AWS Cloud Practitioner

- On demand self service.
- Broad network access.
- Resource pooling.
- Rapid elasticity. (grow or shrink on demand)
- Measured service (pay for what we use)

Service Models

- IaaS – Infrastructure as a Service
- PaaS – Product as a Service
- SaaS – Software as a Service

Infrastructure & Applications

- Resiliency • Security • Durability • Performance
- Cost-effectiveness • Scalability • Automation

Process & Workflow:

- Agile • Flexible • Efficient • Secure

Business:

- Secure • Low CapEx • No long term commitments
- Fast time to market.

AWS Provides:

- On demand resources.
- Pay as you go.
- No long term commitments.
- Highly automated.
- Managed services.

Benefits:

- OpEx over CapEx
- Gain flexibility, agility.
- Immediate scalability.
- Lower time to market.
- lower upfront cost.
- Easier cost allocation.
- Stop running datacenters.

AWS Global Infra

Choosing a Region:

- Available services
- Cost of services
- Latency
- Disaster recovery
- Security and compliance

Availability zone (A-Z): Collection of Data Centers.

Edge location: Content is cached at Edge locations.

Well Architectured Infrastructure

- Reliable : Fault Tolerance ; High availability ; Durability;
- Secure ; ; Cost Effectiveness ;
- Performant ;
- Operationally Excellent: Monitored ; Automated.

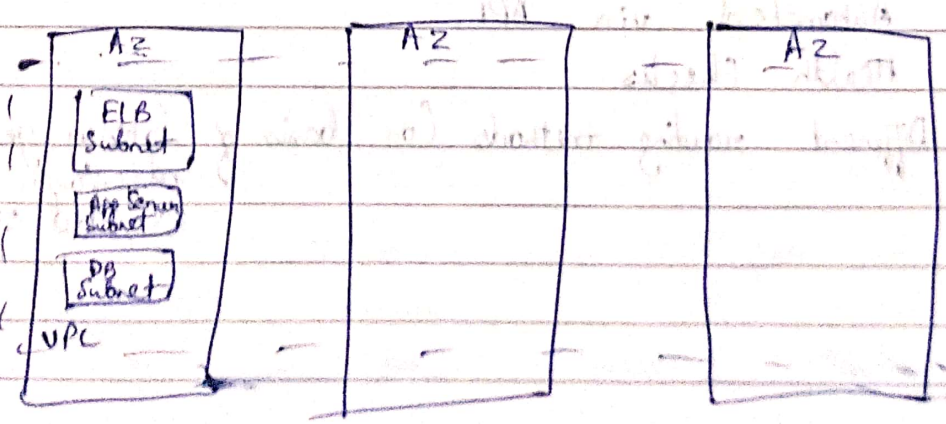
Amazon VPC:

- Logically Isolated network.
- Created per account per region.
- Spans a single region.
- Can use all AZs within one region.
- Can peer with other VPCs.
- Internet and VPN gateways.
- Numerous security mech.

Subnet: We launch applications in a subnet not directly in a VPC. They are specific to one AZ

3-Tier Architecture:

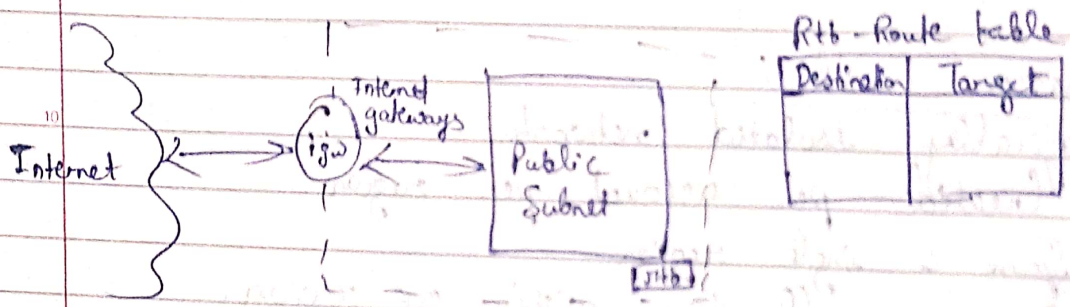
- Load Balancing tier
- Application tier
- Database tier.



Subnet Enables:

- Secure via isolation.
- High Availability.
- Fault Tolerance.
- Performance.

Routing:



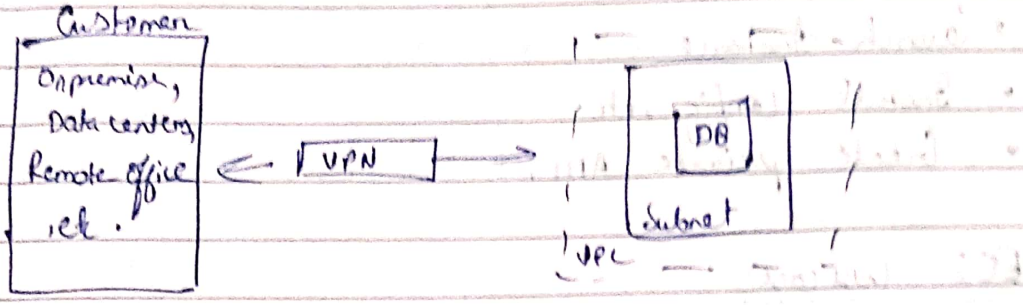
Network Access Control List (NACLs) : Firewalls for entire subnet as whole.

Security Groups : Firewall for individual machines. i.e instances or databases.

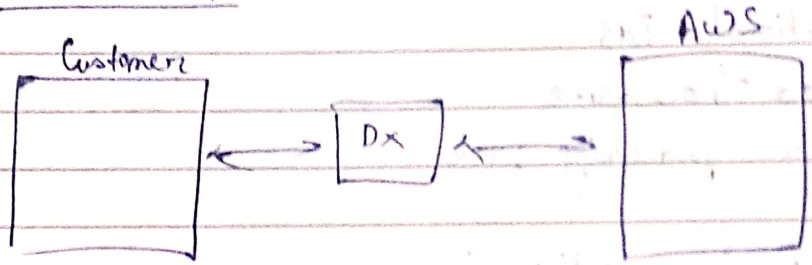
Amazon Route 53 : DNS Service

- Register Domain
- Use AWS nameservers
- Public and private DNS zones.
- Automated via API.
- Health Checks
- Different routing methods (on basis of latency, geography and percentage of weighted sets)

AWS Hardware VPN:



AWS Direct Connect:



Amazon EC2:

- Virtual machines (Instance)
- Our choice of OS
- Combination of CPU, memory, disk, IO.
- Launch one to thousands
- Different billing models
- AWS Marketplace offers canned solutions.

Amazon Machine Image (AMI):

- Bit for bit copy of root.
- Choice of OS
- We can find AMIs from AWS provided, AWS marketplace, Community.

Launching an Instance:

- Choose AMI
- Launch Instance
- Install, Config., etc
- Create private AMI.

EC2 use cases:

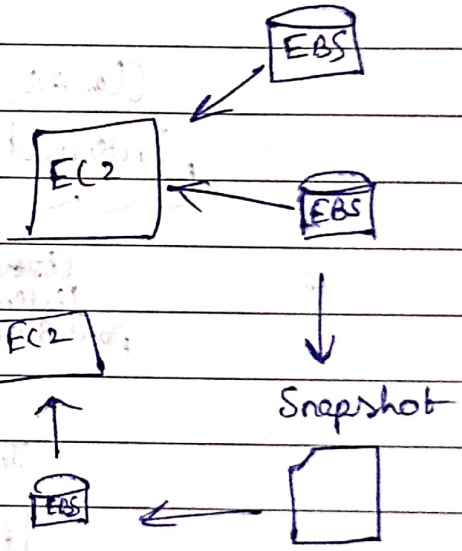
- Enterprice application
- Web servers
- Relational DB
- Video transcoding
- Batch processing, etc

EC2 Best practices:

- Treat as dispesable.
- Immutable Infrastructure.
- Treat logs as streams.
- Leverage roles.
- Automate Deployment.
- Monitor with CloudWatch.
- Enable scaling and self healing with Auto Scaling.

Block Storage :	Object Storage
• Update volume blocks with relevant bits	• Upload entire 10 GB file
• Uses more efficient protocols	• Uses HTTPs for transfer.
• Can be mounted.	• Can't be mounted.
• Best for radom IO	• No radom IO.

Amazon Elastic Block Store (EBS):

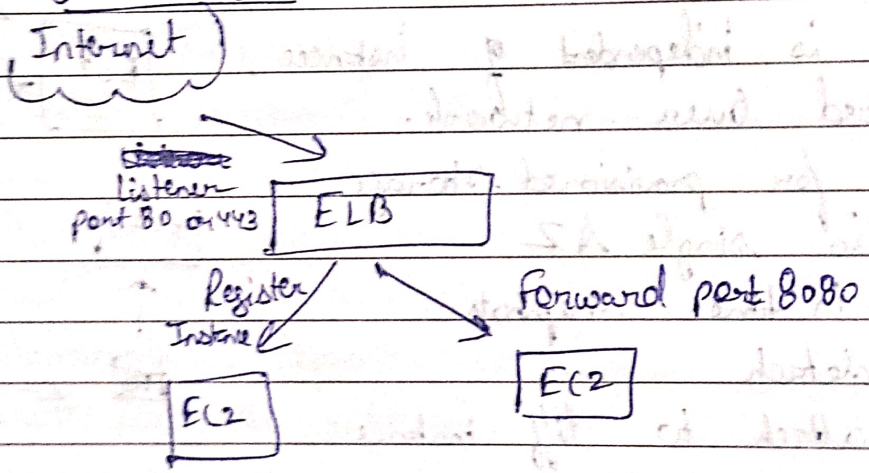


- Data is independent of instance.
- Connected over network.
- Pay for provisioned storage.
- Exist in single AZ
- Point in time snapshots.
- Can detach
- Can attach to diff instance.
- Can be encrypted.
- Can be used in RAID.
- If you need file system or radom IO.
- It provides durability.

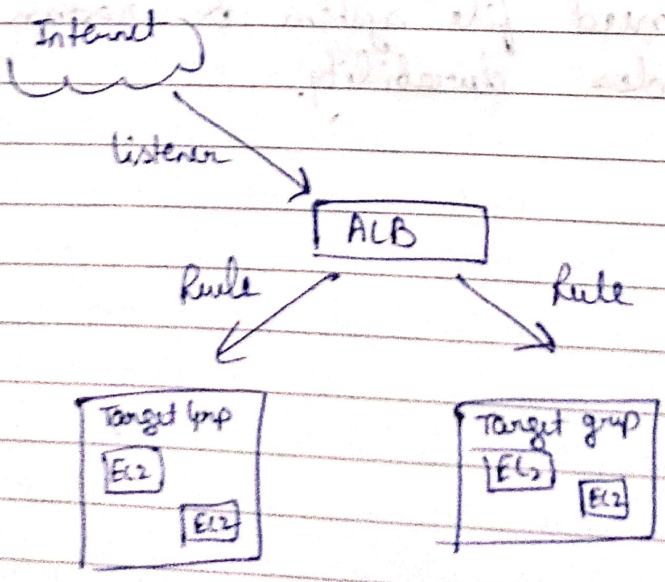
Elastic load Balancing (ELB):

- Distributes health check.
- Spans region
- Inherently secure, resilient and scalable.
- Supports health check.
- Integrates with Auto scaling.
- Integrates with Route 53.
- 3 types: • Classic
  • Application
  • Network

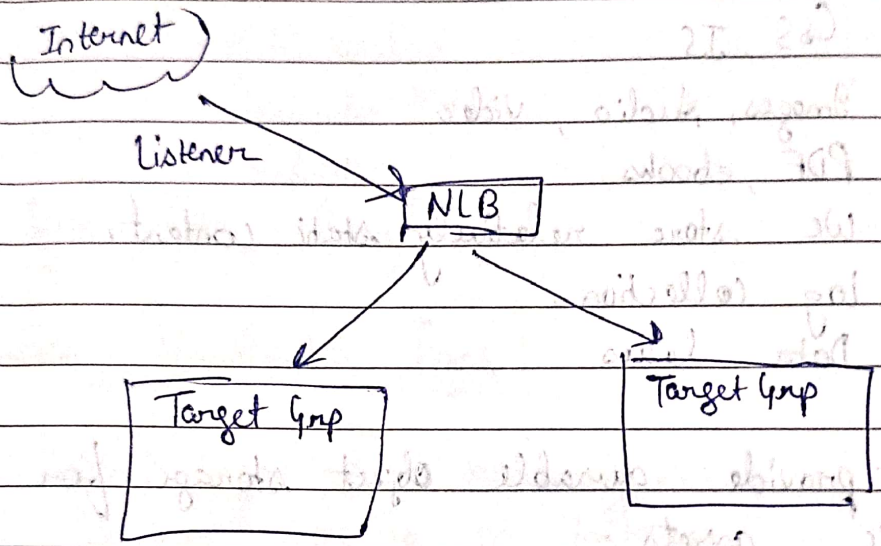
Classic LB:



Application LB:



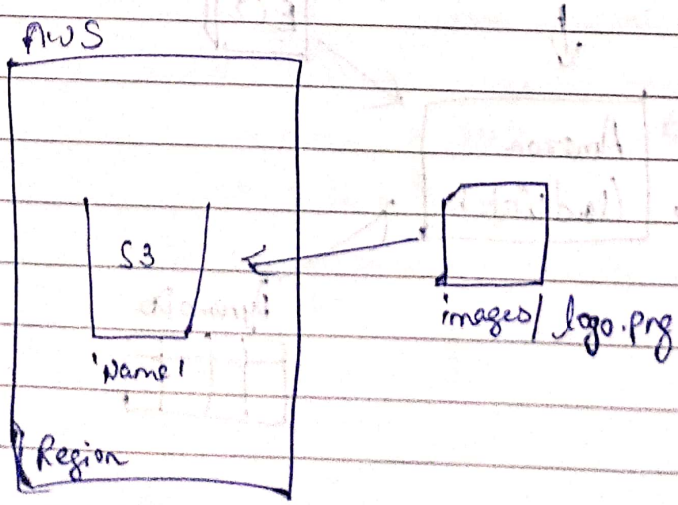
Network LB



- ELB enables secure, fault tolerant operation of application.

Amazon Simple Storage Service (S3)

- Object storage.
- Buckets and objects
- Cluster span region
- Durable to loss of 2 AZ.
- Server Side Encryption.



S3 use cases

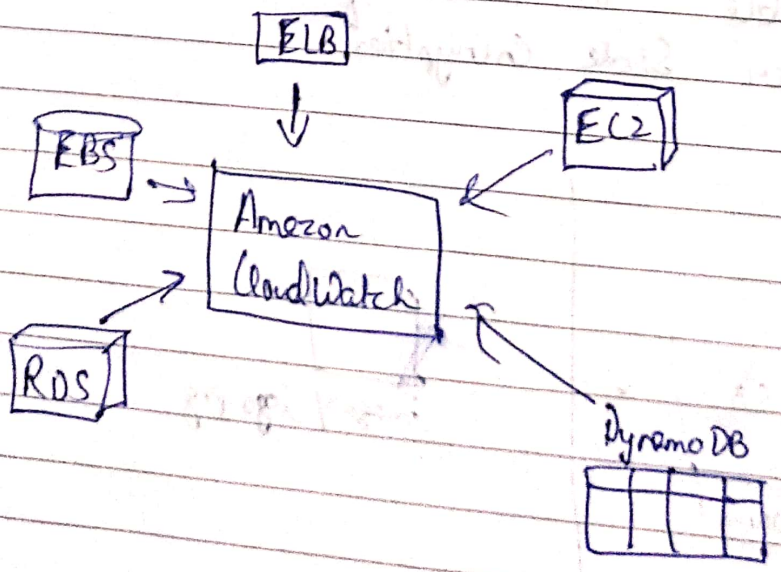
- Host Static HTML
- CSS, JS
- Images, Audio, Video
- PDF, ebooks
- We store relatively static content.
- log collection.
- Data lakes

- S3 provide durable object storage for static assets.

Advanced Core Services:

Amazon Cloudwatch:

- Collects metrics
- Stores metrics for 2 weeks.
- Accessible via API.
- Unique metrics set per service.
- Custom metrics.



Amazon Cloudwatch Alarms:

- Triggered on breach of threshold
- Can trigger:
  - Auto Scaling
  - Termination
  - Reboot
- Upto 5000 alarms/acc

Amazon Cloudwatch logs:

- Collect logs by streaming
- Configure agents on instances
- Collect Route 53 DNS queries
- Monitor CloudTrail Events
- Default retention indefinite
- Can archive to Amazon S3
- Stream to Amazon Elastic Search
- Process with lambda

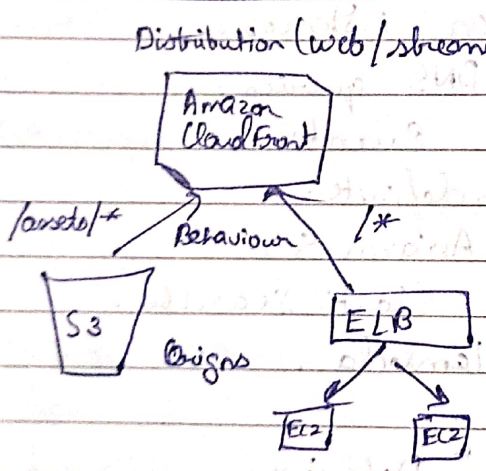
Search and filtering log Data:

- Search using specific syntax
- Create metric filters
  - Counts as custom metrics
  - Create alarms such as
    - No. of 404s
    - Bytes transferred
    - Customer conversions
    - No. of exceptions

Auto Scaling

- Replaces failed instances.
- Change capacity acc to load.
- Maintains fixed size fleet.
- Works with Amazon Cloudwatch.
- Events :
  - SNS
  - Lambda

Amazon Cloud Front :



- Caches content at Edge location.
- Static & dynamic content
- Customizable cache behavior
- Custom domain name.
- Custome SSL Certificates.
- RTMP and HLS streaming

Cached content improves end user's experience.

AWS Lambda:

- Serverless Infrastructure.
- Great for:
  - Scheduled tasks
  - Microservice
  - Event handlers
- Pay for compute time per 100ms
- Create functions.
- Invoke functions
  - CLI or SDK.
  - Events.
- Amazon handles:
  - Infrastructure
  - Deployment
  - Scaling

Lambda provides serverless, event-driven computing.

Amazon Relational Database Service (RDS):

Benefits:

- Choice of:
  - MySQL
  - SQL Servers
  - Oracle
  - PostgreSQL
  - MariaDB
  - Amazon Aurora.
- Reduces operational Burden.
- Focus on application.
- Read replicas.
- Automation.
  - Backups
  - Failovers
  - Os installation and patch

Database Migration:

- Dump & import.
- Backup / restore.

- **AWS Database Migration Service:**
  - Support widely used DBs.
  - Heterogeneous / Homogeneous DBs.
  - Virtually zero down time.
  - Schema Conversion tool.
  - Consolidate DBs.
  - Continuous replications.

Amazon DynamoDB:

- NoSql DataStore.
- Exclusively backed by SSD.
- Single digit ms response.
- Built-in security, resilience.
- Replicated across multiple AZs.
- No limit to storage or throughput.
- Provisioned throughput.
  - Read. Writes. Can auto scale

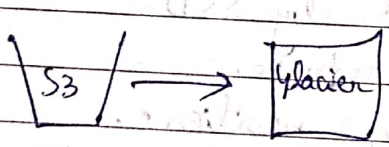
Amazon DynamoDB Table:

- Tables, items, attributes.
- No joins / relationship.
- Schema-less.
- key value & documents
- Unique primary key req.
- Secondary indexes.
- No table size limit.
- 400kB item size limit.
- Item level Time-to-live (TTL).

DynamoDB Use cases:
- AD impressions
- Gaming leaderboard
- Shopping carts
- Operational state / history.

Amazon Glacier:
- Archival storage
- Lower cost vs S3
- Write archives
  - Transition from S3
  - Direct upload.
- Download via retrieval req
  - 3-4 hr wait
  - pay for faster retrieval

Lifecycles Rules:



Amazon Redshift:
- Pb scale data warehouse.
- Fully managed.
- Fork of PostgreSQL
- SQL Compliant
- Parallel queries.
- Ideal OLAP & BI application

OLAP - Online Analytical Processing

Other Services

Info of Automation:

- Manual process is:
  - Slow • Unreliable • Difficult to repeat
  - Lack of documentation • less secure
- Automation is:
  - Fast & efficient • Reliable & consistent
  - Repeatable • Documentation is inherited
  - Secure.

Tools for Automation:

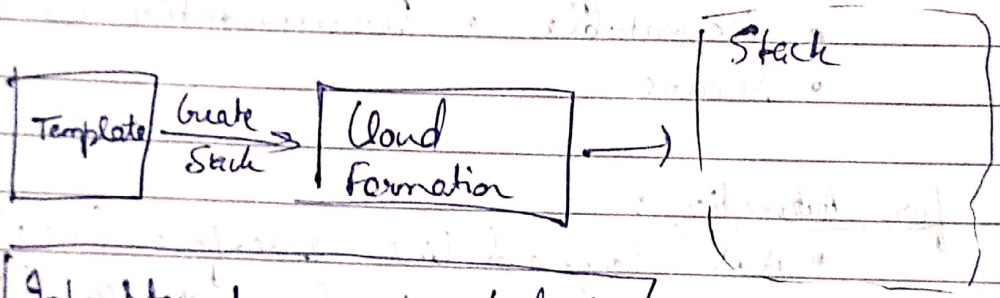
- AWS Command line Interface (CLI)
- AWS Software Development kits (SDK)
- AWS Cloud Formation.
- AWS Elastic Beanstalk
- AWS Ops Work

AWS Elastic Beanstalk:

- Application management platform.
- Provides easy entry
- Choice of:
  - Java • .NET • Node.js • Docker
- Simply upload application
- Ideal for developers
- Automatically handles
  - Capacity provisioning • load balancing
  - Auto scaling • Monitoring • Deployment

AWS Cloud Formation

- Templates based infra management.
- Declarative programming.
- Offer access to full breadth of AWS
- Store in source control.
- Write once deploy many.
- Library for common architecture.
- No imposed model.



Infrastructure as code:

AWS WAF : Web Application Firewall.

- Layer 7 content filtering.
- Support rules to block/allow/count
- Integrates with Amazon CloudFront
- Protect against:
  - SQL Injection
  - Cross site scripting.
- Block based on
  - IP address
  - HTTP headers | body
  - URI strings.
- Rate limiting per client IP.
- Managed rules for common threats:
  - OWASP
  - Bots
  - Common Vulnerabilities and Exposures (CVE).

AWS Shield:

- Distributed Denial of service (DDoS) protection service.
- Standard
  - UDP reflection
  - SYN floods
  - SSL renegotiation.
  - Slow loris attack.

AWS Shield Advanced:

- Additional detection/ mitigation.
- Near real time visibility.
- Integrates with AWS WAF.
- Access to DDoS Response Team.

IAM Policies:

- Determine authorization
- Written in JSON.

IAM Roles:

- Use temporary credentials.

IAM Best Practices

- Root credentials
  - Email address + password • Protect at all cost • Do not use for day-to-day
- Follow principle of least privilege.
- Rotate access keys.
- Enable MFA
- Monitor with CloudTrail.

AWS Organisation:

- Eases management of multiple AWS account.
- Automate creation of AWS accounts.
- Service Control Policies control service use.

Consolidated & detailed billing

- Consolidated billing:
  - One bill many acc.
  - Aggregated volume pricing.
  - Reserved instances apply to all acc.
- Detailed Billing:
  - Published to S3.
  - Import into spreadsheet.
  - Filter/sort by service, tag, etc.

AWS Assurance programs:

- Certifications
- Laws/Regulation/Privacy
- Alignments/Frameworks

AWS Config:

- Resource inventory
- Configuration history
- Change notif
- Determine compliance against rules
- Enable:
  - Compliance auditing
  - Security analysis
  - Change tracking

AWS Service Catalog:
- Manage catalogs of approved IT servics.
- Achieve consistent Governance.

AWS Artifacts:
- Access reports of >2500 security control.
- On demand access to AWS security and compliance documents.

AWS Cloudtrail:
- Records all call made to AWS API.
- Delivers log files to S3 bucket.
- Includes:
  - Identity
  - Source IP
  - Request/Response detail.
- Does not record:
  - OS system logs
  - DB queries.

- AWS key Management Service (KMS):
  - Fully managed
  - Create/Manage encryption keys.
  - Integrates with many other services.
  - Multi tenant software backed by HSMs.

- AWS Cloud HSM:
  - Single tenant Hardware Security model.

Vulnerability / Penetration Testing

- Permission is req.
- Must request permission via root credentials.
- Identify instances to be tested.
- Specify start & end date/time.
- AWS doesn't permit testing of:
  - m/c.small
  - t2.micro
  - t2.nano
- AWS policy permits:
  - EC2 • RDS • Aurora • CloudFront
  - API Gateway • Lambda • Lightsail
  - DNS Zone walking.

AWS Pricing

- Compute Pricing

EC2: On demand pricing
- No long term commitments
- Transform large fixed costs into smaller variable cost.
- Fee include OS license.
- Per hour billed hour forward
- Per second min 60 sec.

EC2 Reserved Instances:
- Upto 75% discount vs On demand.
- Provide capacity reservation.
- 1 or 3yr term
- Attributes:
  - Instance type • Platform • Tenancy • AZ

Types of Reserved Instance Types

- Standard RIs:
  - Upto 75% off on-demand
  - Best for steady state usage
- Convertible RIs:
  - Can change attributes of instances
  - Upto 54% off on Demand.
  - Best for steady state usage
- Scheduled RIs:
  - Available during time window.
  - Best for predictable, recurring schedule.

EC2 spot pricing:

- Gain discount on spare capacity.
- Save upto 90%.
- Price
  - Set by instance type + AZ
  - Determined by supply / demand.
- Spot instances can be interrupted
- Great for apps with flexible Start / end times.
- Development / test environment.
- Use for:
  - Image rendering
  - video processing.
  - Analytics / ML

AWS Lambda Pricing:
- Charged per GB per 100ms
- Charged per 1M req/
- Free tier:
  - 1M req/month
  - 400000 GB-Sec/month
- Addn charges for
  - Bandwidth
  - Amazon S3.

Data transfer pricing:
- Inbound generally free.
- S3 to Cloudfront is free
- Outbound to internet
  - $/GB/month
  - Applies cross regio traffic
  - Tiered pricing.
- Cross AZ traffic $/GB/month.
- VPC peering $/GB/month.

Database Pricing:

RDS pricing:
- Price determined by:
  - Instance type
  - Database engine
  - Reserved instance discount
- Multi AZ deployments 2x $
- Storage
  - $/GB/month
  - $/provisioned IOPS/month

Dynamo DB pricing:

- Charged for provisioned throughput
  - $/ write capacity unit
  - $ / Read capacity unit.
- Charged for storage Consumed.
  - $/GB/month

Storage pricing:

EBS pricing:

- $/GB/month of provisioned storage
  - General purpose SSD.
  - Provisioned IOPS storage
  - Magnetic volumes.
- Additional costs for:
  - $/provisioned IOPs.
  - EBS snapshots to S3.

S3 pricing:

- $/GB/month of consumed storage
- Additional costs for req:
  - PUT, COPY, POST, LIST $/1000
  - GET. $/1000
- Storage access:
  - Infrequent Access
  - Glacier.

AWS Trusted Advisor

- Automatically analyzes environment
- Offer best practice recommendation
- Cost optimization
- Performance
- Security
- Fault Tolerance.

Seven Core Checks

- S3 Bucket permission
- Security grp "
- IAM use
- MFA on root acc
- EBS public SS
- RDS " "
- Service limits.