AWS Cloud

**Lambda**

Serverless service

It only has virtual functions

Run on demand

Scaling is totally automated

Benifits

Easy price

- Pay per request and compute time

- Even for free tier 1 million request and 400,000 GBs of compute time

- It can be integrated with whole AWS suite services

- It is event driven so when we need it

- Easy monitoring through cloud watch

- Easy to get more resources per functions (up to 10 GB of ram)

- Increse RAM will also improve CPU and network

Langugae support

Node.js (javascript)

Python

java

C# (.NET core)

Golang

C# / powershell

Ruby

Custome runtime API (Rust)

Lambda container image

Leveraging the global infastructor of AWS

Route 53

It is a globle service doesnt needed regions. Take a domain if want to use route 53.

Route 53 service will allow you to derive the trafic comes from a contry to specific geographic location or lattency based.

This service will redirect you domain to configured server in AWS.

Route 53 will not comes free. It will cost $12 for domain and $0.5 for hosted domain.

Select region -->>chooseAMI-->>choose instance type-->>configure or choose previously used instance-->>Add a storage-->>Add a tag-->>Configure security group-->>SelectEC2 instance-->>Add a little code of heloworld-->> Review and launch-->> Launch instance

AWS cloud front service

Content delivery network CDN

Improve the read performance, as content is cached at the edge of locations at 216 point globally

Provides ddos protection

Integrated with AWS web application firewall

Cloud front will connect with S3 and http. It will cache the data from main server and serve according to contry needed.

The data fetched from the server and located at a contry will be read only. So that hacker will not get the chance to hack the main server.

Create bucket-->> Do necessory setings like encription..-->> create

It is a global service

Amazon S3 transfer acceleration

You got the speed comparison of same file transfering

AWS Globle accelerator

It improove the globle application availibility and performance using the AWS globle networks

It will leverage the AWS internal network to route and optimize your applications around 60%

It will create the edge location and transfer all the data to that edge location so that you will get a low latency

Differnce between accelerator and cloudfront

Both use AWS globle network and edge locations around the world

Both uses AWS shield for DDOS

Cloud front is content delivery network, which improoves cachable contents like images videos etc and content served at the edge

Globle accelerator Nocaching The application running on the all the configured server on one or more AWS region

It will be improove performance of TCP or UDP

There is one tool which will give you speed speedtest.globle accelerator.aws

Gives the detail with globle accelerator and without accelerator

AWS outposts

Associated with hybrid cloud.

It is the server racks that offers a same infractures, services, APIs, & tools to build your own applications on premises just as in the cloud.

AWS will setup the racks at your premises

Physucally we will be responsible for the security

Benifits,

Low latency access to on premises system

Local data processing

Easier migration from on premises to cloud

Data residency

Works with EC2, EBS, S3, EKS, ECS, RDS, EMR

AWS Wavelength

Wavelength zones are deployed at the edge of 5G networks

It works with EC2, EBS, VPC..

Ultra low latency application through 5G network

High bandwidth and secure connections to parent AWS region

It will used in smart cities, ML, Connected vehicles, AR/VR, Real time gaming

AWS local zones

Places AWS compute , storage, database, and othe rselected services close to latency sensitive

Extend your location to more VPC

Compatible with EC2, RDS, ECS, EBS, Elasticache, direct connect

To setup the zones

Go to EC2-->>zones-->> local zone-->>enable-->>chose ami and remaining things

Globle application architecture

Single region

SQS Service

Simple queue service

Oldest service

Multiple proucer -->> SQS Queue -->> COnsumer

Scale from 1 messgage/sec to 10000message/sec

Deffaulr retention of message 4 days to 14 days

No limit for messages

Message were deleted by queue once consumer will read

Low latency <10 ms

Go to amazon SQS

Create queue-->>Selecte standard-->> give name-->> Create queue

Amazon SNS

Simple notification service

Event publishers will only sends messages to one sns topic

As many as subscriber as we want to listen for topic notification

SNS subscriber can be a http/https, emails, SMS messages, mobile notifications, SQS queue, Lambda functions

Click on serachbar type sns

Click on create

Create subscription based on need

Amazon kinesis

Kinesis=real time big data streaming

Manage service to collect, process and analyse real time streaming data at any scale

Kinesis data stream : Low latency services scale from hundread, thousands of sources

Kinesis data firehouse : load stream onto the s3, redshift, elastic search

Data from iot devices,

IoT devices-->>kinesis stream-->>analysys-->>firehouse-->>S3 bucket or redshift

Amazon MQ

It is like MQTT, AMQP protocoal

MQ=manage apache activeMQ

Doesnt scal at SQS/SNS

It has both features SQS, SNS

Amazon cloud watch metrics

It provides metrics for every services in AWS

It have a timestamp, CPU utilization, Network utilization

Can create cloud watch dashboard

EC2 -- CPU Utilisation, Status check, network, default metrics at 5 min, Detail at 1 min

EBS volumw -- disk read/write

S3 -- bucket sizebyte, no of objects, all requests

Billing -- total estimated charge

Service limit -- How much you have been using service api

Custome metrics Push your own metrics

Amazon cloud watch alarms

Used to trigger the notification for any metrics

Alarm action

Auto scaling Increse or decrese EC2 desired count

EC2 action -- stop, terminate, reboot or recover EC2 instance

Various options sampling, %, max, min

Can choose period on which need to evaluate the alarm

For example create billing alarm

Create alarm->> choose service-->> create as needed

Cloud watch logs

No logs goes to cloudwatch

You need to run cloud watch agent on EC2 to push the log file you want

Make sure IAM permissions are correct

The cloud watch log agent can be setup on premises too

Cloudwatch events/eventbridge

It is trigger when event comes for ex trigger lambda function, email SNS, SQS etc

Eventbridge

Next evolution of cloudwatch

Events generated by aws services

Can use zendesk, datadog, segment, auth0 etc

Can create custome eventbridge for your application

Model schema registery

Choose service you want notification-->> Event trigger type-->>Create rule as needed

AWS Cloud trails

Provides governance, compliance, audit for your AWS account

It enabled by default

Get a history/API call made within the AWS account

Console

SDK

CLI

AWS Services

Can puts logs from cloud trail to cloud watch or S3

If resource will be deleted then AWS will investigate cloudtrail first

Events are stored for 90 days

If you need logs more then 90 days then you need to log them into S3 or athena

You can see indepth who has done change/addd/delete of anything here

Cloud trail inside

It is used to detect unusual activity in your account

Detect pattern

Inaccurate resource provisioning

Hitting service limit

AWS Xray

Debugging in production the good old way

Test locally

Add log statement everywhere

Redeploy

Troubleshooting bottlnecks

Review behaviour

Find errors

Are we meeting time SLA?

Amazon codeguru

ML powered service for automated code review and application performance recommended

Codeguru reviewer automatic code review for static code analysys

Identify critical issues, security valunerability, hard to find bug

To identify memory leak, resource leak

Support java and python

Codeguru profiler Visibility/recommendation about application performance during runtime(production)

Help to understand runtime behaviuor of the applications

Identify and remove code inssuficienty

Improove efficiency performance

Decrese compute cost

Provide heap memory summery

Anomaly detection

Support in AWS or on premises

Minimal overhead on application

AWS Status- service health dashboard

Show all region, all service health

Shows historical info

RSS feed to subscribe

AWS personal health dashboard

Provides alerts and remediation guidance when aws is experiancing event that may impact you

While service health dashboard will display general status of aws services

It will shows issues, open issue on alert section

VPC-->>virtual private cloud it is the private network to deploy your resources

Subnets-->>Allows you to partition your network inside your VPC

Publick subnets-->>It is a subnets that is the accesible from the internet

Private subnets-->>not accessible from the internet

Route table-->> To define the access to internet and between subnets we use route table

Internet gateways and nat gateways will help here

Network ACL & security group

NACL It is a firewall which controll from and to subnets

Can have allow and deny rules

Are attatched at subnet level

Rules only includes IP adress

Security group

A firewall that controll traffic to and from an ENI/EC2 instance

Can have only a;llow rules

VPC FLow logs

It will help to monitor and troubleshoot connectivity issue

Subnet to internet

Subnet to subnet

Internet to subnet

Capture network infirmation from the ELB, elasticache, RDS, Aurora

VPC flow log data can go to S3 / cloud watch logs

VPC Peering

Can connect 2 VPCs privatly using the AWS’S network

And make them behaave if they were in the same network

Must not have overlapping CIDR

VPC peering connection is not transitive

VPC Endpoints

Allow you to connect AWS services using private network instead of public network

This gives you enhanced security and low latency to access AWS services

Also connect with dynamodb & S3

Site to site VPN & Direct connect

Onprmises service must connected with AWS network.

For site to site it will go over internet with automatically encrypted, publick network

Uses customer gateway (CGW), Virtual private gateway (VPW)

Other one is DX direct connect It is a physical connection between on-premises and AWS.

It is provate secur and fast

It costs high cost, fater more reliable

Transit gateway

It works with DX, VPN connection

One single gateway to provide the functinality

It is the transit peering between thousands of VPC, on premises, hub and spoke connection star connection

Security and compliance,

RDS

AWS responsibility Manage underlying EC2 instance, disable SSH acess, Automate DB patching, OS patching, Audit the underlying instance, disks, gaurentee its function

Your responsibility

Check the ports, IP, security group, inbound rule, in DB’s SG

In databse user creation and permission

Creating databse with or without publick access

Ensure parameter group or DB is configured to only allow SSL connection

Data encription setting

Example for S3

AWS responsibility

Gaurentee you got unlimited storage

Gaurenteed you get encription

Ensure separation of data between different customers

Ensure AWS employee can not acess your data

Your responsibility

Bucket configuration

Bucket policy/publick setting

IAM user

DDos

Distributed denial of service

AWS shield standard protects against DDOS attack for your website and applications for all customers at no extra cost.

AWS shield advanced 24/7 premium DDoS protection

AWS WAF filter specific request based on rule

Cloud front and route 53

Availibility protection using globle edge network

Combined with AWS shield, provides attack mitigation at the edge

**AWS shield standard** free service that is activated for every AWS customer

Provides protection from attackes such as SYN/UDP floods, reflaction attacks and other layer 3/layer 4 attack

**AWS shiled advance**

Optinal DDos mitigation service($3000 per month per organization)

Penetration testing

Without prior approval we can use 8 services

Amazon EC2 instance, NAT gateway, Elastic load balancer

Amazon RDS

Cloud front

Aurora

API gateway

Lambda and lambda edge

Lightsail

Elasric beanstalk

Prohibited activities

DNS zone walking via amazon route 53 hosted zone

DoS, DDoS, Simulated DoS, Simulated DDoS

Port flooding

Protocol flooding

Request flooding

Encription with KMS

Data at rest vs data at transit

AWS KMS AWS will manage key for us

Encription optin

EBS

S3

Redshift

EFS

Encription automatically enabled

Cloud trail logs

S3 glacier

Storage gateway

Cloud HSM

KMS=> AWS manages softwares for encryption

CloudHSM=>AWS provision hardware

Dedicated hardware (HSM = Hardware security modules)

With that you manage your own encryption key entirly (not aws)

**Types of CMK**

**Customer managed CML** cutomer can enable disable, possibility of rotation, policy, Possibility to bring your own key

**AWS Managed CMK** on behalf of customer, used by AWS service

**AWS owned CMK** collection of cmks that an aws service owns and manages to use in multiple accounts

**cloudhsm keys** key generated from your own cloudhsm hardware device

Cryptographic operations are performed in cloudhsm cluster

**ACM AWS certification manager**

It will easily provision, manage, deploy SSL/TLS certificates

Used to provide in-flight encryption for website https

It supports both public and private TLS certificates

Free of charge for public TLS certificates

Automatically TLS certificate renewal

Integrated with elastic load balancer, cloud front, APIs on API gateway

AWS secret manager service

Newer service for storing secrets

Capaability of rotation of secrets every x days

Automate generation of secrets

Integrated with amazon RDS

Secrets are encrypted with KMS

Mostly meaned for RDS

**AWS Artifacts**

Portal that provides on-demand access to AWS compliance documents and aws agreements

Artifact reports

It provides AWS security and compliance documents like ISO certification, payment card industry, system and organization control

Artifact agreement

Allows you to review, accept, track BAA, HIPPA

**Amazon guard duty**

intelligent thread discovery to protect AWS account

Use machine learning algorithem

One click to enable no need to install software

VPC flow logs, cloudtrail logs, DNS logs go to guard duty

**AWS Inspector**

Automate security assessment for EC2

Analyze the runnin OS against known valunrable

Analys against unintended network accesibility

It needed AWS inspector agent must be installed on OS in EC2

After inspection you will get a report of valunaries

194

**Amazon macie**

Amazon macie is the fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Macie helps identify and alert sensitive data such as personal identifiable information (PII)

S3 bucket-->>Analyse-->>Macie-->>notify-->>Cloud watch event bridge-->>Integration

**AWS Security hub**

Central security tool to manage across several AWS accounts and automate security checks

Integrated dashboard showing current security and compliance status check to quickly take action

Guardduty

Inpector

Macie

IAM Access manager

AWS System manager

AWS Forewall manager

AWS partner solution

Must first enable AWS config service

**Amazon detective**

Guard duty, macie and security hub are used to identify potential security issues or findings

Sometimes security findings required deeper analysis to isolate the root cause and take action Its a complex processs

Amazon detective will analyse , investigate and quicly identify the root causes of security issues or suspecius acitivity using ML and graphs

Automatically collect, and processes events from vpc flow logs, cloud trails, guard duty, and create unfied view

Produces visulization with details and context to get root causes

**AWS Abuse**

Reports suspected AWS resources used for abusive or ilegal purpose

Abusive and prohibited behaviours are

SPAM receive undesired emails from AWS owned IP adress, website, & forums spammed by AWS resources

Port scanning Sending a packet to your ports to discover unsecured ones

DoS or DDoS attacks AWS owned IP adress attemtpting to overwhlem or crash your servers /softwares

Instrusion attemts Logging in on your resources

Hosting objectionable or copyrighted content Distributing illegal or copyrighted content without permission

Distributing malwares AWS resource distributing software to harm computers or machines

Contact to AWS abuse form or abuse@amazonaws.com

**Root user previleges**

Root user = account owner (Created when account is created)

Has complete access to all AWS services and resources

Lock away your AWS account root user keys

Do not use root account for everyday task, even adminstrative tasks

Action that can be performed by the root user

Change account setting

View tax invoices

CLose your AWS account

Restore IAM user permission

Change or upgrade your AWS support plan

Regoster as a seller reserved instance market place

Configure an amazon S3 bucket to enable MFA  
Edit or delet an amazon S3 bucket policy that included an invalid VPC ID or VPC endpoint ID

**Machine Learning**

Amazon rekognition Use to recognize object, people, text, scenes, in images and video usin ML.

Do the facial analysis, facial search, to do a verification

Create a databse of the familier faces or compare against celebrities.

Use cases

Labeling

Content moderation

Text detection

Face detection and analysis (gender, age range, emotions)

Face and search verification

Celebrity recognition

Check more on website aws.amazon.com/rekognition

**Amazon transcribe**

Automatocally convert speech to text

Uses deep learning process called automatically speech recognision (ASR) to convert speech to text quickly and accurately

Use cases Transcribe customers service call

Automate closed captioning and subtitiling

Generate metadata for media assets to create fully searchable archives

**Amazon Polly**

Turns text into lifelike speech using deep learning

Allows you to create application that talks

**Translate**

Natural and accurate langauge translation

Allows you to localize content such as website and application for intenratinal users and easily translate large volumes of text efficiency

Source langauge-->> Target French langauge

**Amazon lex & connect**

It is the same technology that powers alexa.

It worked as ASR automatic speech recognision to convert speech to text

Natural language understanding to recognise the intent of text, callers

**Amazon connect**

Receive calls , create contact flaws, cloud based virtual contact center

Can integrate with other CRM, system or AWS

No upfront payments, 80% cheaper than traditional contact center solution

Phone call schdule call-->>connect-->>strean-->>lex (intent recognision)-->>invoke-->>lambda-->>schedule-->>CRM

**Amazon comprehend**

For natural language processing

Fully managed server less services

Use ML to find insight and relationship intext

Language of text

Extract key phrases, places, people, brands, or events

Understand how positive or negative the text is

Analyse text using tokenization and parts of the speech

Automatically organise a collection of text files by topic

Sample usecases

Analyse customer interactions to find what leads to a positive or negative experiance

Create and group articles by topic that comprehanded that will be incover

**Amazon sagemaker**

Fully managed service for developer / datascintist to build ML model

Let us take an example for what score you got at your cloud certified exam?

Historic data (Years of exper, Experiance with AWS, Time spend) for billions of student-->>Lable that data-->>Take score-->> Compare data-->>Build machine learning model-->>Train and tune it And add new data on timely bases

**Amazon forecast**

Fully managed ML services

Predict the future sales of a raincost

50% more accurate then data

Reduce firecast time from month to hour

Historic data-->>Features, price, discount, traffics, store location..-->>upload-->>S3-->>Amazon forecast-->>model-->>Future sales $500000

**Kedra**

Fully managed document searchable services.

Text, pdf, HTML, power point, MS word, S3, salesforce, drive, custome APNs-->>indexing-->>kendra-->>Ask question Where is the IT support desk? Ask by user-->> give answer it is on first floor

**Amazon personilite**

Fully managed ML-service to build app with realtime personilized recommendation

Integrated with existing website

Implement in a day (No need to build, train, deploy, ML solutions)

Amazon S3/personilzed API-->>Amazone personilized-->>CUstomized AP-->> websites, mobile apps, SMS, Emails

Same technology used by the amazon.com

**Account management, billing, support**

**AWS Organizations**

Globle service

Allows you to use multiple accounts

Main account is the master account

Cost benifits--consolidated billing across all accounts, single payment menthod

Pricing benifits from aggregated usage (Volume discount for EC2, S3)

Pooling of reserved EC2 instance for optimal savings

API is available to automate AWS account creation

Can create accounts per department, per cost center, per dev/test/prod, based on regulatory restriction (using SCP), for better resource isolation (VPC), to have a separate per account service limits, isolated account for logging

Multi account vs one account multi VPC

Use taging standards for billing purposes

Enable cloud trails on all account, send log to central S3 account

Organization unit example (OU)

Based on business unit

Environment lifecycle

Project bases

**Service controll policy,**

White list or black list IAM actions

Applied for OU level and account level

Does not apply to master level

SCP is only allocate to user and role of accounting

Doesnt apply to service lined role

216

**Pricing model of the cloud**

**EC2**

Only charge for what you used

No of instaNCES

Region

OS and SW

Instance typen& size

ELB will run based on the time and amount of data processed

Lambda & ECS

Pay per call

Pay per duration

ECS

EC2 launch model no additionl fees you pay for AWS resources stored and created.

Farget

Launch type model pay for VCPU memory resorces, allocate your memory to container

S3

S3 standard

S3 infrequenct access

S3 one zone IA  
S3 intelligent tiering

S3 glacier deep archive

No and the size of the objects price can be tiered

No and type of request

Data transfer out of the S3 region

S3 transfer acceleration

Lifecycle transfer

EFS pay per use

**Storage pricing EBS**

Volume based

Storage volume in GB per month provisioned

IOPS

General purpose SSD

Magnetics no of request

Provisioned amount in IOPS

Snapshot

Added data cost per GB per month

Data transfer’ Outbound data trnsfer tiered for volume discoungt

Inbound is free

RDS

Per hour billing

Database charactristics

Engine type

Size

Memory class

Purchase tyoe

Ondemand

Reserved instance

Backup storage

There is no storage it si free for a region

Databse pricing

Additional storage

No if io requests

Deployemenr type

Single AZ

Multi AZ

Data transfer

Outbound data transfer are tiered for the volume discount

Inbound is free

Content delivery - cloud front

Pricing is different based on the geo region

No of http/https request

**Saving plan overview**

Commit a certain $ amount per hour for 1 or 3 year easiest way to setup long term commitement on AWS

EC2 Saving plan which will give you a 72% discount compared to on demand

Commit the usage of individual instance familiy in a region

Regradless of AZ size tenancy

All upfronts, no uofront, partial upfronts

Compute the savings plan

Upto 66% discount compared to ondemand

It is regardles of family, region, OS, tenancy, compute options

Compute EC2 farget, lambda

AWS cost explorer

Will shows saving plans

AWS cost management

**COmpute optimizer**

Reduce costs and improove performance by recommending optimal resources for your resources

Helps which one is over position and under position

Use resources configurations and cloud watch metrics

Supported resources are

EC2 instance, EC2 auto scaling group, EBS volume, Lambda functions

Lower your cost by upto 25%

Recommendation can be exported to S3

**Billing and costing tools**

Estimated cost in cloud

TCO calculator

Simply monthly calculator/pricing calculator

**Tracking cost in cloud**

Billing dash boar

Cost allocation tag

Cost and usage reports

Cost explorer

**Monitoring against cost plan**

Billing alrams

Budgets

**TCO Total cost ownership will give you Onpremises**

AWS will helps you to reduce TCO by reducing need to investigate in large capital expenditure and provide pay as you go model

TCO will allow you cost savings & provide a report that can be used In executive presentation

Compare the cost of your applications in onpremises or traditinally hosting, in

Server

Storage

Network

IT Labor

GO to awstcocalculator.com

**Pricing calculator per services**

Estimate the cost for your archicture solution

**AWS Billing dashboard**

**AWS free tier dashboard**

**Cost allocation tags**

Use tag to track the AWS cost on a detailed level

**AWS generates a tag** & it will automatically apply to the resources you created

**User defined tags** Defines by the user, start with prefix user,

Tags are used for organizing resources like

EC2 load balancer, security group

RDS, VPC, Route 53, IAM user

Resources created by the cloud formation are tagged the same way

Free nameing

Common tags are Name, environment, team

Tags can also be used for the create resource group

Create maintain, and view collection of resources, that shares common tags

Manage this tags using tag editor

**Cost and usage report**

Dive deeper into your AWS costs and usage

Can see pricing models

Use of detailed services, cost allocations

Can be integrated with athena, redshift, quicksight

**Cost explorer**

Visulise, understand and manage your aws cost and usage over time

Create custome reports, that analyse cost and data

Use monthly, hourly, resource level granularity

Can choose optimal savings plan

Can **forcast** 12 month usage based on previous usage.

**AWS Budgets**

Create alarm and send alarms when cost exceeds the budget

3 type of budgets

usage, cost, reservation

For reserved instance (RI)

- Track utiliztion

- Support EC2, Elasticcache, RDS, Redshift

- Can confiugure emails and alerts

**Trusted Advisor**

No need to install anything-high level AWS account assesement

Cost optimize

Security

Fault tolerance

Service limit

**7 core checks**

S3 bucket permission

Security groups

IAM use

MFA on root account

EBS public snapshot

RDS publick snapshots

Service limit

**Full checks**

Business and enterprise support plan

Full check available on 5 category

**AWS developer support plans**

All basic support plans

Business hour email access

Case sevirity/responce time

General guidance < 24 hours

System impaired < 12 hours

Production system impaired < 4 hours

Production system down < 1 hour

Acces to infrastructure event management for additional fee

**AWS enterprise support team**

Access to a technical account manager

Intended to use with mission critical workloads

All of business suport plan+

Intended to be used if you have mission critical workloads

Production system impaired < 4 hours

Production system down < 1 hour

Business critical system down <15 min

**Account best practices**

Operate multiple account using organization

Use SCP to restrict account power

AWS controll tower

Use tags and cost allocation tags

IAM guidelines MFA, Least previledge, password policy, password rotation

Config to record all resources configurations and compliance over a time

Cloid formation to deploy stack across accounts and regions

Trusted advisor to get insights,

**Advanced identity**

AWS STS security token services

Enables you to create temporary limited previledge credential to access your AWS resources

IAM user-->>STS service will provide temporary security credentials

Short term credential you configure expeiation period

**Amazon cognito**

It is the way for your mobile and web application user to provide **identity**

Instead of creating user in **IAM** we will create in **cognito**

With the help of the cognito we can login with social identity provider like **google, facebook, Twitter**

**Directory service**

Microsoft active directory

Found on any windows server with AD domain services

Centralized security management

Create account and assign a permission

**AWS directory services**

AWS manage microsoft AD

Support MFA

Can create own AD

Establish trust connection with your on premises AD

**AD Connector**

Directory gateway to redirect on premise AD

Users are managed on the on-premise AD

**Simple AD**

AD-compatible managed directory on AWS

**AWS SSO single sign on**

Centrally sign on to acess multiple account and 3rd party business application

Like dropbox, office365, slack, AWS management consol

Integrated with AWS organizations

Support SAML 2.0 markup

Integration with on premise active directory

**Amazon workspace**

DaaS desktop as a service Solution to provide windows or linux desktops on the cloud

Great to eliminate the on premises virtual desktop

Fast and quckly scalable to thousands of users

Secured data using KMS

Pay as you go

User-->>Virtual desktop-->>Corporate data center/AWS cloud

**Amazon appstream**

Desktop application streaming service

Deliver to any compouter without acquiring infrastructor

The application will delivered within the webbrowser

Diffreance between workspace and appstream

**Workspace**

Fully managed VDI and desktop available

The user connect to VDI and open native or WAM application

Worlspaces are on demand or always on

**Appstream2.0**

Stream as a desktop application to web browser

Work with any device

Allow to configure an instance type per application like CPU, RAM, GPU

**Amazon sumarian**

Create and run VR, AR and 3D applications

Can be used to quiclky create 3D models with animation

Ready to use templates ans assests No programmer or 3D expertise needed

All this will accessible with webbrowser, URL, and popular hardware for AR/VR

**AWS IoT Core**

Core allows you to easily connect the device to the AWS cloud

Devices can be serverless, secure, scalable to build billions of devices and trillions of messages

Your applications can be connected with your devices even when they are not connected

Integrated with Lambda, S3, Sagemaker, etc

Your device-->>AWS IoT core-->>AWS

Build IoT applications that gather, process, analyse, and act on data

**Amazon elastic trancoder**

Elastic transcoder is used to convert the file stored on S3 into media file required by consumer playback devices (Phone etc…)

S3 input bucket-->>Transcoding pipeline-->>S3 output bucket-->>Smartphone, tablets,PC

Benefits

Easy to use

Highly scalable

Cost effective

Fully managed and secured

Pay for what you used

**AWS device farm**

Fully managed service that tests your web and mobile apps against desktop, browser, real mobile device, and tablets

Run tets concurrntly on multiple devices

Ability configure device settings (GPS, Language, Wi-Fi, Bluetooth)

User-->>Test applications-->>Real time device farms

It interact with devices

Shows reports, logs, screenshots

**AWS Backups**

Fully managed service

On demand and scheduled backups

Supports PITR point in time recovery

Retension period, life cycle management, backup policies

Cross region backups

Cross account backups

AWS Backup-->>Crate plans-->>(EC2. Dynamodb, RDS, EBS, Storage gateway, EFS, FSx)-->>S3

**Disaster recovery strategies**

Backup and restore AWS cloud-->>Corporate data center it cuts the costs

Pilot light AWS Cloud-->>EC2

Warm standby AWS Cloud-->>EC2 High cost

Multisize/hot site Full version of app at full sized

**Cloud endure disater recovery**

Quicly and easily recover physical, virtual, and cloud based servers into AWS

Protect your most critical databse oracle, mysql, sql server

Enterprise app SAP, protect withransomewere

**AWS datasync**

Move large amount of data from onpremises to AWS

Can synchronise to S3, EFS, FSx for windows

Replications task can be scheduled hourly, daily, weekly

The replications task can be incremental after full load

On premises-->>TLS-->>Regions AWS sync

**AWS Fault injection simulation FIS**

Fully managed service for running fault injection experiment on AWS workload

Based on chaos engineering

Stress an applications

Obser how sys will respond

Imolement improovement

Helps you to uncover hidden bugs and performance bottolnecks

Supports on EC2, ECS, EKS, RDS

AWS FIS-->>Create-->>Resources(EC2, ECs, EKS, RDS)-->>monitor cloud watch and event bridge -->>Stop-->> DO visual checks

Well architected framework

General guiding principals

Stop guessing your capacity needs

Test system at a production scale

Automate to make architecture experiments easier

Drive architecture using the data

Improove through game days

Design practices

Scalable vertical and horizontal

DIsposable resources :- dervers should be disposable and easily configured

Automations serverless, infrastructor, auto scaling

Loose coupling Monolith is the application that will do more and more over time becomes bigger

Break it down to smaller, loosly coupled components

Think more on services not servers

Don’t use just EC2

Use managed services, databses, serverless etc

5 pillers for architecture

Operational excellance

security

reliability

Performance efficiency

cost optimization

They are not something to balance or trade they are a synergy

**Operational excellance**

Includes the ability to run and monitor system to deliver business value and to continually imorove supporting process and proceducers

Design process

Perform operations as a code infrastructor as a code

Annotate documentation Create and annotate after every build

Make frequnt, small, reversible changes SO that in case of failure you can recover it

Refine operation proceducer frequenctly And ebsure that the team members are familier with it

Anticipate failure

Learn from all operational failure

For preparation use AWS cloud formation

-->>AWS config

Operate

AWS cloud formation

-->>AWS config-->>CLoud trails-->>Use cloudwatch-->if necessory use XRAY

Evolve

AWScloudformation

AWS codebuild-->>AWS codecommit-->>AWS code deploy-->>AWS codepipeline

**Security**

Includes ability to protect informations, system and assests while delivering business values

Design principle

Implement a strong identity foundation centralise priviledge management and reduce reliance on long term credential

Principle of IAM

Enable traceability

Integrate logs and metrics with system to automate respond and take actions

Apply security at all level

Like edge network, VPC, Subnet, load balancer, every instance, OS and application

Automate security best practices

Protect data in transit and at rest Encryption, tokenization, access control

Keep people away from data reduce and eliminate the need for direct access or manual processing of data

Prepare the security events

Run incident responce simulation, and use tools with automation to increse your speed of detection investigstion, recovery

**Security services**

Identity and access management

IAM, AWS STS, MFA Tocken, AWS organization

Detective controls

AWS config, AWS cloud trails, Amazon cloud watch

Infracture protection

Amazon cloud front, Amazon VPC, AWS shield, WAF, Inspector

Data protections

KMS, S3, ELB, Amazon EBS, Amazon RDS

Incidence responce

IAM, Cloud formation, cloud watch events

**Reliability**

Ability of system to recover from infrastructor or service disruption

Design principal

Test recovery proceduceres

Automatically recovery from failure

Scal horizontally to increse aggregate system availibility

Stop guessing capacity

Manage change in automation

**AWS Services for reliability**

Foundations

IAM, VPC, Service limit/quota, Trusted advisor

Change management

AWS auto scaling, Cloud watch, cloud trail, AWS config

Failure management

backups, cloud formation, S3, S3 glacier, route 53

**Performance efficiency**

Includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes the technology evolve

Design principles

Democrate advanced technologies

Go globle in a minutes

Use serverless architectures

Experiment more often

Mechanical symphathy

Selection

Auto scaling, Lambda, EBS, S3, RDS

Review

Cloudformation, NEWS BLOGS

Monitoring

Cloud watch, Lambda

Tradeoff

RDS, Elastic cache, Snowball, cloud front

Cost optimise

Includes the ability to run the system to deliver business value at the lowest point

Design principle

Adopt consumption mode Pay only what you use Let us say use a lambda where you pay for what u used. unlike RDS

Measure overall efficiency Use cloud watch

Stop spending money on data center operations

Analyse and attributes expeditures see ROI,

Use managed and applications level services to reduce cost of ownership

AWS services for cost optimzation

Expenditure awareness

AWS budget, cost and usage report, cost explorers, reserves instances reporting

Cost effective resources

Stop instance, reserved instances, S3 glaciers

Matching supply and demand

Auto scaling, Lambda

Optimizing over a time

Trusted advisor, Cost and usage report, News block

**AWS Well architected tool**

Free tool to review your architecture against the 5 piller well archotected framework and adopt architecdtural based practices

How its works?

Select your workload and answer questions-->>Review answers against 5 piller-->>Obtain advice

**AWS right sizing**

EC2 has many instance types but chossing the most powerfull tool isnt the best practices. Because the cloud is elastic

Right sizing is the process of of matching types and size to your workload performance and capacity requirement at lowest possible cost

It is the important to right size

before a cloud migration

Continuosly after the cloud onboarding process

Can use cloudwatch, costexplorer, trusted advisor, 3rd party tools can help

AWS ecosystem - Free Resources

AWS blogs

forums

Whitepapers

Quick start

AWS solutions

AWS support

Developer

Business hour cloud support assosiates

General guidance <24 hour

System impaired <12 hours

Business

24x7 phone, email, chat access, cloud support

Production system impaired <4 hour

System down <1 hour

Enterprise

Access to technical account manager

Concierge support team (for billing and account best practices)

Business controll syetem down <15 minute

AWS Marketplace

Digital catalog with thousands of software listing from independent software vendors

For ex sell

custome AMI

Cloud formation templates

Software as a service

Container

If you buy through the AWS marketplace it goes into AWS bill

You can sell your own solution on the AWS marketplace

**AWS Training**

AWS Digital online and classroom training

Private training for organization

Training and certificates for the USA governemt

Training and certificates for the Enterprises

AWS academy

**AWS professional services and partner**

Globle team of expert

They work along side with your team and choosen a member of the APN

APN=AWS partner network

APN technology partner provide hardware, connectivity, software

APN COnsulting partner

APN Training partner

AWS COmpetency program

**AWS Knowledge center**

Contains the most common and frequent questions and requests

**AWS certified cloud practitioner guide**