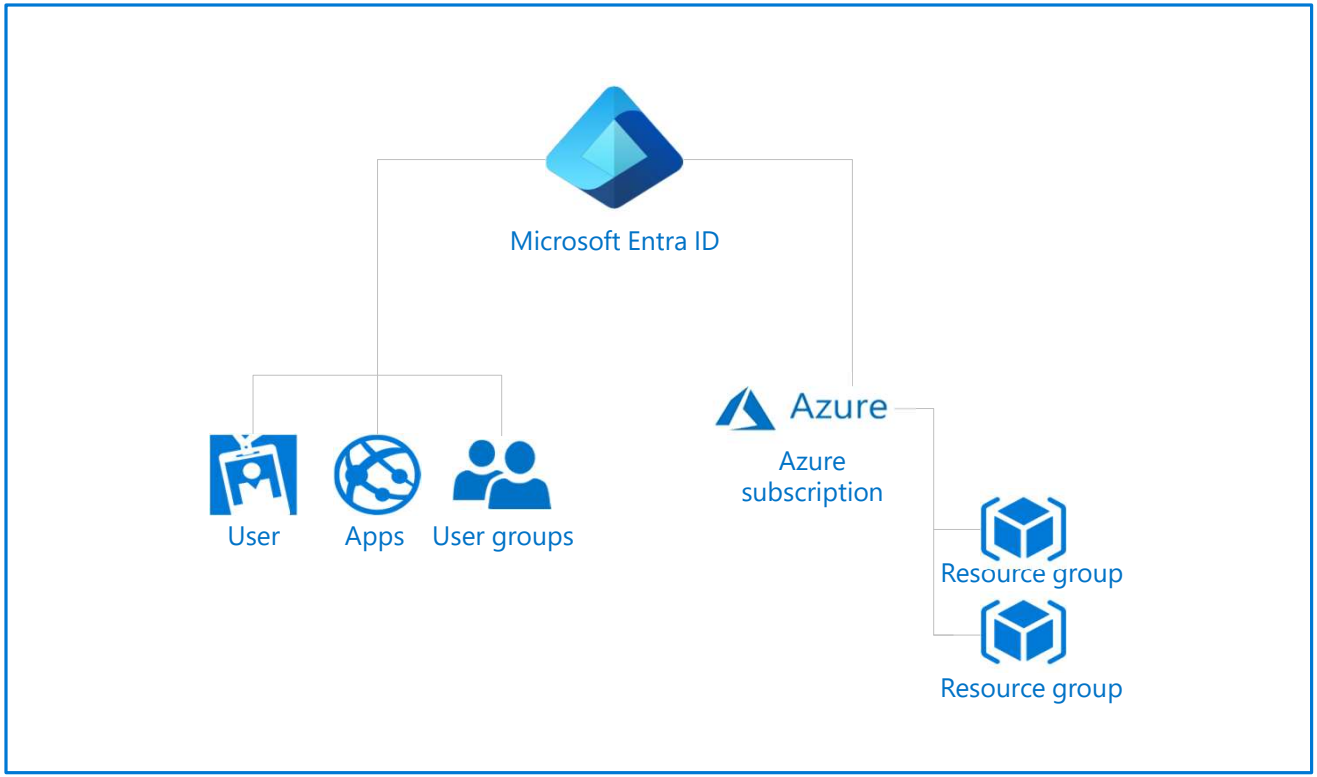
Conditional Access is used to bring signals together, to make decisions, and enforce organizational policies.

- **User or group membership**
- **IP location**
- **Device**
- **Application**
- **Risk detection**

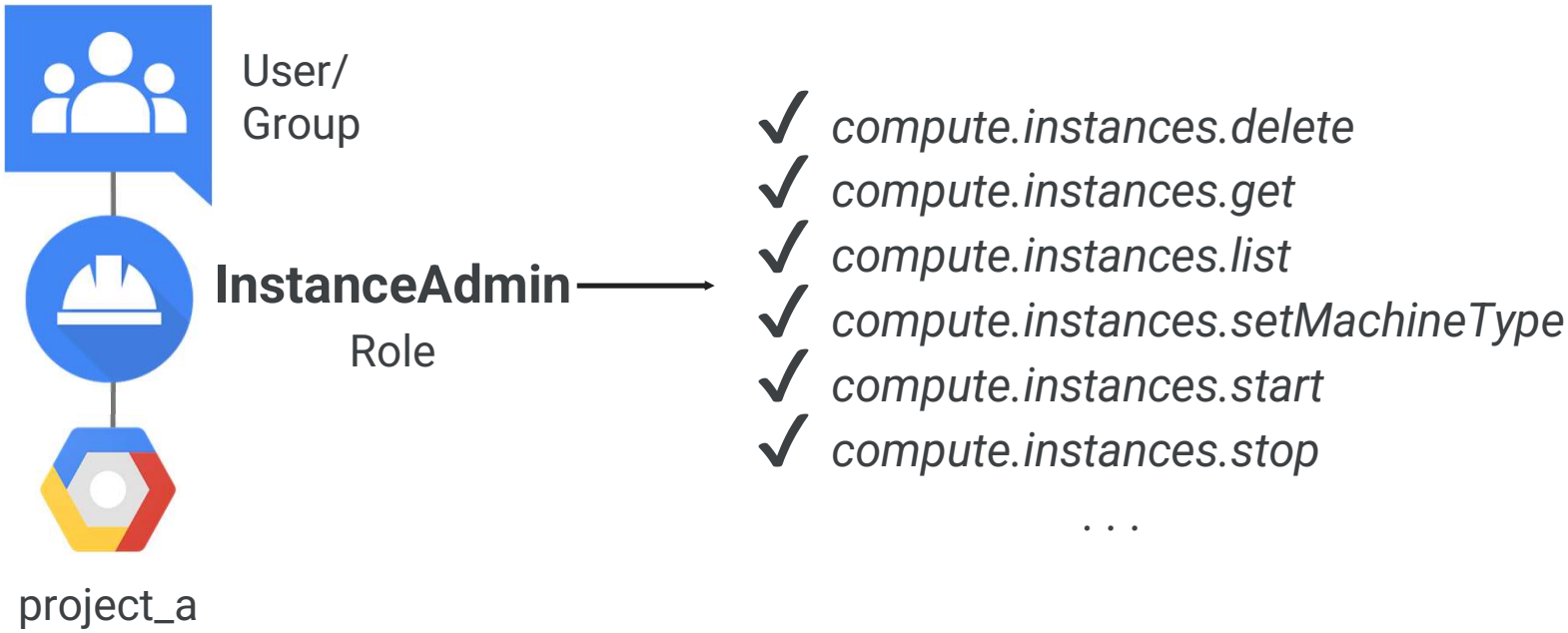


Role-based access control

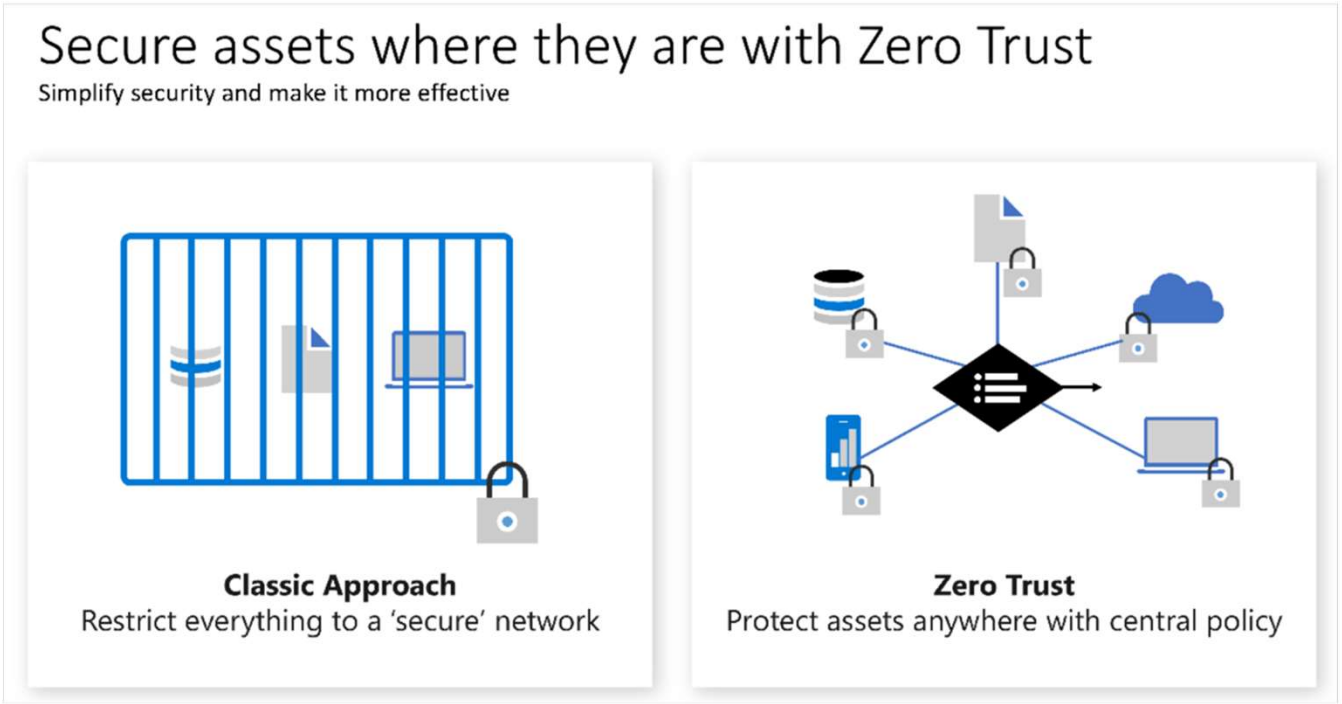
- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.



IAM predefined roles offer more fine-grained permissions on particular services

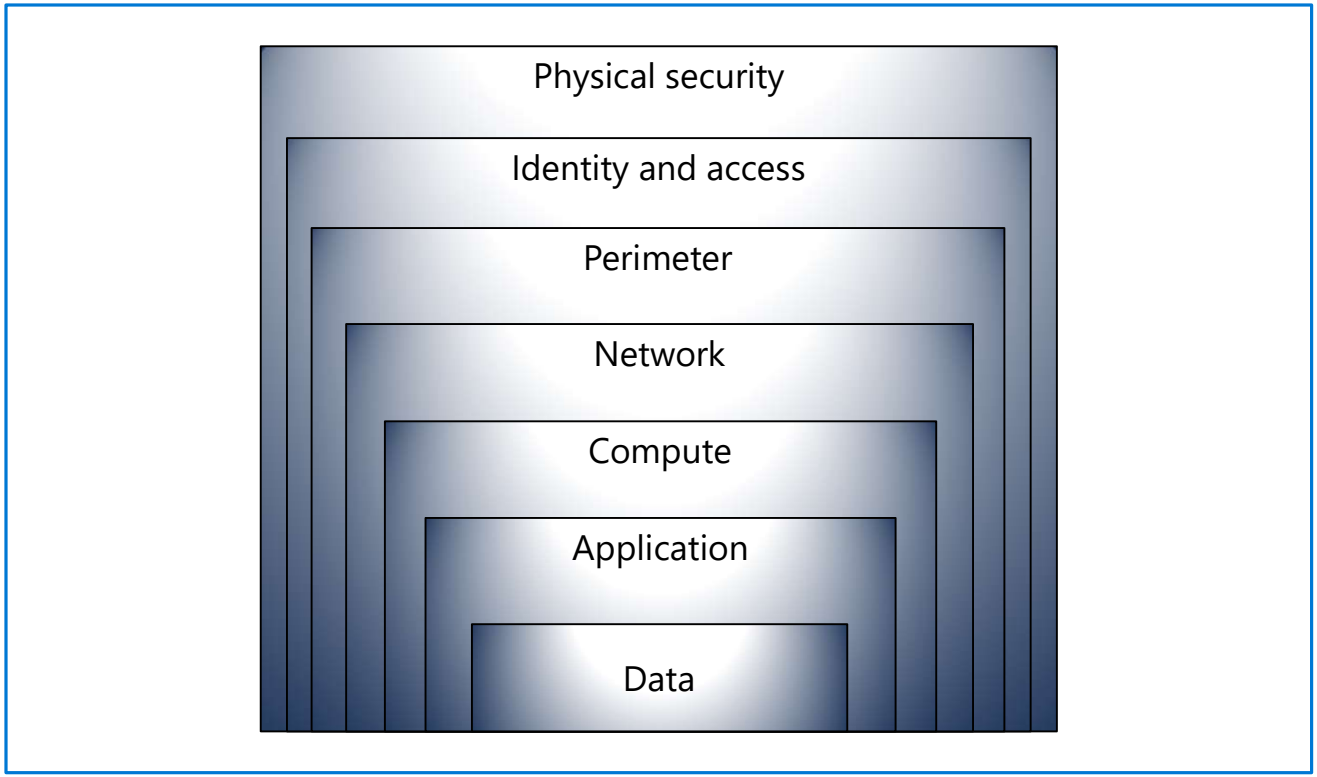


Zero Trust



Defense in depth

- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Storage Service Encryption

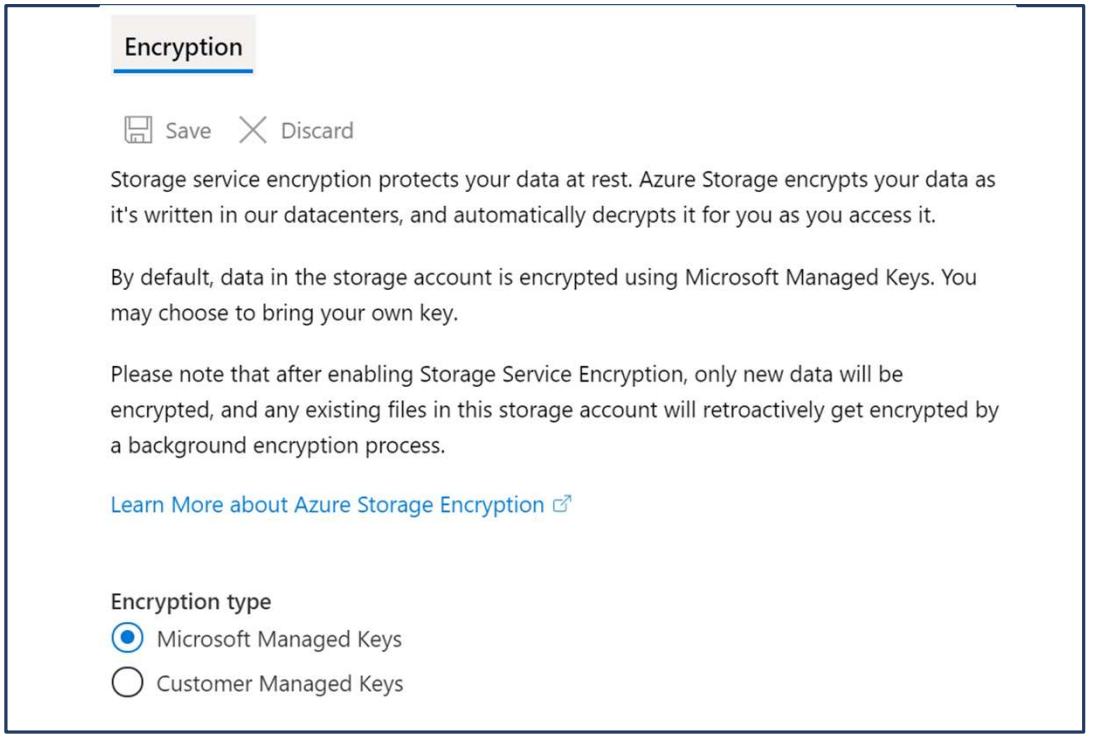
Protects your data for security and compliance

Automatically encrypts and decrypts your data

Encrypted through 256-bit AES encryption

Is enabled for all new and existing storage accounts and cannot be disabled

Is transparent to users



You can use your own key

Resources management

Resource Manager

- Provides a consistent management layer
- Deploy, update, or delete resources in single coordinated operation
- Provides security, auditing, tagging features
- Provides alternative ways that work best for users

There are four ways to interact with Azure

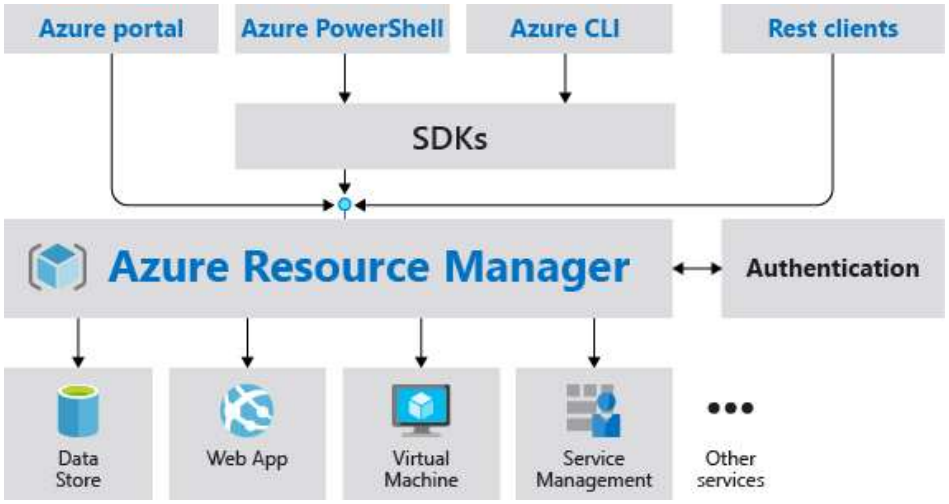
Azure portal – provides Graphical User interface (GUI)

Azure Powershell – command line interface uses powershell commands

Azure CLI – command line interface uses linux commands

REST full API – enable orchestration / automation process thru declarative languages

Azure Mobile App – monitoring resources, quick diagnosis, manage resources (cloud shell)



There are four ways to interact with GCP

Cloud Platform Console

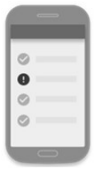
Web user interface

Cloud Shell and Cloud SDK

Command-line interface

Cloud Console Mobile App

For iOS and Android

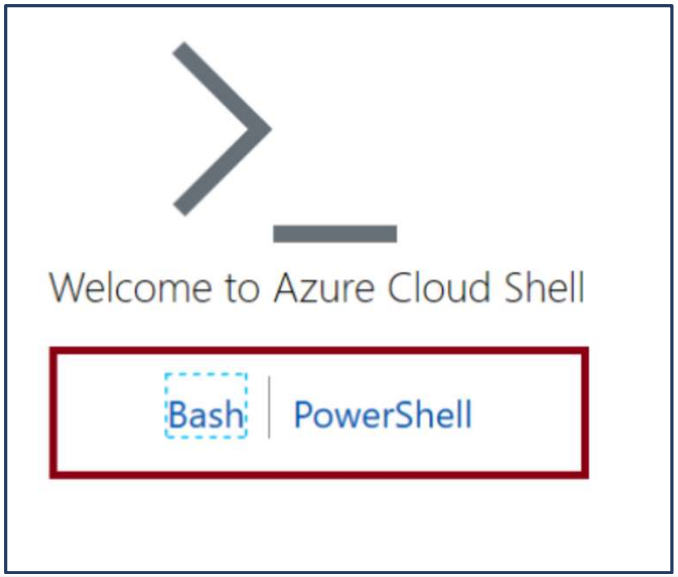


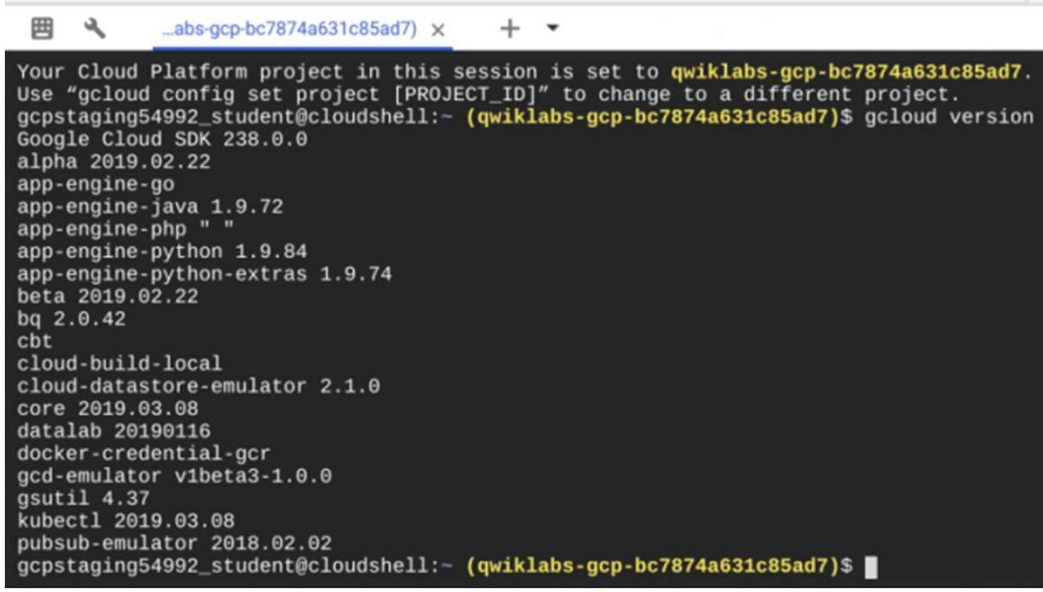
REST-based API

For custom applications

Cloud Shell

- Interactive, browser-accessible shell
- In Azure, offers either Bash or PowerShell
- Is temporary and provided on a per-session, per-user basis
- Requires storage account
- Authenticates automatically
- Integrated graphical text editor
- Is assigned one machine per user account
- Times out after 20 minutes





DEMO

Questions and Closing Thoughts?

The End...

Thank you

We look forward to seeing you in another session