→ Cloud formation: Converts Infrastructure into code ie creates a template for any website and that template can be used at any location to replicate it

→ It saves enormous amount of time.

Architecting for the cloud

→ overflow traffic send to the cloud

→ Design for Failure

→ Decouple your Components - SQS

→ Elasticity

1) Proactive Cyclic - (weeks, days, year)
2) Proactive Event - (By metrics)
3) Auto Scaling by demand

→ Secure your application by giving Firewall with giving Permissions & denying.

Well Architected Framework

1) Security Pillar:

AWS Shared Responsibility Model

Customer Data

Customer → IAM, Platform, applications

OS, Firewall, Network

Client side, Server side, Encryption

Network Traffic Protection.

AWS → Compute, Storage, DB, N/w

Regions, AZ, Edge Locations.

Definition:

→ Data Protection - ELB, S3, EBS, RDS

→ Privilege Management - IAM, MFA

→ Infrastructure Protection - VPC

→ Detective Controls. - Cloud Trail, Config, Cloud Watch

2. Reliability:

→ Foundation – IAM, VPC

→ Change Management – cloud Trail

→ Failure Management – cloud Formation.

3. Performance Efficiency:

→ Compute – Auto Scaling

→ Database – RDS, Pyramo DB, Redshift

→ Storage – EBS, S3, glacier

→ Space Time Trade off – cloudFront, Elasticcache, Direct connect, RDS Read Replicas.

4. Cost optimization:

→ Matched Supply and Demand – Autoscale

→ Cost effective resources – EC2, AWS Trusted Advisor

→ Expenditure awareness – SNS, Cloudwatch

→ Optimizing over time – Blogs, Trusted advisor.

5. Operational Excellence

→ Preparation

→ Operations — Code Commits Codestar etc.

→ Responses. — Cloudwatch.

→ Redshift for Bussiness Intelligence

Elastic Map Reduce for Big Data Processing

Consuming, bringing to cloud is Kinesis

→ EBS can be detached and reatached whereas Instance Store Volumes cannot.

→ Instance - Ephemeral - small time.

→ OPSworks consists to maintain a Consistent State

Chef
recipes
Cookbooks
} → OPSworks

→ Elastic Transcoder

→ Starters → starts

↓

Workers → works.

↓

Deciders → Decide flow

→ Consolidated Billing - discounts

→ 20 linked accounts only

→ Billing alerts.

→ Cloudtrail is Per account and region to Combine them we need an s3

→ unused unreserved instances for EC2 are applied to the whole group.

→ AWS organizations allows you to manage multiple AWS accounts at once. Policies can be applied on the groups.

→ Cross account access.

→ Resource groups is way of grouping the tags together.

1) Classic - Global

2) AWS Systems Manager - Region based.

→ VPC Peering must be in a single region.

→ If they share any addresses then VPC Peering doesnot work.

→ Direct Connect is to establish a dedicated Connection from Premises to AWS.

→ 10GbPS
1GbPS
ethernet VLAN trunking (802.1Q)

→ VPN is fast and Direct Connect is slow
VPN has Internet whereas Direct Connect doesn't

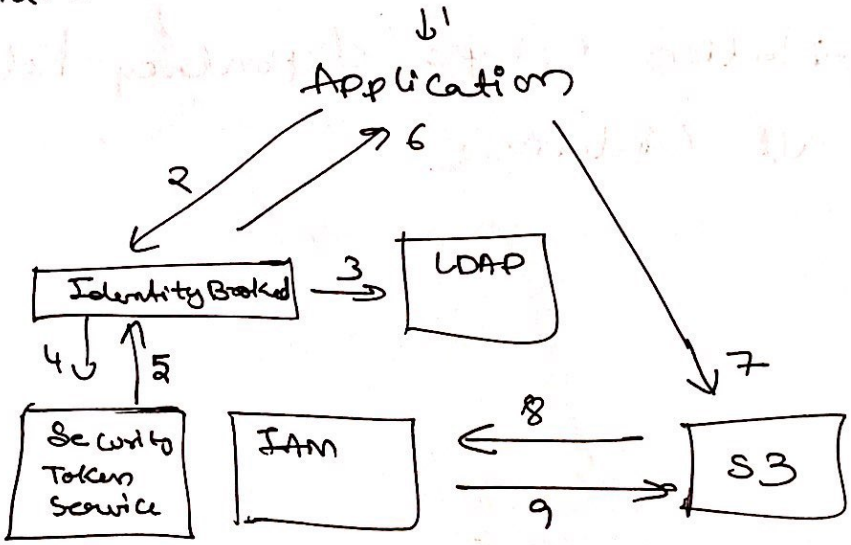
→ Security Token Access

1) Federation - SAML
- FB/google
- Cross account access.

→ Identity Broker - A services that allows you to takes an identity A and join it

Identity Store - Services like FB

Identities - A user of service like FB etc.



→ using SAML we can authenticate Active Directory

→ Authenticate Active directory first and then credentials are given.

→ Workspace is a cloud based replacement for a traditional desktop.

→ windows 7, Server 2008 R2.

→ Persistent

→ D:// is backed up every 12 hours

→ Don't need any AWS account to login to workspace

→ Elastic Container Service. - AWS Dockers.

→ Docker is a s/w platform that allows to build, test and deploy applications quickly.

→ Packages into Containers.

→ Docker, Containerization escape dependency hell and isolates all containers.