Security, Identity & Compliance

AWS Global Infrastructure / AWS Cost Management / Migration & transfer / Storage / Compute / Networking / Databases

IAAS / PAAS / Serverless

AWS

Availability zone ⇒ Datacenter

Support plan

Region

AWS account
Console
command line (programmatic)
SDK

Advantages

- Trade Capital expense for variable
- Massive economies scale
- Stop guessing about capacity
- Increase speed and agility
- Stop spending money running data centers
- Go Global

Edge locations ⇒ endpoints used for caching.
CloudFront CDN
150 Edge locations

S3 object = key value store
Key — Value
Version - Metadata
Subresources
Access

S3
object based
Storage
5TB
Limit
Unlimited
Universal namespace
Storage

S3

e/ 99.99 availability built for
e/ 99.9 amazon guarantee availability

/ 11x 9's durability

UNIVERSAL NAMESPACE

Successful uploads will generate HTTP 200

Service
No. Region
IAM + STS
Route 53

Key value } store
object
5TB limit per file
Unlimited

Consistency
- Read after write PUTs
- Eventual Consistency overwrite PUTs / DELETEs
Add new file → read immediately
Existing file overwrite → May see the old version

restrict access to entire bucket → Bucket policy

restrict access to object → Access control

Features
- Tiered Storage
- Lifecycle Management
- Versioning
- Encryption
- ACL + Bucket policy

Storage classes

Standard
e/ 99.99 av
99.11x9 dura
can survive 2 facility loss

S3-IA
rapid access when needed
Cheap

S3-Onezone IA
low cost
one site
really cheap

S3-Intelligent
Depends on usage moves
Minimum 30 day

S3 Glacier
Archive
Data retrieval
min → hour
Min 90 day

Glacier-Deep Archive
lowest + cost
retrieval time
12 h
Min 180 day

Cost / Charged for:
- Storage
- Request
- Storage management
- Data transfer
- Cross region
- Transfer acceleration

optional
Versioning
object tag
Tag
transfer accel
Encrypt
Requester pay

- Bucket policies → note S3 bucket
- can host static website public
- S3 scales automatically

AWS Global Infrastructure

Storage

AWS Cost Management   Migration & Transfer   Compute   Network Delivery   Databases

Security, Identity & Compliance

IAAS / PAAS / SaaS

AWS   godaddy host   Gmail

Support plan

Advantages

- Trade Capital Expense for variable
- Massive economies scale
- Stop guessing about capacity
- Increase speed and agility
- Stop spending money running datacenter
- Go Global

Availability Zone => Datacenter

Free Basic - Community, account + billing

$29 Developer 1 primary contact, 12-24 h response

$100 Business Trusted Advisor, 24x7 chat/phone

$15000 Enterprise TAM

Region

Edge locations => endpoints used for caching.

CloudFront + CDN

150 Edge locations

AWS account

Console

Command line (programmatic)

SDK

S3

object based storage

5TB Limit

Unlimited storage

Universal namespace

~~Cross-origin~~

S3 object = key value store

Key — Value

Version - Metadata

Subresources Access

S3

p/ 99.99 availability built for / 11x9's durability UNIVERSAL NAMESPACE / No. Region
p/ 99.9 amazon guarantee availability + consistency

Service
IAM + S3 + Route53

Successful uploads will generate HTTP 200

Key value } store
object
5TB limit per file
Unlimited

- Read after write PUTs
- Eventual Consistency overwrite PUTs / DELETEs

New file → read immediately
Existing file overwrite → May see the old version

restrict access to entire bucket → Bucket policy

restrict access to object → Access control

Features
- Tiered Storage
- Lifecycle Management
- Versioning
- Encryption
- ACL + Bucket policy

Storage classes

Standard
p/ 99.99 av
99.11x9 dur
can survive 2 facility loss

S3-IA
rapid access when needed
cheap

S3-Onezone IA
low cost
one site
really cheap

S3-Intelligent
Depends on usage moves
Minimum 30 day

S3-Glacier
Archive
Data retrieval min→hour
Min 90 day

Glacier-Deep Archive
lowest + cost
retrieval time 12 h
Min 180 day

Cost / Charged for:
- Storage
- Request
- Storage management
- Data transfer
- Cross region
- Transfer acceleration

optimize
Versioning
object tag
Tag
transfer accel
Encrypt
Requester pay

- Bucket policies → make S3 bucket public
- can host static websites
- S3 scales automatically

AWS Global Infrastructure

Storage

AWS Cost Management Migration & Transfer Compute Network Delivery Databases

Security, Identity & Compliance

IAAS / PAAS / Saas

AWS godaddy hosting Gmail

Support plan

Advantages

- Trade Capital Expense for variable
- Massive economies scale
- Stop guessing about capacity
- Increase speed and agility
- Stop spending money running datacenter
- Go Global

Availability Zone => Datacenter

Free Basic Community account + billing

$29 Developer 1 primary contact 12-24 h response

Region

$100 Business Phone Answer 24x7 chat/phone

$15000 Enterprise Team

Edge locations => endpoints used for caching.

CloudFront + CDN

150 Edge locations

AWS access

Console

Command line (programmatic)

SDK

S3

object based storage

5TB Limit

Unlimited Storage

Universal namespace

~~Operations~~

S3 Object = Key value store

Key — Value

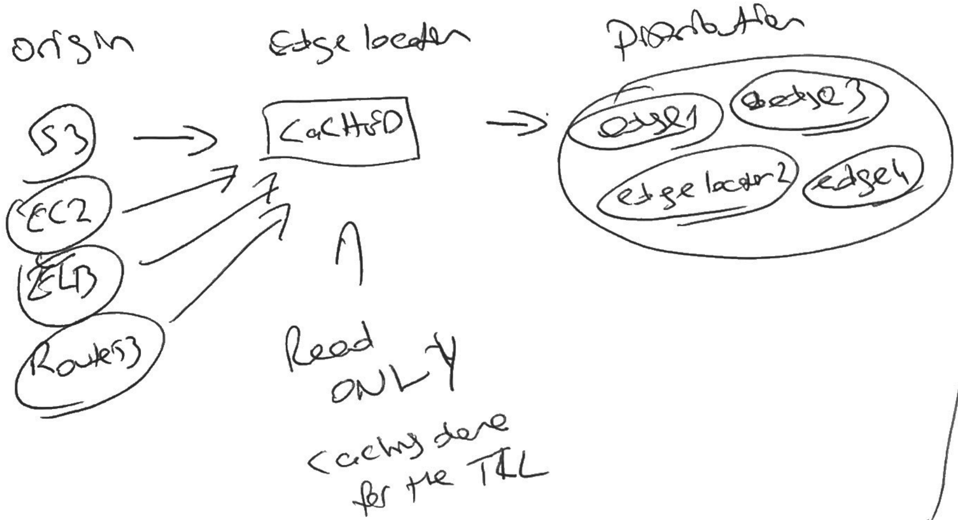
Version - Metadata

Subresources

Access

Cloud front

Web distribution / RTMP (media) flash server



EC2 types

- F1 — Genomics/video
- I3 — Highspeed Storage
- G3 → Graphics
- H1 → High disk throughput
- T3 — lowest cost General
- D2 — Dense Storage — Datawarehouse
- R5 → Memory
- M5 — General purpose
- C5 — Compute
- P3 → General GPU
- X1 → Memory
- Z1D → Memory + CPU

ELB

App load balancer — Layer 7

Network load balancer — Extreme performance / Static IP

Classic — Retiring (Test / Dev)

EC2

- On demand
- Reserved — Standard — Convertible — Scheduled Reserved Instances
- Spot
- Dedicated host — regulatory — per hour — reservation allow

EBS

Block device
(HDD)

SSD — General GP2 — Provisioned Iops IO1

Magnetic — throughput optimized ST1 — Cold HDD SC1 — magnetic (previous)

Using Roles in EC2 I can see access without aws config key

Roles are more secure

Roles are Universal

Architecting for Cloud

Cloud computing difference

1- IT assets becoming programmable resources
2- Global available unlimited
3- Higher level managed services
4- Security built in

DynamoDB for NON RELATIONAL DB for autoscaling

Aurora/MySQL => RDBS

Redshift -> Data warehouse + Business intelligence

S3 Transfer acceleration use AWS network ~~AWS Zones~~ EDGE LOCATION

S3 Flat files

Design ~~principles~~ principles

- Scalability
  - UP number
  - OUT -> load balancer
  - S
  - stateless Apps
  - stateless components (cookies, save state in)
  - stateful components (history)
- Automation
- Loose coupling
  - well defined interfaces
- service discovery
- Database
  - RDS / Aurora
  - Scalable
  - High available
  - Anti-pattern (NoSQL)
- optimize for costs
  - Right sizing
  - Elasticity
- Take advantage of variety of purchasing
  - reserved capacity

- Disposable Resources (cattles)
- Bootstrapping (scripts)
- Golden Images => AMI
- Hybrid of two
- Infra as code

} How

- Asynchronous Integration (SQS)
- Graceful failure apply this
- Services not servers
- Data warehouse redshift
- Search service (Amazon cloud search)
- Remove single point of failure
- Automated Multi datacenter
- Fault isolation + traditional horizontal scaling
  - Sharding
- caching
  - app (elasticache)
  - Edge caching (cloudfront)
- Security

AWS pricing

You pay what you use

- pay as you go
- pay less when you reserve
- pay even less per unit by using more
- pay even less as AWS grows
- Custom pricing

EC2 pricing

- Clock hours of server time
- Machine configuration
- Machine purchase type
- Number of instances
- Load balancing
- Detailed monitoring (every min VS 5 min)
- ~~Auto scaling~~ (pricing EC2)
- Elastic IP
- OS & Software

Free services

- Amazon VPC
- Elastic Beanstalk (resources no)
- Cloud formation
- IAM
- Auto scaling (ec2 you pay)
- Opsworks
- Consolidated billing

3 Charges in AWS

- Compute
- Storage
- Data out

Data transfer IN always free

S3 pricing

- Storage class (Standard or IA)
- Storage
- Request
- Data transfer

RDS pricing

- Clock hours of server time
- Database characteristics
- Database purchase type
- # of instances
- Storage
- Request
- Deployment type
- Data transfer (out)

Cloud front pricing

- Traffic distribution
- Requests
- Data transfer out

Support plans

BASIC	Developer	Business	Enterprise
free	$29	$100	$15000
~~Resources~~	Business hour email support	24-7 email, chat, phone	24-7
	1 person/unlimited case	unlimited	+
	severe <24h	severe <24	TAM
	impaired <12h	impair <12	Prod down <4
		Prod <4 impaired Prod down <4	Prod down <1
			Business down <16 min

Next: Certified Solution Architect

Tags

- Key value pairs
- Metadata
- Can be inherited
  Cloud formation
  EC2 Beanstalk

Consolidated billing ⇒ Volume discounts

Resource groups
make it easy to your resources
using tags

Consolidated Billing
1 bill for all
20 accounts for Consolidated Billing
↑ Limit
Cloud trail: per account
but can aggregated into
a single bucket

Aws quickstart
to get you started

- Aws simple monthly calculator
- Total cost of ownership calculator
  AWS TCO Calculator

Scale up down
ELASTIC
Always Available
High Available

Shared responsibility model
Aws ⇒ security of the cloud
Client ⇒ security in the cloud

AWS Compliance

WAF - SHIELD
App Layer 4
DDOS
Standard layer 3 4
Advanced Layer 7

Customer data
platform, app, IAM
OS, Network, firewall config
Client side data / Server side encryption / Network traffic protection

EMR
Large datasets

AWS RISK COMPLIANCE
- Risk management
- Control environment
- Information security

Inspecter - Advisor
Full trusted advisor
Enterprise
Business

Compute, Storage, Database, Networking
Regions
Edge locations
AZ zones

First AWS service SQS 2004
Official AWS launched 2006
180000 developers in class 2007
Amazon.com move to aws 2010
First re:Invent 2012
Certification launches 2013
(first associate)

Key features of IAM
- Centralled
- Shared access
- Granular perms
- Identity Fed
- MFA
- Temp access
- Rotate pass
- Integrates
- PCI/DSS (credit card)

AWS certified Solutions Architect
ASSOCIATE

IAM
- Users
- Groups
- Policies
- Roles (one part of ms doing something with another write S3 from the ec2

IAM
- Universal
- Root has admin access
- New users NO access
- New users Access key + Secret access are assigned first access
- Access are seen once
- You can create your own pass rotation policies

Power user → access all AWS
But no IAM user/groups

S3 ⇒ Object storage
5TB perfile limit from 0 → 5TB
UNIVERSAL
200 code with plead
Data consistency
Read after upload
Eventual consistency
ACLS

Core fundamentals S3
- Key
- Value
- VersionID
- Metadata
- Subresources
  - ACL
  - Torrent

S3
Built 99.99% availability
Amazon S3 99.99% availability
99.(11x9) durability
S3
Standard
IA IA(one zone)
30 days
Glacier (3-5 hours)
Minimum 90 Days

READ S3 FAQ

Storage Gateway

- On premise ⟹ (upload) AWS (Glacier, S3)
  - virtual appliance
- Available as VMware

Types

1 - File gateway (NFS) pictures videos etc
2 - Volumes Gateway (iSCSI) ← operating system / drives
  - Stored Volume ← entire copy onsite
  - Cached Volume ← only store recently accessed data in premise
3 - Tape Gateway (VTL) in AMAZON

S3

File GATEWAY

- Flat files
- Server ⟷ (NFS) Storage Gateway → (upload internet) S3, S3 IA, Direct Glacier

Volume Gateway

- ISCSI (block based storage)
- Asyncronous, point in time
- Stored as EBS snapshots
- Incremental backups
- Compressed

Volume Gateway - Stored Volume

- Primary data local, async backup to aws (:
- Off site backups (incremental)
- As EBS in S3
- 1 - 16TB in size

Volume Gateway Cached Volume

- S3 as primary storage
  - Frequently accesed only
- Volume up to 32 Tib attaching as iSCSI device
- 1 - 32 Tib cached volume

Tape Gateway

- VTL interface
- leverage existing tape backup
- GW with media changer and tape drives
- Available as iSCSI devices
- Netbackup, Veeam, Backup exec

~~Password~~

S3 2ond AI Availibility of S3 .50

Scalability on current Elasticity added more

Dynamo db query

S3 bucket limit per account 100 buckets

Multipart uploads

Types
SnowBall EDGE
SNowBall
Snowmobile

Exabyte > Petabyte > Terabyte > Megabyte > ... > bit SNOWBALL

Import to S3
Export from S3

Petabyte

SNowBall

- 80 TB Snowball all regions
- 256 bit encryption
- Trusted Platform Module (TPM)
- Auto delete data securely

Snowball Edge

- 100 TB
- onboard storage + compute
- can cluster
- your apps can run on snowball

Snowmobile

- Pete / Exabyte data
- 100 PETABYTE

S3 transfer acceleration

- uses Cloud front edge network to accel uploads to S3

Distant urls ⇒ S3

File upload

EXAM TIPS
Cloud Practitioner

PASSED

AWS Compliance (CLA)
1 – Certification/Attestation (evidence)
2 – Laws et Regulations
3 – Alignment and frameworks

AWS migration services
– Snowball
– Application Discovery Service

AWS Compliance program (IRC)
– Risk management
– Control environment
– Information security

Users are entirely responsable for
AWS IAAS
ec2 – vpc

Scale horizontal
NEW

VPC
↓
Networking & content Delivery

Free to use
1 IAM
2 CloudFormation
3 Elastic Beanstalk
4 Auto Scaling
5 Vpc

Dynamodb
SCAN
find primary key

IAM Groups ⇒ Recomended
- User
- Role
- Permission
- Groups
GURP

Dynamodb Compound keys

Classic load Balancer
Least utilized Record

Round Robin
- ALB1 ratio rule round robin strategy
- Classic TCP only

Classic load Balancer
Cross availability Zone enabled
Default

Lightsail
Platforms
source

Complex queries
petabytes
REDSHIFT

Trusted advisor
- Cost optimization
- fault tolerance
- Performance
- Secure instance
- Security

CFRSS

Auto scaling components
- Policy
- Launch config
- Group
AWS ARN

EC2 101 Remeber

Types FIGHTDRMCPX

F1 I3 G3 H1 T2

D2 R4 M5 C5 P3

X1

EBS

- General purpose (GP2)
  price+performance
  3IOPS per GB up to 10000
- Provisioned (IO1)
  I/O ~~intensive~~ RDBS/NoSQL
  >10.000 Iops
  up to 20.000 per volume

EBS

- Throughput HDD (ST1)
  - No boot
  - Big data
  - Logs
  - Data warehouse
- Cold HDD (SC1)
  infrequent
  Low cost / No Boot

- MAGNETIC
- Lowest price
- BOOTABLE
- Infrequent

AMI

- Termination is off by default
- EBS root cannot be encrypted (only via AMI)
- Root EBS deleted when instance terminated
- Additional volumes can be encrypted
- Security group is a virtual FW

Security Groups ONLY ALLOW All rest denied

All inbound Blocked
Outbound ALLOWED
IMMEDIATE AFFECT
MULTIPLE Security Groups EC2
STATEFUL - if I allow inbound outbound will be allowed
Cannot block specific IP
↳ use Access controll list

Load Balancers

3 TYPES
Application Layer 7
Network Layer 4
ELB (classic) Layer 7-4 X
SG4 → cannot reach to EC2
Behind Load balancer
X-Forwarde → client address

Volumes & Snapshots

Volumes → EBS
Snapshots → S3
point in time
Incremental

Create AMIs → INSTANCES
can change size type
Volumes + EC2 → Same AV zone
Never different

Copy snapshot to another AV zone

Snapshots Encrypted if volume encrypted
Share snapshots if NOT ENCRYPTED
↓ AWS account ↓ public

Snapshot root stop instance #1/6m/6m

Standard cloudwatch Monitoring 5 min
Detailed 1 min

Alarm - treshold passed

Events - respond state changes

Logs - store aggregate, monitor logs

Cloudwatch monitoring //

Cloudtrail → Audit //

1 Subnet → one Availability zone

In service
Out of service ← Load balance

Health check → talk to instance

ONLY DNS one (new ip address)

EC2 placement Groups

Clustered ——— Spread

- Some Availability zone — Multiple
- Unique name in your aws
- only certain types of instances (X, G, M etc) no T instance
- Homogeneous (same) instances
- No merge
- No move existing instances only ami ⇒ move to placement group

EFS

Elastic filesystem

- Storage for EC2 (block based)
- support NFS 4
- Only pay for storage
- Scale to Petabytes
- 1000's of connections
- Stored in Multiple AZ's
- Read after write consistency

Field sensitive
I storage Datawarehouse NOSQL
G graphics ⇒ Video encoding
H High disk output requirements
T general
D Dense storage storage
R memory optimized instance
M general
C compute
P graphics machine learning, bitcoin
X Memory Spot more

Get info on an instance

curl http://169.254.169.254/latest/meta-data/
/user-data/

AWS XEN + Nitro Superviser

DNS

- 4 Billion ip adress IPV4
- ELB ⇒ ONLY DNS (No IP)
- CNAME: NO NAKED DOMAIN
- Choose Alias over CNAME
- Alias Route 53 automatic ip change

Record types
- MX
- PTR ⇒ reverse lookup

- SOA
- NS
- A
- CNAME

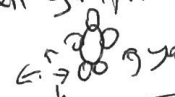
Route policies

- Simple
- weighted
- Latency
- Failover
- Geolocation

[redacted]

SWLGF

Swell girlfriend



Route 53

You can only have 1 entry.
Route 53 returns them in random order

Multiple answer

50 domain limit but can be unlocked by contacting support

Databases 101

Non relational

Collection = Table

Document = Row

Key Value Pairs = Fields

RDS Backups, Multi AZ, Read Replica

Backups

- Automated => recover db "retention time" 1-35 days
- Database Snapshots

Automated Backup — enabled default
- free S3 backup storage
- 1-35 days
- 1 full + incremental (transaction logs)
- Point in time recovery up to 5 min

Snapshots
- Manual
- delete after RDS delete

DynamoDB NoSQL

- SSD Storage
- 3 geographic distinct data centers
- Eventual Consistent Read (Default) (read 1 sec) => best read
- Strongly Consistent read (all writes are confirmed before reading)

Provisioned Throughput Capacity

write throughput $0.0065/h 10 units

Read $0.0065/h 50 units

$0.25 1GB/month

KMS encryption RDS + Backups + Data

↳ existing DB

snapshot => copy => encrypt

Multi AZ

- Oracle
- SQL
- MySQL
- Postres SQL
- MariaDB

Example

Calculation 1M write + Read 3$

Write capacity = (0.0065/10) x 12 x 24 = $0.1872

Read capacity (0.0065/50) x 12 x 24 = $0.0374

Read replica

Asyncronous replication

RDS => read replica

Support
- MySQL
- Postres
- Maria
- Aurora

~~MySQL Oracle~~ NO

Not DR!

Must have Automatic Backup turned on

Up to 5 replicas

Each replica with its own point

CAN MULTI AZ

MULTI AZ => Read

Read replica promoted to be a Database of its own

Redshift

- Petabyte datawarehouse
- 1/10 of the cost
- Columns + Join
- 1 node 160GB
- Multinode
  - Leader node - connection
  - Compute node - work 128 nodes

Columnar Data Storage:

- Data by column
- fewer I/O

Advanced Compression:

column

No Index or materialized views

Massive Parallel Processing (MPP)

Encrypted SSL / AES-256
1 2

HSM → own key

AKMS

$

+ Compute hours across
No leader price

3 node = 2,160 instance hour

+ Backup

+ Data transfer (node VPC)

No Multi AZ

ONLY 1
can restore snapshot

Elasticache

Caches in memory

ELASTICACHE

Memcached

- Object caching

↑

READ Heavy
Not much change

Redis (OLAP)

- Key value store
- Sorted sets of lists
- Master / Slave
- Multi AZ

↑

for analytics processing

Aurora 6

- 5x times Mysql RDBS

Scaling (Auto)

10GB increments 64TB

32 vCPU + 244 GB memory

2 copies of data with 3 AZ

6 Copies of Data

Can survive: loss of 2 write, 3 read

No T instances

starts with R instances

2 replicas

Auto Replicas 15 (auto fail mode)

Mysql Read 5

Databases Summary

RDS ← TRANSACTION ← OLTP

- SQL
- MySQL
- PostgreSQL
- Oracle
- Aurora
- MariaDB

35 Days retention

DYNAMODB - NOSQL

- push button scaling
- SSD Storage
- 1EU consistency Reads ← write slow
- Strong consistent Read ← write immediate

Datawarehouse

↓ ANALITIC

OLAP

REDSHIFT - DATAWARE House

Single node (160GB)

Leader

Compute

ELASTICCache - INMEMORY

- Memcached
- Redis

Aurora 6 copies

2 write } failure
3 read }

Aurora replica

Mysql Red replica