|  |  |  |
| --- | --- | --- |
| Pillar | Design Principal | AWS Services |
| Operational Excellence | * Perform operation as code. * Annotate document. * Make frequent small reversable changes. * Refine operation procedure. * Anticipate failure. * Learn from failures |  |
| Security | * Strong identity foundation -IAM * Enable traceability – logs and metrics. * Apply security at all layers – edge network VPC. * Automate security. * Protect data in transit and rest. * Keep people away from data. * Prepare for security events – use tools for automating testing |  |
| Reliability | * Test recovery procedures. * Automatically recover from failure * Scale horizontally. * Stop guessing capacity. * Manage change in automation |  |
| Performance Efficiency | * Use/ democratize advance technologies. * Go global in minutes. * Use serverless architecture. * Experiment more often. * Mechanical sympathy |  |
| Cost Optimization | * Adopt consumption mode, pay for what u use. * Measure overall efficiency. * Stop spending money on data centre operations. * Analyse attribute expenditure – use tags. * Use managed and application-level service to reduce cost ownership. |  |
| Sustainability | * Establish sustainability goals. * Maximize utilization. * Anticipate and adopt newer solutions. * Use managed services. * Reduce the downstream impact of your cloud architecture. |  |

|  |  |  |
| --- | --- | --- |
| Database | | |
| Service | Use | Use Case/ Keyword |
| Amazon Aurora | * Relational database – SQL – AWS OWNS IT * Supports PostgreSQL and mysql, cloud optimized. * 5x better than mysql and 3x better than PostgreSQL on RDS * AUTO GROW IN 10GB up to 128 GB. * MORE EFFICIENT than RDS * NEED SERVER., costs money | **MORE CLOUD NATIVE** |
| Amazon DynamoDB | * NO RDS, low cost * Managed, Autoscaling SCALES MASSIVELY, NO SERVERS (NO EC2) * FAST, 100 TB Storage * LOW LATENCY. Integrated with IAM for security. * Has standard and infrequent Table class * FLEXIBLE SCHEMA | **KEY VALUE DATABASE**  **SUPPORTS HIGH AVAILABILITY** |
| Amazon ElastiCache | * Managed Redis and Memcached database * Reduce load on database for read intensive tasks. * AWS takes care of OS maintenance patching optimizations. * Takes and gives from cache for read intensive tasks | **ELB -> EC2 -> Elasticache /RDS.**  High performance, low latency |
| Amazon RDS | * OS patching taken care off by AWS. * Continuous backup according to time stamp, dashboard, improved read performance with read replica. * cannot SSH to instance, can be scaled vertically and horizontally * Storage backed by EBS | **ELB -> EC2 -> RDS**  FREE. TO CREATE Relational DATABSE.  **cannot be used as an in-memory database.**  **READ REPLICA IMPROVES SCALABILITY** |
| Amazon Redshift | * For analytics and data warehousing * Load data every 1 hr. * Pay as u go. * Has SQL interface for queries | Integrated with quicksight.  10x better performance, scale to pb of data |
| Amazon DocumentDB | * Fully manged noSQL * Replication up to 3 AZ * Highly available * Scales to workload with millions of requests per second * Grows in increments of 10gb up to 64tb. * Automatically scales workloads. | **MONGODB** |

|  |  |  |
| --- | --- | --- |
| VPC | | |
| Service | Use | Use Case/ Keyword |
| VPC | * Private network to deploy ur resources, regional |  |
| Subnets | * Allow u to partition network inside VPC.   Public Subnet   * Accessible from the internet   Private subnet   * Not accessible from the internet | TO define access to internet and between subnets  Use ROUTE TABLES |
| Internet Gateway | * Connects public VPC instances to the internet. * Public subnet got a route to the internet gateway. |  |
| Nat Gateway | * Connects private subnet to internet | **Nat must be created in public subnet.**  **Private subnet >> Nat gateway>> internet gateway>. internet** |
| Network ACL | * A firewall that controls traffic from and to subnet * CAN HAVE ALLOW AND DENY RULES * Filter traffic in and out * Rules can be IP addresses only. * **A network access control list (network ACL) contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic** | SUBNET LEVEL |
| Security groups | * Controls traffic in and out of EC2 * Can have Allow rules. * Rules include IP address and other security groups. * **A security group is stateful, that is, it automatically allows the return traffic.** | EC2 INSTANCE LEVEL |
| VPC FLOW LOG | * Capture information about IP TRAFFIC in our interface. * VPC Flow Logs * Subnet Flow Logs * Elastic network interface | MONITOR AND TROUBLESHOOT CONNECTIVITY ISSUES |
| VPC peering | * Connect 2 VPC privately using AWS. * Make them behave as if they were from the same network. | CANNOT HAVE OVERLAPPING IP A-> B B-> C C CANNOT TALK TO A  A NEED TO BE CONNECTED TO C  gets difficult to manage. |
| VPC endpoint | * Connect to AWS services using private network. * GIVES U BETTER SECURITY AND LOWER LATENCY   VPC Endpoint Gateway -> for S3 AND DYNAMODB ONLY  VPC Endpoint Interface -> for the rest |  |
| PrivateLink | * If u want to use services running on 3rd party VPC like from marketplace * Ask Vendor to private link to you VPC | Vendors create Network Load balancer  U create Elastic network interface  Use both and create PRIVATELINK |
| ClientVPN | * U have your own computer and want to privately connect to AWS VPC * Use OpenVPN * Goes over public internet. * Connects to EC2 OVER PRIVATE IP |  |
| Transite Gateway | * Connect thousands of VPC and more | STAR  A WAY TO CONNECT 1000 OF VPC WITH ON PREMISES |

|  |  |  |
| --- | --- | --- |
| Analytics | | |
| Service | Use | Use Case/ Keyword |
| Amazon Athena | * Makes it easy to analyse data in S3 using SQL. * SERVERLESS ONLY PAY FOR QUIRIES U RUN * helps you analyse unstructured, semi-structured, and structured data stored in Amazon S3 * integrates with Amazon QuickSight for easy data visualization | Generate reports or to explore data with business intelligence tools or SQL clients. |
| Amazon Kinesis | * Realtime big data streaming * Cost-effectively processes and analyses streaming data. * Handle any amount of streaming data from thousands of sources and process it with low latencies. | Apps for application monitoring, fraud detection |
| Amazon QuickSight | * Business intelligence service * Build interactive dashboards and visualizations. * Automatically scalable | Data Exploration, Data Visualization |
| Neptune | * Manged graph database * 3 AZ 15 read replicas * powerful and fully managed graph database service that simplifies the development and management of graph-based applications. |  |
| QLDB | * RECORDING OF FINANCIAL TRANSACTION * Used to review history of all changes u made to application. * No decentralized component | **IMUTABLE**  **FINANCIAL TRANSACTION/LEDGER** |
| Manged Block chain | * Build application for people to execute transaction without a central authority. * Can join public block chain. * Or create own | **ETHEREUM**  **HYPERLEDGER FABRIC** |
| GLUE | * Prepare and transform data for analytics. * Fully serverless service * Take from s3, or RDS transform using glue load to redshift database | **ETL, EXTRACT TRANSFORM LOAD SERVICE** |
| DMS / DATABASE MIGRATION SERVICE | * Helps in databse migration by making it quick and secure. * Make it resilent and slef healing. * Eveeyrhting remains available during migration. | **MIGRATION OF DATABASE** |

|  |  |  |
| --- | --- | --- |
| Application Integration | | |
| Service | Use | Use Case/ Keyword |
| Amazon Elastic Container Service (Amazon ECS) | * Used to launch docker containers. * Must provision and maintain infrastructure Ur self. * AWS will start and stop it. * Has integration with ALB for u to create web application | **RUN DOCKER CONTAINER ON AWS** |
| Amazon Elastic Kubernetes Service (Amazon EKS) | * Run and deploy Kubernetes on the cloud. * Auto manage the availability and scalability |  |
| AWS Fargate | * Launch docker container but NO PROVISIONING NEEDED | Bttr than ECS  RUN DOCKER CONTAINER ON AWS WHEN U D W PROVISION ANYTHING |

|  |  |  |
| --- | --- | --- |
| Machine learning | | |
| Service | Use | Use Case/ Keyword |
| Rekognition | * Used to identify People, text, scenes in images | Facial analysis, labelling detection, ect |
| Transcribe | * Convert speech to text using automatic speech recognition (ASR) * Remove personal details (PII) using Redaction. * Supports Automatic Language Identification | Speech to text |
| Polly | * Opposite of transcribe text to speech | Allow u to create talking applications |
| Translate | * Natural Accurate language translation | Helps u localise content for international audience |
| Lex | * Automatic Speech recognition * Natural Language understanding to recognize the intent of text/call | Tech that powers Alexa and helps u build chatbots and call center bots |
| Connect | * Receive calls, create flow to solve their requests. * No upfront payment 80% cheaper than other solutions | Build call/contact centers |
| Comprehend | * Fully manged and serverless * Can understand language, key phrases, text tone + or – organize text file by topics | **Natural Language Processing -> NLP**  Analyse Customer interactions |
| SageMaker | * Fully manged for developers to build ML models | Predicting exam scores |
| Forecast | * 50% more accurate * Reduce time taken to forecast from months to hours | Predict future sale of raincoats.  Financial planning. |
| Kendra | * Document search service using ML, Extract Answers from documents * Put in documents from diff resources and it will learn from it and answer ur questions. * Learn from user’s instructions/feedback | **Document Search service** |
| Personalize | * Build apps with Realtime personalized recommendations. * Read from S3 where ur activity is stored and use PERSONALIZE API to send stuff to Personalize | Amazon recommending similar stuff to the stuff u buy.  **ML service to build recommendation** |
| Textract | * Extract Text from anything being scanned | Extract data from forms and tables |

|  |  |  |
| --- | --- | --- |
| Developer Tools: | | |
| Service | Use | Use Case/ Keyword |
| AWS CodeBuild | * compiles source code, runs tests, and produces ready-to-deploy software package | TAKE FROM CODECOMMIT -> CODE BUILD -> CREATE PACKGES TO BE DEPLOYED. |
| AWS CodeCommit | * secure, highly scalable, fully managed source control service that hosts private Git repositories | Like GITHUB |
| AWS CodeDeploy | * fully managed deployment service that automates software deployment * automate software deployments, eliminating the need for error-prone manual operations | SOURCE >> BUILD >> TEST >> STAGING >> PRODUCTION |
| AWS CodePipeline | * continuous delivery service that helps you automate your release pipelines for fast and reliable application. * CICD. | Serverless CRON JOB: define schedule run a script, |
| Cloud 9 | * IDE Used within web borwser. * Allows code collaboration like google docs. * Like vs code | Cloud ide |
| AWS CodeStar | * quickly develop, build, and deploy applications on AWS. * easy for your whole team to work together securely. * Project Templates, Integrated Tools: AWS CodeCommit (version control), AWS CodeBuild (build automation), AWS CodeDeploy (deployment automation), and AWS CodePipeline | * UNIFIED UI TO MANAGE SOFTWARE DEV ACTIVITIES IN ONE PLACE. |

|  |  |  |
| --- | --- | --- |
| Management, Monitoring, and Governance: | | |
| Service | Use | Use Case/ Keyword |
| AWS Auto Scaling | * Monitors and adjust capacity to maintain performance at lowest possible price |  |
| AWS Budgets | * set budget to track cost and usage. * can choose to be alerted by email or sns when ur about to exceed limit. |  |
| AWS CloudFormation | * The CloudFormation template is like a set of instructions for AWS to follow. It tells AWS which resources you want to create (like servers, databases, storage, etc.), how they should be configured, and how they should connect to each other. It's like giving a to-do list to AWS. * Leverage existing templates. | Infrastructure is on code.  cost saving, Easy to create and destroy infrastructure |
| AWS CloudTrail | * Track user activity and api calls, records accnt activity across AWS. * auditing service (who did what and when) | Security and Compliance, Troubleshooting and Debugging, |
| Amazon CloudWatch Metrics | * have timestamp, can create cloud watch dashboards for metrics. Default every 5 min can make every 1 min if u pay. * CloudWatch as a performance monitoring service (how much resource was used |  |
| Amazon CloudWatch Alarms | * used to trigger notification for any metric * increase or decrease EC2 for auto scaling * send SNS notification |  |
| Amazon CloudWatch Logs | * collect from ecs, lambda, CloudTrail, CloudWatch log agent, rout53 for DNS queries. * . IAM needed | NEED TO RUN AGENT FOR THING TO GO INTO LOGS |
| AWS Config | * recording config and changes overtime * Can be stored in S3 to be analysed by Athena * Can receive SNS for changes * Helps maintain compliance * CAN SEE COMPLIANCE OVER TIME * CAN SEE WHO MADE CHANGES WITH CLOUD TRAIL | PER REGION THING  NOT FREE |
| AWS Cost and Usage Report | * publishes your AWS billing reports TO S3 * tracks your AWS usage and provides estimated charges * gain better visibility into your AWS spending patterns | customize TO BE either by the hour, day, or month. |
| Amazon EventBridge | * simplifies the building and management of event-driven applications by allowing different AWS services * custom applications to communicate with each other through events. * object being created in an S3 bucket, a new message arriving in an Amazon SQS queue, or a new record being added to an Amazon DynamoDB table. | SaaS |
| AWS Managed Services | * helps you manage your software licenses in the AWS * keeps u within license restriction, can use ur own one and not use aws one, centralized dashboard | ALLOW BUISSNESS TO TAKE CARE OF INNOVATION BY TAKING CARE OF INFRASTRUCTURE |
| AWS License Manager | * organizations migrate, operate, and optimize their workloads in the AWS cloud in a managed and secure manner. * Simplify adaptation of cloud |  |
| AWS Organizations | * centrally manage and govern multiple AWS accounts as a single entity * reserved instance can be shared * restrict account privileges using service control policies (SCP). * resource ISOLATION like VPC needs multi accnt * uses tagging standard for billing purposes * MUST enable CloudTrail on all ACCOUNTS * ADD cloudwatch logs to central logging account | API is avail to automate accnt creations  PER ACCNT SERVICE LIMITS, ISOLATED ACCOUNT FOR LOGGING |
| AWS Secrets Manager | * Enables u to rotate and manage credential, like API key and other secrets. |  |
| AWS Systems Manager | * Get insights abt ur infastructure * automates tasks across AWS resources, manage EC2 AND ON- PREM STUFF * Need install ssm agent * For Amazon AMI it is already installed | **PATCHING FLEET OF EC2 INSTANCES or RUN CMD CONSISTANTLY ACROSS ALL SERVERS**  **UNIFIED UI** |
| AWS Systems Manager Parameter Store | * store and manage configuration data and secrets * secure key-value store for sensitive information |  |
| AWS Trusted Advisor | * High level accnt assessment * Support plans: S3 bucket permission, Security groups to see if specific ports are unrestricted, IAM USE- one user at least, MFA on root accnt, EBS public snapshots, RDS public Snapshots, (can cause data leak) Service limits. * automated advisor * having a helpful consultant that examines your AWS setup and suggests improvement * notify of service limit breaches. | COST OPTIMIZATION, PERFORMANCE, SECURITY, FAULT TOLERENCE, SERVICE LIMITS |
| Opswork | * **CHEF AND PUPPET** – PERFORM SERVER CONFIGURATION AUTOMATICALLLY | SSM ALTERNATIVE |

|  |  |  |
| --- | --- | --- |
| Networking and Content Delivery: | | |
| Service | Design Principal | AWS Services |
| Amazon API Gateway | * Managed service for developers to **publish, maintain, monitor and operate** APIs in any scale | Pay as u go  takes care of running APIs securely and reliably at a scale |
| Amazon CloudFront | * improve read perf, content is cached at edge * Improve user exp * **216** edge locations * DDos protection * Integrated with shield and WAF * S3 BUCKET: caching the objects at the edge into CloudFront * security control can use CloudFront Origin Access Control.’ * delivering content from a nearby warehouse instead of shipping it from a far-away one. | **CDN content delivery network**  S3/HTTP >> CLOUDFRONT -> LOCAL CACHE >> CLIENTNext time take from local cache.   * caches the static files from your S3 bucket in its Edge Locations * user requests a file from your website, the request goes to CloudFront first * faster loading times * Reduced Load on Web Servers: |
| AWS Direct Connect | * Establish physical connected btw on premises and AWS * takes a month to be established * goes over a private network | PRIVATE, FASTER |
| Site to Site VPN | * Connect on-prem to AWS, connection is encrypted * might have security issues and limited bandwidth | PUBLIC, SLOWER  ON-PREM MUST HAVE CUSTOMER GATWAY, AWS MUT USE A VIRTUAL PRIVATE GATEWAY  **Customer Gateway (CGW) and CUSTOMER SIDE**  **Virtual Private Gateway (VGW) AWS SIDE** |
| Amazon Route 53 | * Managed DNS(rule book) * simple routing -> no health checks * Weighted routing policy -> divides traffics to EC2 instances * Latency Routing -> closes servers to location minimize latency * Failover routing -> 2 servers one primary one failover helps during disaster recovery. |  |

|  |  |  |
| --- | --- | --- |
| Compute and Serverless | | |
| Service | Use | Use Case/ Keyword |
| AWS Artifact | * Portal for compliance reports * Support internal audit and compliance to things * HIPAA for BAA agreements | **On demand access to AWS compliance documentation and agreements** |
| AWS Certificate Manager (ACM) | * Provision and mange SSL/TLS certificates * Used to provide in-flight encryption for websites * EC2>> ASG>> ALB>> CERT MANAGER >> HTTPS FOR CLIENT * Supports both public and private * Free for public TLS * Automatic renewal | **WHAT SERVICE CABN HELP US DO IN FLIGHT ENCRYPTIONS AND GENRATE CERTIFICATION** |
| AWS CloudHSM | * ENCRYPT BOTH AT REST AND IN TRANSIT * AWS MANAGES HARDWARE * U mange ur own encryption key | HSM device is temper resistant |
| AWS KMS | * Mange the encryption keys for us | **ENCRYPTIOON FOR SERVICE** |
| Amazon Cognito | * Provide Identity from web mobile users * IAM is for people who belong to company * So u create User in Cognito | BUILDING APPLICATION AND WANT TO MANAGE USERS ON AWS |
| Amazon Detective | * Find how security issues happened * Finds the root cause * Collect and process events from vpc flow logs, cloudtrail, gaurdduty |  |
| Amazon GuardDuty | * Helps u do intelligent threat duty, * Uses ML, 30 day trial * Input data – cloudtrail logs, vpc flow logs, dns logs, optional features can sent up event brdidge rules to be notified in case of findings | **BEST FOR CRYPTO CURRENCY ATTACK**  Guard dutry >> eventbridge >> lambda/sns |
| AWS Network Firewall | * Layer 3 to layer 7 * Much better than Nacl as this operate at VPC level and that operate at subnet level. | **HOW TO PROTECT ENTIRE VPC** |
| Amazon Inspector | * Run **automated** security assessments * Leverage System manager agent * INSPECT >> ECR CONTAINER IMAGE//LAMBDA//SSM AGENT * Integration with AWS security * Sends findings to security hub and event bridge | **Only evaluates**  EC2, CONTAINER IMAGES , LAMBDA  INFRASTRUCTURE WHEN NEEDED  VULNERABILITIES IN THE ABOVE  NETWORK RECHABILITY  RISK SCORE WILL BE ASSOCIATED |
| Amazon Macie | * Fully manged data security and privacy service * ML, discover and protect sensitive data * Identify and alert u to sensitive data | **S3 >> MACIE>> EVENTBRIDGE >>** |
| AWS Shield Standard | * NO additional cost …. For ALL customers * Provide protection from attacks like SYN/UDP floods, reflection attacks, layer 3 and layer 4 attacks |  |
| AWS Shield Advanced | * 24/7 premium DDos protection * Protect against more sophisticated attack. * There is a response team | * 3000 per month |
| AWS WAF | * Filter specific requests based on rules. * Protect web application from common web exploits LAYER 7 * Deploy on Application load balancer, API gateway, cloudfront.   **FOR ENTIRE DDOS PROTECTION NEED SHIELD, WAF, ROUTE 53, AND CLOUDFRONT** | **Protects from common attack –** SQL injection and cross-site scripting.  Size constraints |
| AWS Security Hub | * Central security tool for all aws account * Automate security checks. * MUST ENABLE AWS CONFIG SERVICE * FIND Potential ISSUES FROM OTHER SERVICES | **GENERATES RESULTS INTO EVENTBRIDGE**  **AUTOMATE CHECKS USING HUB**  **INVERTIGATE USING DETECTIVE**  FIRST 10 000 EVENT ARE FREE |
| AWS Abuse | * Report suspected AWS resources used for abusive or illegal purpose |  |
| Root user privileges | * Account owner. * Has complete access to everything. * Need lock away root user access keys. | * Change account setting. * View certain tax invoices. * Close aws account * Restore IAM user permissions. * Change or cancel AWDS support plan. * Register as seller in marketplace. * Configure s3 to enable MFA. * Edit or delete s3 bucket poly that includesVPC |

|  |  |  |
| --- | --- | --- |
| Storage | | |
| Service | Use | Use Case/ Keyword |
| AWS Backup | * Centrally Manage and automate Backups across AWS * Cross region or cross account backup * Backed Up into S3 |  |
| Amazon Elastic Block Store (Amazon EBS) | * Network drive to attach to EC2 while they run. * Allows instance to persist data even after it is stopped even if the instance is recreated can get back data. * Can only be mounted to one instance at a time. * Bound to specific availability zone. * 30 gb free * Can be detached and attached quickly. * Can move if u do snapshot. * Need a provisioned capacity. | AUTO ENCRYPTION USER NEED CHOOSE |
| Amazon Elastic File System (Amazon EFS) | * Can be mounted to 100s of EC2s. * Works only with **LINUX** * Works on multi-AZ * Highly available and scalable, expensive, pay per use. * No capacity planning. * Use EFS Mount Target to go into EFS. | INFREQUENT ACESS  -92% LOWER THAN THE OTHER IN COST  WILL AUTO MOVE FILE BASED ON LAST TIME IT WAS USED  Enable EFS-IA WITH A LIFE CYCLE POLICY  JUST FOR COST OPTIMIZATION |
| Amazon S3 | * Main building block * Infinitely scaling * Stores files into buckets as objects * Buckets need to have globally unique names. * Buckets are defined in a specific region.   Objects   * Have key. * Key is the full path. * Key = prefix + object name * No directory * Object is the content of the body. * 5TB, 5GB per upload only * Objects can have metadata – by system or by user. * Objects can have tags and version ID.   Static Website hosting   * URL will depend on region. * 403 forbidden error means bucket is no public so need add policy to make bucket public.   Versioning   * Enabled in bucket level. * Best practice // supports unintentional delete// easy rollback * Suspending versioning won’t delete the old stuff   Replication  Enable versioning in source and destination buckets.   * CRR –different region (Compliance, lower latency, replication) * SRR – Same region (log aggregation, live replication) * Proper IAM permissions must be given.   Durability  99.99999999%.  Availability  Not available 53 min a year | **AUTO ENCRYPTION**  **AWS OPERATES INFRASTRUCTURE LAYER, OPERATING SYSTEMJ AND PLATFORMS**  BACK UP AND STORAGE  DISASTER RECOVERY  ARCHIVE  HYBRIDE CLOUD STORAGE  APPLICATION/ MEDIA HOSTING  HOSTING STATIC WEBSTS  NASDAQ/ SYSCO  S3 one zone  frequently accessed data  S3 one zone IA  **lowest availability**  accessed less frequently but requires rapid access when needed  **KEY VALUE DATABASE** |
| S3 bucket policy | * JSON based policies. * Resource based policies. * Allow deny API |  |
| Amazon S3 Glacier | * Low cost, meant for a ARCHIVING /BACK UP * Pricing is price of storing and retrieving   INSTANT RETRIVAL   * Millisecond retrieval * Good for data accessed once every 3 months * Min storage for 90 days   Glacier Flexible retrieval   * 1 to 5 min expedited , standard 3 to 5 hrs , bulk 5 to 12 hrs * Min storage 90 days * secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup   Glacier Deep archive   * Standard 12 hr or bulk 48 hr * Min storage 180 days.   Intelligent tiering   * Small monthly monitoring auto-tiering fee * Moves objects btw access tires based on usage   No retravel charges in this  Tires: Frequent access, Infrequent Access (30days) Archive Instant Access (90 days) , Archive Access tier (90-700+ days) |  |
| S3 Standard | * For frequently accessed data * Low latency * Can sustain 2 concurrent facility failures | Big data analytics, mobile and gaming applications, content distribution |
| S3 infrequent access | * Data that is not frequently accessed * Lower cost than S3 | Disaster recovery, backups  Storing secondary backup copies of on-premise data |
| S3 encryption | * SERVER-SIDE ENCRYPTION/ BY DEFAILT BY THE SERVER AFTER RECEIVING INTO S3 (DEFAULT) * User takes file and encrypts before uploading CLIENT-SIDE ENCRYPTION. |  |
| Shared responsibility modal | AWS   * Infrastructure * Configuration and vulnerability analysis * Compliance validation   User   * Versioning * Bucket policy * Replication * Logging and monitoring] * S3 storage class * Encryption at rest and in transit |  |
| AWS Snow family | * Secure portable devices to collect and process data at the edge and migrate into and out of AWS * IF IT TAKES MORE THAN A WEEK THEN U USE SNOWBALL DEVICE | AWS SHIP DEVICE TO CUTOMER LOAD STUFF THEN SHIP TO AWS THEN IT IS STORES ON S3 |
| AWS Snowball Edge | * For data transfer * For TB or 1PB of data in or out * Alternative to moving over the network and paying network fee * Provide block storage * Edge STORAGE optimized * Edge COMPUTE OPTIMIZED | LARGE DATA CLOUD MIGRATION, DISASTER RECOVERY |
| AWS Snowcone | * Small and portable, rugged and secure * Used for EDGE COMPUTING, STRAGE, DATA TRANSFER * SNOWCONE – 8TB OF HDD * SNOWCONE SSD – 14 TB OF SSD * use snowcone where snowball does not fit ( SPACE SAVING) * must QPROVIDE OWN BATTERIES | 1. REQUEST FOR SNOWBALL FROM AWS 2. INSTALL THE SNOWBALL CLIENT/ OPSHUB ON UR SERVERS 3. CONNECT SNOWBALL TO SERVER COPY FILE USING THE CLIENT 4. SHIP BACK |
| AWS Snowmobile | * Transfer exabytes of data * Has 100PB of capacity |  |
| AWS Storage Gateway | * BLOCK STARAGE * EBS * EC2 * File * EFS * Object * S3 * Glacier   **Bridging on premisses data and cloud data in S3**  **hybrid cloud storage service** |  |

|  |  |  |
| --- | --- | --- |
| Types of Customer Master Keys (CMK) | | |
| Service | Use | Use Case/ Keyword |
| Customer Manged CMK | * Create, manage and used by customer | Can bring own key |
| AWS Manages CMK | * Create managed used by AWS on the customer behalf |  |
| AWS Owned CMK | * Collection of CMK that AWS service own * AWS can use that to protect account | U cannot view you own key |
| CloudHSM Keys | * Generated from your own CloudHSM device |  |

|  |  |  |
| --- | --- | --- |
| Compute and Serverless | | |
| Service | Use | Use Case/ Keyword |
| AWS Batch | * Dynamically launch EC2, provision compute and memory automatically * Submit batch schedule only * cost optimisation, focuses less on infrastructure | NOT SERVERLESS RELIES ON EC2 |
| Amazon EC2 | * create and run virtual servers in the cloud * limited by CPU and ram config provided * Continuously running, scaling means to add and remove servers. |  |
| AWS Elastic Beanstalk | * No infrastructure way of deploying an application without ALB ASG * worry about code * FREE, MANAGED(no configuration) * Developer friendly * Health agent on every EC2 push into cloud watch. | PaaS  1 instance – dev  LB + ASG good for production  ASG good for non-web apps |
| AWS Lambda | * Virtual functions, serverless * limited by time, run on demand * scaling is automated. Easy pricing * event driven, reactive service, can be monitored in **Cloudwatch.** * 10gp RAM * Pay per Calls , * eventbridge trigger lambda every 1 hr. | Serverless CRON JOB: define schedule run a script,  charged based on the number of requests for your functions and the duration, the time it takes for your code to execute |
| AWS Lambda Container Image | * let’s u run docker container over lambda, * images must implement lambda runtime API | ECS/Fargate is preferred for running containers though |
| Amazon LightSail | * simpler alternative * Build application and websites with preconfigured resources | For people who don’t have AWS experience |
| Amazon WorkSpaces | * Can have laptop in the cloud * pay as u go pricing * fast and scalable * to minimise latency deploy closer to user | **VIRTUAL LAPTOPS OR MANAGED DESKTOP** |
|  |  |  |

appsync - storing data foe mobile web apps using **graphql**

Amplify – set of tools that help u develop and deploy full stack web and mobile applications

DeviceFarm – tests web and mobile app against desktop browsers real mobile devices and tablets.

Disaster recovery strategy – backup and restore

Elastic disaster recovery – recover, physical, virtual and cloud based servers, Continuous block level replication

Datasync – move large amount of Data from on-premises to AWS synchronise with S3, replication **INCREMENTAL**

Application Discovery service – scan servers and understand what and how to migrate can run with agent and without

Application Migration service – lift and shift(rehosting) converts everything to run on AWS, minimal downtime and reduce cost

AWS Migration Evaluator – help build a data driven business case for migration to AWS, install agentless collector to conduct discovery analyse state, define target state, develop migration plan.

AWS Fault Injection Simulator – fully managed service for running fault injection experiments on workloads, supports EC2, ECS, EKS, RDS uses pre built templates

Step functions – Build serverless visual workflow of lambda functions use case is order fulfilment, data processing and more.

Ground station – lets u control satellite communication, allows u to download satellite data to ur vpc within seconds can send them to s3 and then process it, weather forcasting, surface imaging, video broadcasts are some use cases

AWS pinpoint – outbound and inbound marketing communication service , use cases run campigns by sending bulk smses in SNS everything needs to be managed, pinpoint don’t need it use templates, delivery schedules, targeted segments, Next evolution of sns and SES

Data Migration service - involves moving databases from one region to another, AWS Database Migration Service can be a valuable tool. It supports both homogenous and heterogeneous database migrations/ AWS Database Migration Service (AWS DMS) cannot help with the entire IT resources migration.

AWS Service catalouges – For people who d k how to use AWS, organized list of IT services and resources available, HELPS COMPANY CONTROL COSTS, employees can find and request for things easily.

AWS Cloudshell – allows users to access AWS CLI WITHOUT HAVING TO DOWNLOAD IT useful for quick command-line tasks

Amazon Machine Image – preconfigured template to create instance contains necessary info to launch instance SIMPLIFY PROCESS OF LAUNCHING INSTANCE

EC2 Image Builder – simplify process of custom AMI, allows u to automate the creation testing and distribution of custom AMI. Help improve security and consistency of EC2

Elastic load balacer - fundamental component of scalable and resilient applications. Helps distribute traffic btw ec2 improves application availability.

Elastic load balancer – layer 4

Application load balancer – layer 7 designed for modern applications, supports advanced routing features provides integreation with WAF

Network load balancer – layer 4 – made to handle low latency ideal for application that require extreme performance

Global Accelerator – improve global availability and performance improve by 60%. Edge location sends traffic integrated with shield GOOD FOR NON-HTTP USE CASE

Cloudfront only deliver content this one has no caching and this is used to make your request go faster

Outpost- server racks that offere same aws infrastructure … people will come and set up on premises – you will be responsible for physical security

Wavelength - infrastructure deployments embedded within telecommunication providers at the edge of 5G networks

Ultra lowe latency through 5g networks

Local zone – place stuff closer to user to run latency- sensitive applications

MQ – Mannged message broker service for ***ActiveMQ*** and ***RabbitMQ*** only use if company is migrating to cloud witht these two

X Ray- debugging the old way, get visual analysis of application, troubleshooting understand dependencies find errors and exceptions DISTRIBUTED TRACING TORUBLE SHOOTING SERVICE Graph

Code guru reviewer – Ml powered automatic code review thing has integration with github, bitbucket, codecommit

Code guru profiler – recommendations about application performance cost and everything

AWS Health service history – shows all regions and services health, shows historical application for each day, has RSS feed u can subscribe to,

AWS Health dashboard for u – personalized view into performance and availability of the AWS services that u have, provide notification to help u manage events in progress and to manage for future BASICALLY WHEN AWS GOT PROB WILL TELL U STUFF

Control tower – create multi account aws environment within few clicks automate policy management using guardrails moniter compliance through interactive dashboard, auto set up organization and implement SCP

Cost Explorer – visualize and understand aws cost and usage over time, analyze data in high level, choose optimal savings plan to lower price FORCAST BILL FOR 12 MONTHS AFTER DEPLOYEMENT

AWS Cost Anomoly detection- monitars ur spends using ML and detect unusual spend, sends u report with root cost analysis can get notified using SNS

AWS service Quotas- shutdown resources before limit is reached or request a quota increase

Increase availability – diff az

Increase latency – diff region

Billing dashboard – show cost

Cost allocation tags- aws generated , automatically applied to resource u create User-defined tags – define by user FREE NAMING, tags can be used to create resource groups and can be managed using tag editors/ cannot create separate invoices based on tags.

SUPPORT PLAN

Based on what u spend

BASIC

* Customer service 24/7
* Trusted advisor
* Personal health dashboard

Developer

* Customer service 24/7
* Trusted advisor
* Personal health dashboard
* Business hour email to access cloud support associates
* Can have unlimited hours
* If is general reply by 24 hrs
* If anyth down reply by 12

Business

* Use if have production workloads
* Trusted advisor full set and API access
* 24 by 7 phone email and chat to contact cloud support
* Access to infrastructure event management
* Is prod it down will reply by 1 hr
* If prod is impaired will reply by 4 hrs

Enterprise on RAMP

* Use if have production or business critical workloads
* Access to pool of technical account managers
* Concierge support team for billing and account best practices
* Infrastructure event management, well architedtected and operational reviews
* 1hr
* 30 min

Enterprise support

* If u have mission critical workloads
* Access to designated Technical account manager
* Concierge team
* 4
* 1
* 15 min if business – critical system is down

AWS Well architected tool

* Selected work load an sqns against 6 pillars, obtain advice basically a quiz

AWS CAF

Right size before cloud migration, cloudwatch, cost explorer trusted advisor can help with this

AWS PARTNER SOLUTIONS – Automated gold standard deployments

AWS Professional services organization – global team of experts,

APN TECH PARTNER- Hardware, connectivity and software

APN Consulting – help build on AWS

Training Partners- learn AWS

Competency-

Navigate- help partners become better partners

KNOWLEDEG CENTER – CONTAINS MOST FREQUENT AND COMMANQUESTIONS AND REQUESTS

AWS IQ- find professional help for ur aws projects 3rd party

Re:Post- community forum crowd source like stackoverflow

Cloud Foundations - provides a guided path to help customers deploy, configure, and secure their new workloads while ensuring they are ready for on-going operations

Pricing calculator – for when u d h stuff but want projected price

INSTANCE STORE - provides temporary block-level storage for your Amazon EC2 instance.

Global stuff - REGIONAL

WAF

CLOUDFRONT

IAM

ROUE53

AWS Directory Service - simplifies the deployment and management of directory solutions in the cloud

AWS Control Tower - intended for organizations with multiple accounts and teams who are looking for the easiest way to set up their new multi-account AWS environment

Access Analyzer - helps you analyze and identify unintended access to your AWS resources. It uses automated reasoning and logic-based techniques to continuously evaluate your IAM policies and resource policies to detect potential security risks and issues.

AWS Organizations offers Service control policies (SCPs) THAT CONTROLL API USAGES

1. **Backup and Restore**: backing up critical data and systems and storing them in a secure off-site location. In the event of a disaster, the organization can restore the systems and data from the backups to resume operations.
2. **Pilot Light**: maintaining a scaled-down version of the infrastructure in a standby state. Only essential components are kept running in real-time, and when a disaster occurs, the full infrastructure can be quickly scaled up and restored.
3. **Warm Standby**: Similar to Pilot Light, Warm Standby maintains a partially active duplicate of the infrastructure, but with more components and data preloaded, reducing the recovery time.
4. **Hot Standby**: In a Hot Standby approach, a complete duplicate of the infrastructure is kept running in real-time. The failover to the standby system is immediate and automatic when a disaster occurs.
5. **Multi-Region Deployment**: Distributing critical systems and data across multiple geographic regions. If a disaster affects one region, the organization can failover to another region that is unaffected.
6. **Cloud-Based Disaster Recovery**: manages the underlying infrastructure and replication, simplifying the implementation and reducing costs.
7. **Data Replication**: Implementing real-time or near-real-time data replication between primary and secondary sites. This ensures that data is continuously synchronized, minimizing data loss in the event of a disaster.
8. **Continuous Data Protection (CDP)**: Continuous data protection solutions create an ongoing backup of changes to data in real-time, allowing for more granular recovery points.
9. **Disaster Recovery as a Service (DRaaS)**: Outsourcing disaster recovery to a third-party service provider who manages the disaster recovery process, allowing the organization to focus on its core business activities.
10. **Testing and Regular Updates**: Regularly testing the disaster recovery plan through simulations or real-time recovery exercises to ensure its effectiveness. Also, keeping the plan up-to-date to reflect changes in business needs and IT infrastructure.

CLOUDWATCH

- NO AUTOMATION IS PERFORMANCE BASED

Cloudformation – don’t make things cheaper

 (U2F) Security Key is a device that you can plug into a USB port

**Hardware Multi-Factor Authentication (AWS MFA) device** - This is a hardware device that generates a six-digit numeric code based upon a time-synchronized one-time

Amazon EC2 Instance Connect provides a simple and secure way to connect to your instances using Secure Shell (SSH).

An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle

NETWORK LOAD BALANCER – UDP

THE REST IS APPLICATION FOR HTTP