ZOOM
TECHNOLOGIES

AWS | Amazon Web Services

Course Presentation

A Practical Guide to Configuring

AWS

(Amazon Web Services)

Cloud Platform

Course Presentation

Introduction

We are pleased to release the practical guide to configuring AWS (Amazon Web Services). This lab manual can be used as a standalone guide or in conjunction with the AWS course taught at Zoom Technologies.

The list of exercises ranges from the basic to the advanced, with each exercise building over the one before it. All the steps are clearly outlined with screenshots so that students can practically work through the manual by themselves.

Each of the exercises is divided into four sections:

1. Objective
2. Prerequisite
3. Topology
4. Tasks

We hope this practical guide will be a useful addition to an IT professional's collection, providing reliable step by step how-tos for general AWS configuration. Any feedback or suggestions to improve this would be gratefully accepted.

DAY 1
Introduction to Cloud Computing with Amazon Web Services

AWS Cloud Computing
ZOOM TECHNOLOGIES

Introduction to Cloud Computing with Amazon Web Services

AWS

Agenda

ZOOM TECHNOLOGIES

What is cloud ?

Cloud Deployment Model

Cloud Service Model

Advantage of Cloud

Cloud Market and scope

AWS certification

Course content of AWS

AWS

Cloud Definition

ZOOM TECHNOLOGIES

What is cloud ?

•**IBM**

Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis.

- **NIST**

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

AWS

Cloud Definition

ZOOM TECHNOLOGIES

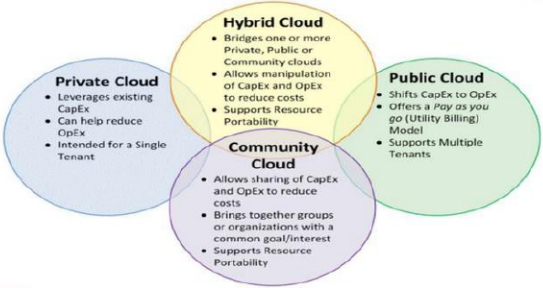
Definitions:

In the simplest terms, cloud computing means it provides services to access programs, application, storage, network, servers over the Internet through browser or client-side application on your PC or Laptop, Mobile, TAB, or Smart TV , by the end user without installing, updating and maintaining them.

AWS

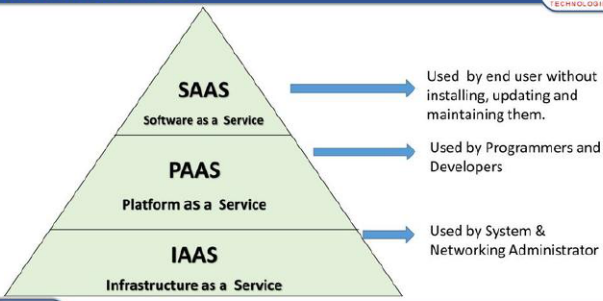
Cloud Deployment Models

ZOOM TECHNOLOGIES



AWS

Cloud Services Models



AWS

Software as a Service (SaaS)

Software as a Service (SaaS) is software distribution model in which applications are hosted by a vendor over the Internet for the end users freeing end users from complex software and hardware management.

Users can subscribe to the service and use the app, normally through a web browser or by installing a client-side app.

SaaS Providers

- •Google – Mail, Calendar, docs, presentation etc..
- •Microsoft - Mail, MSword, paint
- •Twitter,
- •Facebook
- •Flipkart
- •Paypal
- •Gotomeeting
- •Pixlr (image editor)
- •Jaycut (video editor), Aviary (photo editor)

AWS

Platform as a Service (PaaS)

Platform as a service (PaaS) is a category of cloud computing that provides a platform and environment to allow developers to build applications. It frees developers without going into the complexity of building and maintaining the infrastructure.

With PaaS, developers and organizations can create highly scalable custom apps without having to provision and maintain hardware and operating system resources.

PaaS Providers

- AWS beanstalk
- Google App Engine
- Windows Azure
- Force.com from salesforce
- IBM Bluemix
- RedHat OpenShift open source PaaS
- Pivotal CF from VMware

AWS

Infrastructure As A Service (IaaS)

Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources, over the internet. Like CPU, harddisk, memory, switches, routers, firewall, DNS, DHCP, Load Balancer, Autoscaling etc...

IaaS Providers

- Amazon AWS.
- Windows Azure.
- Google Compute Engine.
- Rackspace Open Cloud.
- IBM SmartCloud Enterprise.
- HP Enterprise Converged Infrastructure.
- GoGrid,
- Joyent,
- AppNexus

AWS

Advantages of Cloud Computing

ZOOM TECHNOLOGIES

- Scalability/Elasticity
  - Demand on cloud infrastructures

- Cost saving
  - Reducing up-front IT cost buy server machines, no need for hiring/training manpower.

  - Pay as u go , charges are applied hourly, monthly and yearly basis.

- Disaster recovery and Back up
  - Cloud Services have very high availability of ~99.9999%, by proactively by taking backups, having stand-by virtual resources in place and moving failed instances of Virtual resources across seamlessly

Cloud examples

ZOOM TECHNOLOGIES

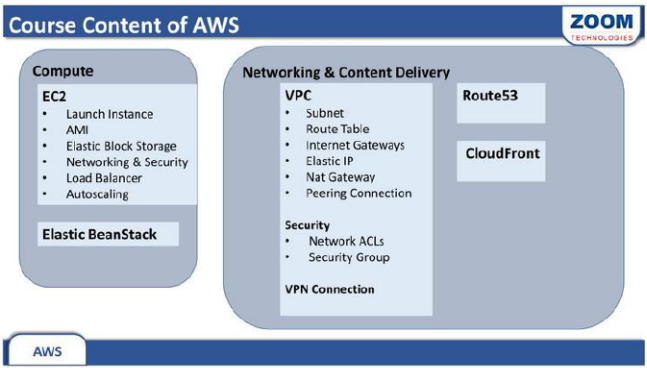
For Example	
DropBox	https://www.dropbox.com/home
Google drive	https://drive.google.com/drive/my-drive
Google Docs	https://docs.google.com/document/u/0/
Google presentation	https://docs.google.com/presentation/u/0/
Google Calendar	https://calendar.google.com/calendar

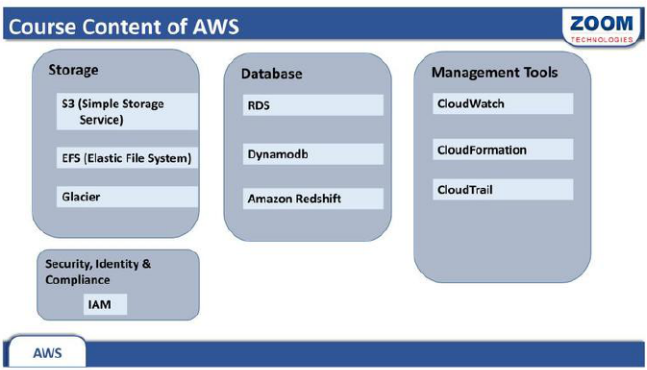
AWS Certification

AWS

Course covered

AWS


Course Content of AWS
ZOOM
TECHNOLOGIES
Compute
EC2
Launch Instance
AMI
Elastic Block Storage
Networking & Security
Load Balancer
Autoscaling
Elastic BeanStack
Networking & Content Delivery
VPC
Subnet
Route Table
Internet Gateways
Elastic IP
Nat Gateway
Peering Connection
Security
Network ACLs
Security Group
VPN Connection
Route53
CloudFront
AWS


Course Content of AWS
ZOOM
TECHNOLOGIES
Storage
S3 (Simple Storage Service)
EFS (Elastic File System)
Glacier
Database
RDS
Dynamodb
Amazon Redshift
Management Tools
CloudWatch
CloudFormation
CloudTrail
Security, Identity & Compliance
IAM
AWS

Course Content of AWS

ZOOM TECHNOLOGIES

Application Integration

- Simple Queue Service
- Simple Notification Service
- Simple WorkFlow Service (SWF)

Advance Topics

- Active Directory Integration
- Server Migration
- Integration with Devops

Customer Engagement

- Simple Email Service

AWS future and Job Scope

ZOOM TECHNOLOGIES

http://www.financialexpress.com/industry/tech/what-the-future-holds-for-india-in-cloud-computing/108207/

http://www.zdnet.com/article/predictions-2017-three-reasons-businesses-cant-ignore-the-rapidly-growing-cloud-market/

http://www.cxotoday.com/story/global-public-cloud-market-to-reach-over-200-bn-in-2016-gartner/

https://www.quora.com/What-is-the-future-of-cloud-computing-in-India

DAY 2

AWS Infrastructure

Launching of Windows and Linux instance

What is AWS ?

Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

The first AWS offerings were launched in 2006 with S3 storage service.

How did Amazon... get into cloud computing?

ZOOM TECHNOLOGIES

?

AWS

AWS global infrastructure over the map

ZOOM TECHNOLOGIES

AWS

AWS Global Infrastructure

ZOOM TECHNOLOGIES

- 16 Geographic Regions

Name	Code Name
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Canada (Central)	ca-central-1
EU (Ireland)	eu-west-1
EU (Frankfurt)	eu-central-1
EU (London)	eu-west-2
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Mumbai)	ap-south-1
South America (São Paulo)	sa-east-1

- 44 Availability Zones
- Coming soon 17 more Availability Zones and six more Regions in Bahrain, China, France, Hong Kong, Sweden, and a second AWS GovCloud Region in the US.
- 90 Edge Location by November 6, 2017

AWS

AWS Region, Availability Zones, Edges

ZOOM TECHNOLOGIES

Regions

An independent collection of AWS resources in a defined geography
A solid foundation for meeting location-dependent privacy and compliance requirements

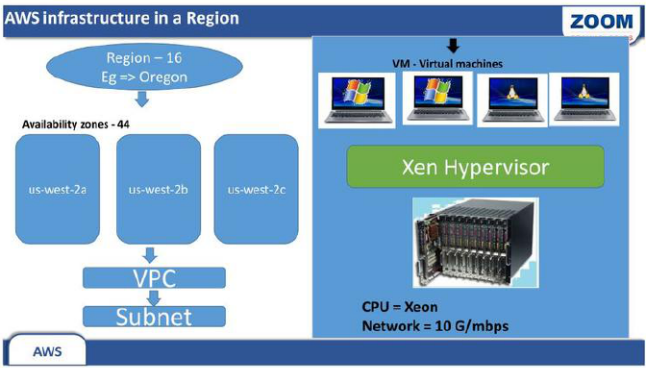
Availability Zones

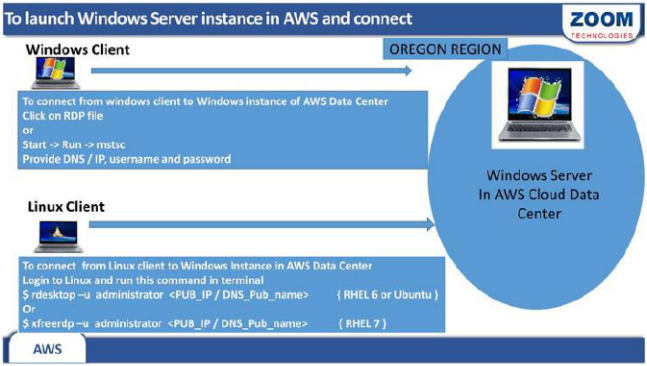
Designed as independent failure zones
Physically separated within a typical metropoliten region

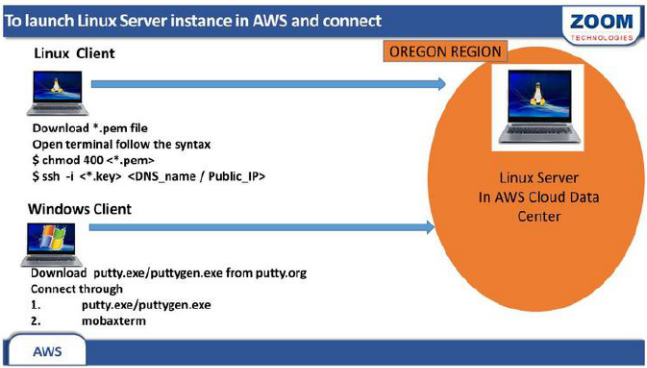
Edge Locations

To deliver content to end users with lower latency
A global network of edge locations
Supports global DNS infrastructure (Route53) and Cloud Front CDN

AWS


AWS infrastructure in a Region
ZOOM
Region – 16
Eg => Oregon
Availability zones - 44
us-west-2a
us-west-2b
us-west-2c
VPC
Subnet
VM - Virtual machines
Xen Hypervisor
CPU = Xeon
Network = 10 G/mbps
AWS


To launch Windows Server instance in AWS and connect
ZOOM
TECHNOLOGIES
Windows Client
OREGON REGION
To connect from windows client to Windows instance of AWS Data Center
Click on RDP file
or
Start -> Run -> mstsc
Provide DNS / IP, username and password
Windows Server
In AWS Cloud Data
Center
Linux Client
To connect from Linux client to Windows instance in AWS Data Center
Login to Linux and run this command in terminal
$ rdesktop –u administrator <PUB_IP / DNS_Pub_name> { RHEL 6 or Ubuntu }
Or
$ xfreerdp –u administrator <PUB_IP / DNS_Pub_name> { RHEL 7 }
AWS



DAY 3

Amazon Elastic Block Storage

Amazon Elastic Block Storage

Types of Storage

- Direct-attached storage (DAS)
- Network attached storage (NAS)
- Storage area network (SAN)
- Cloud Storage i.e. storage over Internet

Direct attached storage (DAS)

ZOOM TECHNOLOGIES

- **Direct-attached storage (DAS)**

  Direct-attached storage (DAS) is attached directly to the computer system mother board connectors or through usb. Examples of DAS include hard drives, CDROM/DVD , external hard drives, optical disc drives, pendrive etc.

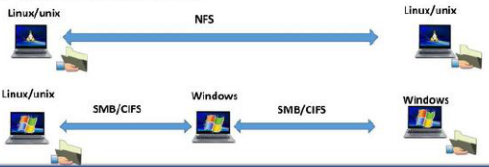
  Amazon provide these facility through **EBS (Elastic Block Storage service)**

AWS

Network-attached storage (NAS)

ZOOM TECHNOLOGIES

- **Network-attached storage (NAS)**
  - NAS uses file-based protocols for sharing folders using NFS for Linux/UNIX, SMB/CIFS for windows.
  - It is a shared folder over the network.
  - Amazon provide these facility through **EFS (Elastic File system)** service.
  - A shared folder cannot be formatted.



AWS

Storage Area Network (SAN)

ZOOM TECHNOLOGIES

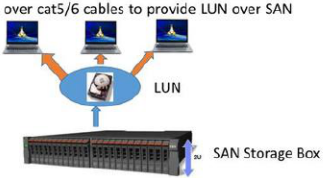
- **Storage Area Network (SAN)**

  A storage-area network (SAN) is a dedicated high-speed network block level data storage, It can be formatted.

  It provide shared pools of storage devices to multiple servers in the form of LUN.

  Fiber cable, bus adapters (HBAs) and fiber switches are used to provide SAN storage.

  ISCSI target make use of normal network over cat5/6 cables to provide LUN over SAN storage.



AWS

Cloud Storage

ZOOM TECHNOLOGIES

- **Cloud storage**

  Cloud storage is a storage over internet provided by cloud service venders.

  It is not a block level storage i.e. cannot be formatted.

  Eg

  Google drive
  One drive
  Dropbox

  Amazon provides this services through

  - S3 (Simple storage service)
  - Glacier service

AWS

Elastic Block Storage

ZOOM TECHNOLOGIES

- Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) is a block level storage volumes which can be formatted according to required filesystem, for e.g. In Windows FAT32, NTFS, in Linux ext3, ext4, resirfs etc.

Data on EBS volume are persistence, they are not lost if a instance is started/stopped or restarted.

When an instance is launched by default it contains an EBS volume which is called as root volume, where operating system is installed.

These EBS root volumes are highly available because AWS by default automatically creates a snapshot of launched instance which are used to recover if any disaster or failover occurs.

Elastic Block Storage

ZOOM TECHNOLOGIES

With Amazon EBS, you can scale your usage up or down within minutes.

Software's like Oracle, SAP, Big Data workloads, Data warehouses, Log processing, Boot Volume are used on EBS volumes.

EBS volumes are 99.9999% Availability, with 0.1% to 0.2% Annual Failure Rate (AFR)

Elastic Block Storage

ZOOM TECHNOLOGIES

EBS volumes are specific to their Availability Zones

An instance can have Multiple EBS volume attached.

These EBS volumes can be attached as well as detached from an instance without any data loss.

EBS volumes at one particular time can be attached to only one instance, it cannot be used with two or more instance at the same time.

EBS volume can be attached to an instance which is in same Availability zone, it cannot be attached to an instance which is another availability zone.

Each EBS volume will have a volume id, which will be used by cloudwatch and other services.

AWS

EBS snapshot

ZOOM TECHNOLOGIES

EBS Snapshot

Snapshot are used to take EBS point-in-time backup.

Snapshot are incremental back up of the EBS volume.

Snapshots are region specific, where as volumes are specific to availability zones.

EBS volumes cannot be increased directly through volumes.

To increase the size of EBS Volumes first create the snapshots, then from this snapshot create the required size of volume.

AWS

EBS snapshot

ZOOM TECHNOLOGIES

EBS Snapshot

Volume size cannot be decrease lesser than the snapshot size

Volumes in another Availability zones can be created using snapshot

To have the same volume in another region, first copy the snapshot in other region, then from this snapshot create the volume in required availability zones .

Volumes are not deleted if snapshots are removed, similarly snapshots are not deleted if volumes are removed

AWS

IOPS / Throughput

ZOOM TECHNOLOGIES

IOPS

Input/output operations per second (#)
After ~33 GB adds 3 IOPS for each GB in general purpose volume

Throughput

Read/write rate to storage (MB/s)

AWS

Types of EBS Volumes

ZOOM TECHNOLOGIES

Volume Types	Hardware Type	Minimum Size	Maximum Size	Max IOPS/Vol's	Max Throughput MB/s	Price
EBS Provisioned IOPS SSD (io1)	SSD	4 GB	16 TB	20,000	Not applicable	$0.125/GB-month $0.065/provisioned IOPS
EBS General Purpose SSD (gp2)*	SSD	1 GB	16 TB	10000	Not applicable	$0.10/GB-month
Throughput Optimized HDD (st1)	HDD	500 GB	16 TB	500	500 MB/s	$0.045/GB-month
Cold HDD (sc1)	HDD	500 GB	16 TB	250	250 MB/s	$0.025/GB-month
Magnetic	HDD	1GB	1 TB	Not applicable	Not applicable	$0.05/GB-month

AWS

Costing of EBS snapshot

ZOOM TECHNOLOGIES

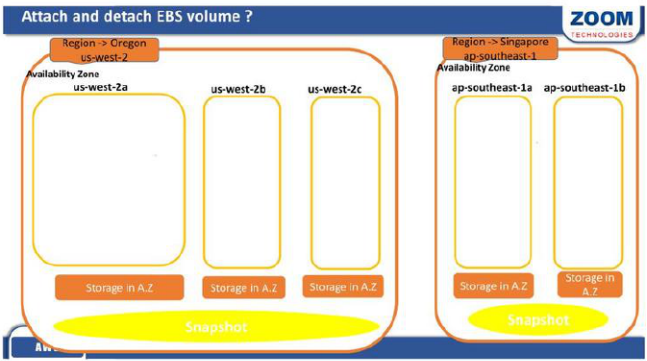
Snapshot are charged around the same as storage for your EBS volumes

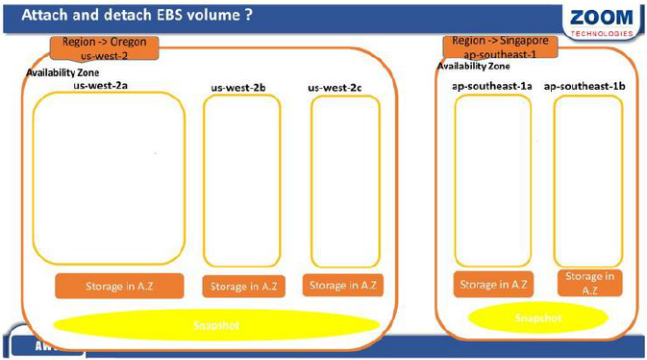
Prices are calculated depending on the type of Volumes.

Scenario

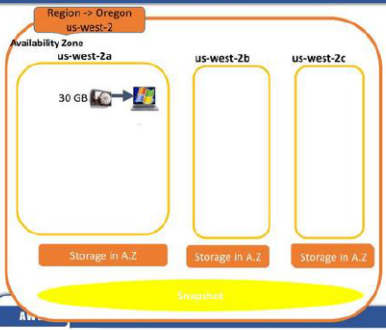
If you take 1TB of local snapshots every day for one month with 3% daily increment changes and a 30-day retention period, it will cost you the same as snapshots for 2TB per month. With $0.10 per GB-month of snapshots, it will cost around $200 ($0.1/GB x 2TB) per disk.

AWS


Attach and detach EBS volume ?
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
Storage in A.Z
Storage in A.Z
Storage in A.Z
Snapshot
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
Storage in A.Z
Storage in A.Z
Snapshot

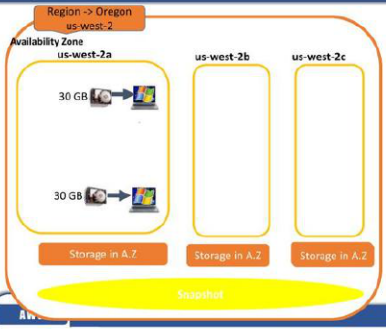

Attach and detach EBS volume ?
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
Storage in A.Z
Storage in A.Z
Storage in A.Z
Snapshot
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
Storage in A.Z
Storage in A.Z
Snapshot

Attach and detach EBS volume ?



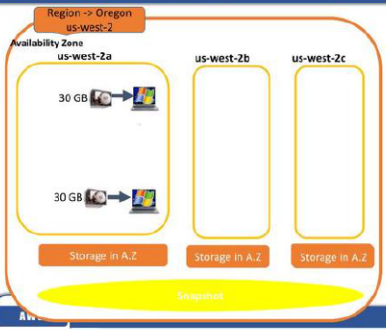
- Launch an instance in one A.Z

Attach and detach EBS volume ?



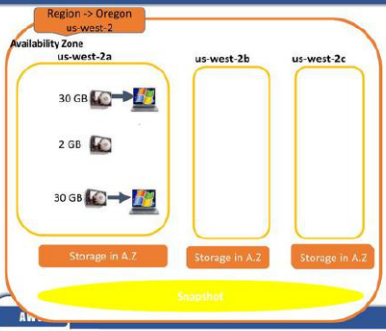
- Launch another instance in the same A.Z

Attach and detach EBS volume ?



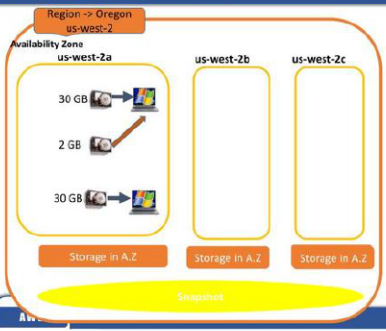
- Create a volume of 2 GB

Attach and detach EBS volume ?



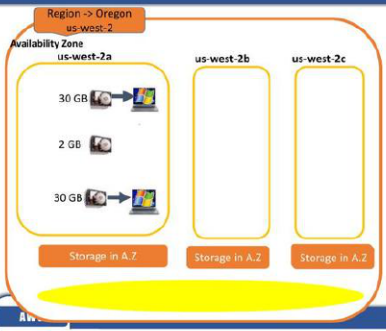
- 2 GB volume got created

Attach and detach EBS volume ?



- Attach the volume to an instance
- EBS volume can be attached to only one instance at one time
- Same volume if u want to use with other instance then, first detach from existing instance and attach to another instance.

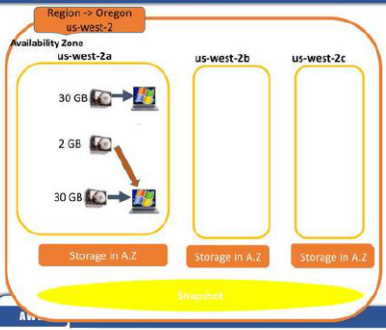
Attach and detach EBS volume ?



- Now volume is detached.
- Now it could be attached to another instance.

Attach and detach EBS volume ?

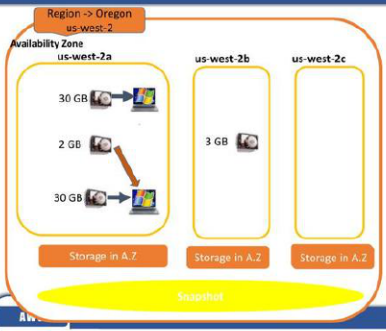
ZOOM TECHNOLOGIES



- Attached to another instance.

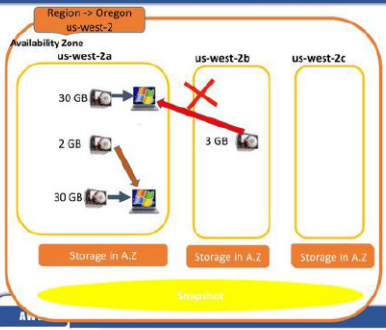
Attach and detach EBS volume ?

ZOOM TECHNOLOGIES



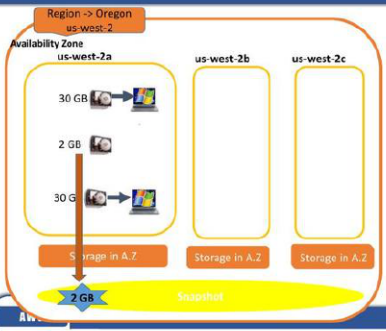
- Create a volume in another A.Z
- A volume of one A.Z cannot be attached to instance in another A.Z

Attach and detach EBS volume of other region S?



- A volume of one A.Z cannot be attached to instance in another A.Z

To Increase the size of the Volume

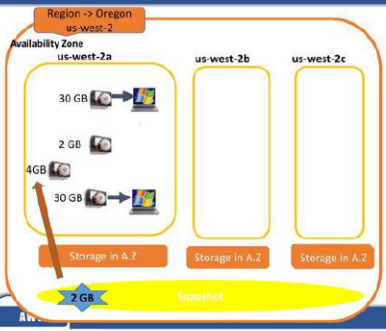


- Snapshots are specific to the region
- To increase the size of the volume first take the snapshot
- Now from this snapshot create a volume of required size.

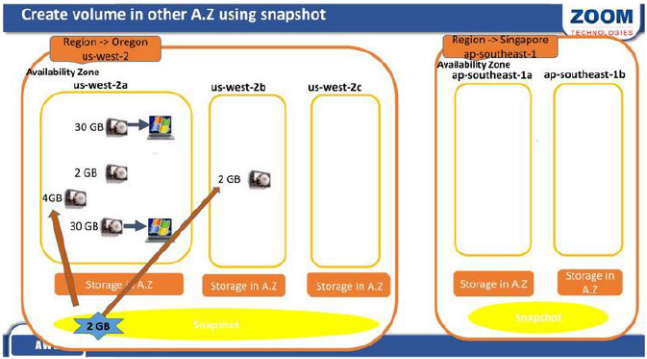
To Increase the size of the Volume

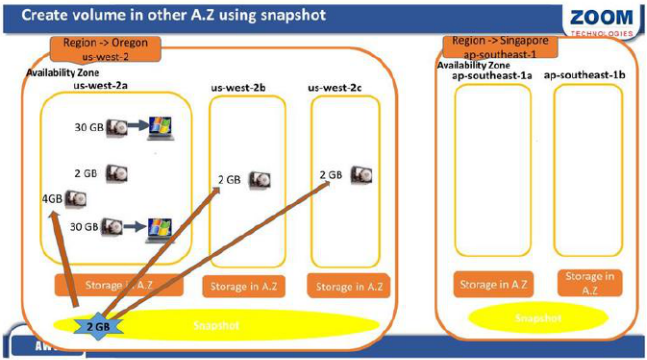
- Snapshot is created
- Snapshot belongs to whole region

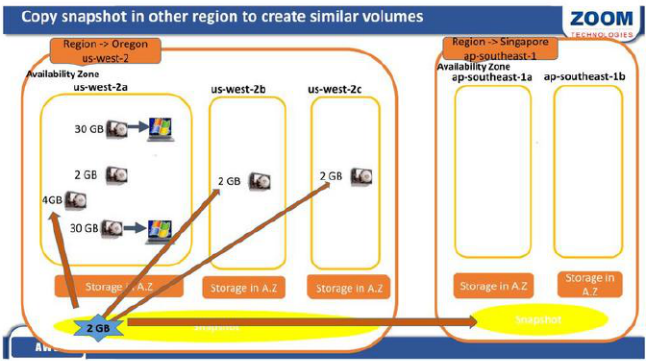
Attach and detach EBS volume ?

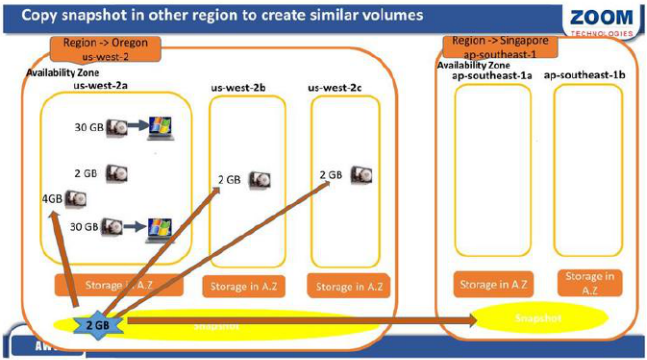


- Now from this snapshot create a volume of required size.

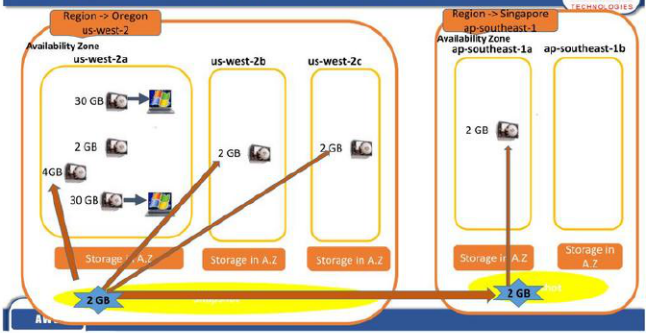

Create volume in other A.Z using snapshot
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
30 GB
2 GB
4GB
30 GB
2 GB
Storage in A.Z
Storage in A.Z
Storage in A.Z
Storage in A.Z
Storage in A.Z
2 GB
Snapshot
Snapshot


Create volume in other A.Z using snapshot
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
30 GB
2 GB
4GB
30 GB
2 GB
2 GB
Storage in A.Z
Storage in A.Z
Storage in A.Z
Storage in A.Z
Storage in A.Z
2 GB
Snapshot
Snapshot


Copy snapshot in other region to create similar volumes
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
30 GB
2 GB
4GB
30 GB
2 GB
2 GB
Storage in A.Z
Storage in A.Z
Storage in A.Z
2 GB
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
Storage in A.Z
Storage in A.Z
Snapshot


Copy snapshot in other region to create similar volumes
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
us-west-2b
us-west-2c
30 GB
2 GB
4GB
30 GB
2 GB
2 GB
Storage in A.Z
Storage in A.Z
Storage in A.Z
2 GB
Region -> Singapore
ap-southeast-1
Availability Zone
ap-southeast-1a
ap-southeast-1b
Storage in A.Z
Storage in A.Z
Snapshot

Copy snapshot in other region to create similar volumes



Managing partitions

- In windows by using diskmgmt.msc drives and partitions can be managed.
- In linux to manage drive and partition use fdisk.

DAY 4

Identity and Access Management (IAM)

Identity and Access Management (IAM)
ZOOM TECHNOLOGIES

Identity and Access Management (IAM)

AWS

Agenda

ZOOM TECHNOLOGIES

IAM (Identity and Access Management)

IAM Users

IAM Groups

IAM Roles

IAM Polices

Multi-Factor Authentication

AWS

What is IAM ?

ZOOM TECHNOLOGIES

- **What is IAM ?**
  - By default when AWS account is created it treats that user as a root user who has the access to all AWS services and resources, but to give the access to AWS services to other users, group members, applications, or instances IAM users, groups and roles are created.
  - (IAM) is a web service that helps you securely control access to AWS resources
  - IAM is a global service, it's free.
  - A primary use for IAM users is to give people the ability to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI.

AWS

Main components of IAM

ZOOM TECHNOLOGIES

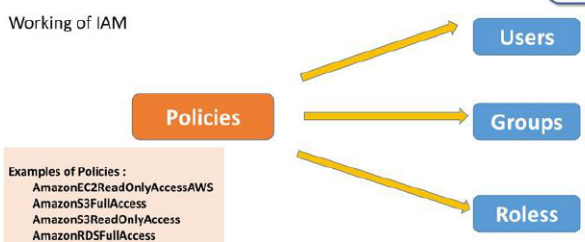
- **The main components of IAM**
  - IAM Users
  - IAM Groups
  - IAM Roles
  - IAM Polices

AWS

IAM

ZOOM TECHNOLOGIES

Working of IAM



Examples of Policies :

- AmazonEC2ReadOnlyAccessAWS
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess
- AmazonRDSFullAccess
- AmazonRDSReadOnlyAccess

AWS

IAM Users

ZOOM TECHNOLOGIES

- **IAM users**
  - IAM users can manage AWS service and resources either through Console access or programmatic Access.
  - If an IAM user is not having any policy attached then that user cannot do any task that means an IAM user without policy is of no use.
  - IAM user requires a username/password to login to console or access/secret key to connect programmatically to use AWS services.
  - An IAM User with only AWS creds can be created so the creds can be used by an application to make API calls into AWS.
  - Multiple policies can be attached to a Single IAM users
  - An IAM user can belong to multiple Groups

AWS

IAM Groups

ZOOM TECHNOLOGIES

- **IAM Groups**
  - An IAM group is a collection of IAM users.
  - Groups let you specify permissions (policy) for multiple users, which can make it easier to manage the permissions for those users
  - Permissions assigned to groups are inherited to all the users in that group
  - Groups can't be nested; they can contain only users, not other groups.
  - IAM user can be a member of 10 Groups

AWS

IAM Roles

ZOOM TECHNOLOGIES

- **IAM Roles**
  - When a policies are applied on an AWS ec2 instance or AWS application or service then it is called as roles.
  - . An IAM role is very similar to a user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS.
  - Roles do not use username and password but they use access key and secret key in order to use the services like ec2, lambda, s3, RDS, autoscaling etc.
  - Scenario

    Suppose you had configured any server and now u want to upload the data to s3 without any user interaction then if that EC2 instance is having a role of s3 then it can automatically upload with the help of script without users interaction.

IAM Policy

ZOOM TECHNOLOGIES

- **IAM Policy**
  - Permissions that we grant to users, groups, and roles are called as policies.
  - These policies will give the access to that service or resource to read, write, or fullaccess.
  - IAM Polices are JSON formatted

Elements of IAM policy

ZOOM TECHNOLOGIES

- Elements of IAM policy
  - Version
  - Statement
  - Contains an array of statements

- Each statement defines whether permissions are allowed or denied

  These are defined by the values of the following elements in each statement:
  - Effect – Allow or Deny
  - Action – array of service actions
  - Resource – array of ARNs that actions can occur on
  - Principal – identifies who/what is allowed/denied access

AWS

Example Policies

ZOOM TECHNOLOGIES

- Allows an Amazon EC2 instance to attach or detach volumes

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
   ],
   "Resource":
        [arn:aws:ec2:<REGION>:<ACCO
UNTNUMBER>:volume/*",
        "arn:aws:ec2:<REGION>:<ACCOUNTNUMBER
>:instance/*"
    ],
    "Condition": {
     "ArnEquals": {
      "ec2:SourceInstanceARN":
"arn:aws:ec2:<REGION>:<ACCOUNTNUMBER
>:instance/<INSTANCE-ID>"
     }
    }
   }
  ]
}
```

AWS

Security firsts for new AWS accounts

ZOOM TECHNOLOGIES

- For AWS root account:
  - Store username/password somewhere safe and secure
  - Setup multi-factor authentication
- Create IAM User(s) with "least privileges" necessary
  - Least privilege = only the permissions necessary to accomplish needed tasks

AWS

Multi factor authentication (MFA)

ZOOM TECHNOLOGIES

- MFA provides added security for AWS resources and account settings.
- It is a two factor authentication
- First factor i.e. it asks for username and password, and the second factor is it ask for MFA code.
- If a user logs in to AWS account he will be prompted for username, password and Multi factor authentication code.
- AWS does not charge any additional fees for using MFA.

AWS

Multi factor authentication (MFA)

ZOOM TECHNOLOGIES

Virtual MFA applications are available for smartphones including Android, iOS and Windows.

❑ These are the list of authenticated mobile application

Android	Google Authenticator; Authy 2-Factor Authentication
iPhone	Google Authenticator; Authy 2-Factor Authentication
Windows Phone	Authenticator
Blackberry	Google Authenticator

Limits of IAM

ZOOM TECHNOLOGIES

Limits :

- **User name 64 characters**
- **Group name 128 characters**
- **Role name 64 characters**
- **Policy name 128 characters**

- **Groups in an AWS account 300**
- **Roles in an AWS account 1000**
- **Users in an AWS account 5000**

DAY 5

Amazon S3 (Simple Storage Service) & Glacier

Amazon S3 (Simple Storage Service) – Object storage

Amazon Simple Storage service (S3)

ZOOM TECHNOLOGIES

- Agenda

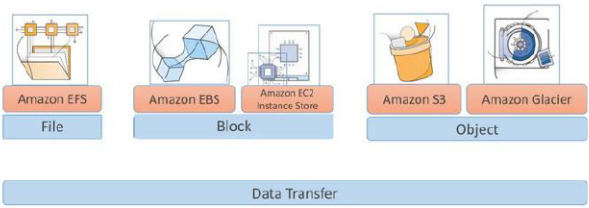
  Cloud Storage
  S3
  Object
  Bucket
  Keys
  Static Web Hosting
  Versioning
  Replication

AWS

Cloud Storage

ZOOM TECHNOLOGIES

Storage is a platform: AWS Storage



AWS

Cloud Storage

ZOOM TECHNOLOGIES

- **Cloud Storage**

Storage over the internet is called as Cloud storage or Object Storage.

Every file on cloud storage is called an object.

Cloud storage differs from block storage (i.e. cannot be formatted) and file storage (i.e. shared folders.)

It is a model in which data is maintained, managed, backed up remotely and made available to users over network (typically the Internet).

Cloud Storage

ZOOM TECHNOLOGIES

Cloud storage is based on a virtualized infrastructure with accessible interfaces, elasticity and scalability, multi-tenancy and metered resources.

Under hood architecture is used to provide highest reliability by replicating objects across multiple servers and hardware and disk drives form the same or different locations.

To configure Cloud storage minimum 3 to 5 nodes are required to maintain multiple copies across the nodes.

Example of Cloud Storage

ZOOM TECHNOLOGIES

Examples of Cloud or Object storage services

Amazon S3	EMC Atmos, EMC ECS
Google Drive	Hitachi Content Platform
One Drive	OceanStore
DropBox	VISION Cloud
Microsoft Azure Storage	
Openstack Swift	

AWS

Amazon Simple Storage service (S3)

ZOOM TECHNOLOGIES

• S3 (Simple Storage Service)

Amazon S3 is a cloud or object storage service, started in 2006 as a first service.

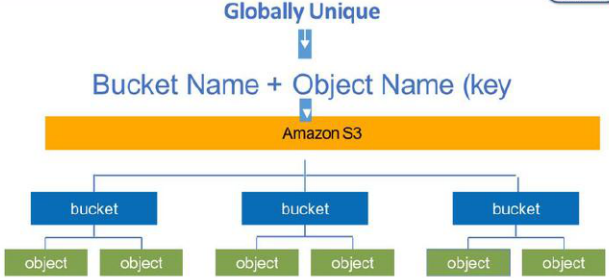
By the end of 2012, 1.3 trillion objects were stored in Amazon S3, the world's largest and most widely known object storage system. Now, that number was growing faster, so the 2 trillion mark is right around the corner.

S3 is a Global service.

S3 enables a customer to upload, store and download practically any file or object .

AWS

Hierarchy of object storage



AWS

Bucket

- **Bucket**

  A bucket is a logical unit of storage in Amazon Web Services (AWS) object storage service,

  Instead of organizing files in a directory hierarchy, object storage systems store files in a flat organization of containers (called "buckets" in Amazon S3) and use unique IDs (called "keys" in S3) to retrieve them.

  Buckets are used to store objects, which consist of data and metadata that describes the data.

  There is no limit to the number of objects a customer can store in a bucket, but each AWS account can only have 100 buckets at one time.

AWS

Object Keys & Metadata

ZOOM TECHNOLOGIES

- **Object Keys**
  When you create an object, you specify the key name, which uniquely identifies the object in the bucket. These names are the object keys.

  The name for a key is a sequence of Unicode characters (UTF-8 encoding) is at most 1024 bytes long.

- **Object Metadata**
  For each object stored in a bucket, Amazon S3 maintains a set of system metadata, which contains object creation date and size, last modified date, etc and uses this information as part of object management.

AWS

S3 Standard and IA

ZOOM TECHNOLOGIES

Amazon S3 comes in two storage classes:

- S3 Standard and ,
- S3 Infrequent Access.

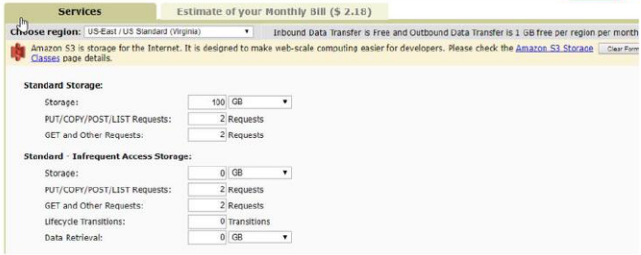
Amazon S3 Standard – Any time could be retrieved or uploaded,

Infrequent Access (Standard - IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed, retrieval of data should be at least after 30 days.

Amazon does not impose a limit on the number of items that a subscriber can store.
A subscriber can choose to keep data private or make it publicly accessible

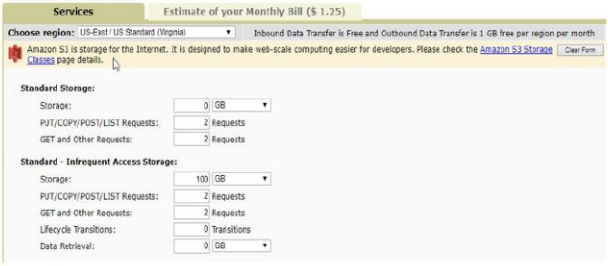
AWS

Pricing of S3 Standard



AWS

Pricing of S3 Infrequent Access storage



AWS

Key features of S3

ZOOM TECHNOLOGIES

- Data Management
  Cost monitoring and controls Lifecycle management
- Ease of use
  Programmatic access using AWS SDKs & REST APIs
  Management Console, AWS CLI
- Event Notifications
  Delivered using SQS, SNS, or Lambda

AWS

Key features of S3

ZOOM TECHNOLOGIES

- Data protection
  Versioning
  Cross-region replication
- Security
  Flexible access control mechanisms
  Time-limited access to object
  Access logs

AWS

Static Website Hosting

ZOOM TECHNOLOGIES

- **Static Website Hosting**

Amazon allow to configure static website on Amazon s3.

It can contains client-side scripts comprised of only HTML, CSS, and/or javaScript at client side, but Amazon S3 does not support server-side scripting.

To configure Static website first create a bucket , then upload all your website code into that bucket.

Add a bucket policy so that all folders, files and subfolders in that bucket can have access.

Enable Static Website Hosting providing index document and error document page.

Provide Endpoint url in brower and check the site.

AWS

Bucket Policy

ZOOM TECHNOLOGIES

```
---------- To create Bucket policy------
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "PublicReadForGetBucketObjects",
                        "Effect": "Allow",
                        "Principal": "*",
                        "Action": "s3:GetObject",
                        "Resource": "arn:aws:s3:::www.indiahydameerpet.com/*"
                }
        ]
}
```

AWS

Versioning is S3

ZOOM TECHNOLOGIES

- Versioning offers an additional level of protection.
- Once versioning is enabled on s3 bucket, then it allows you to preserve, retrieve, and restore every version of every object stored.
- It protects from unintended user actions and application failures,

AWS

Cross-region Replication

ZOOM TECHNOLOGIES

With cross-region replication, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS region that you choose.

Copies of replicated objects inside a bucket are identical to the ones in the destination bucket.

Versioning is required

AWS

S3 in CLI mode

ZOOM TECHNOLOGIES

1) First create IAM user with S3fullaccess policy.

Select AWS access type

Programmatic access

AWS Management Console access

2) In windows install AWSCLI64.msi

3) Configure aws cli providing IAM user access key & secret key

c:> aws configure

Access Key : *********

Secret Key : *********

Region : us-west-2

Note : o/p format are's

a) text

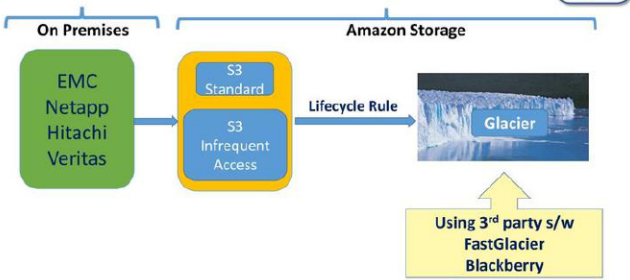
b) table

c) json

AWS

Transferring data to S3 then to Glacier

ZOOM TECHNOLOGIES



AWS

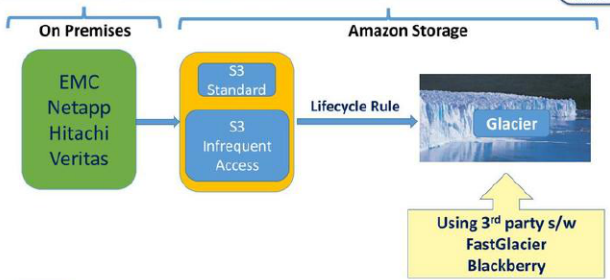
Amazon Glacier

- **Agenda**

  Glacier
  Vault
  Archive
  Tools to use Glacier

Transferring data to Glacier

ZOOM TECHNOLOGIES



AWS

Glacier Definition

ZOOM TECHNOLOGIES

- Glacier is extremely low cost cloud storage, with average annual durability of 99.999999999%.
- It also stores data on multiple facilities before running success on uploaded archives similar to s3, it has built in mechanism for data integrity check.
- It reduces burdens of operating and scaling storage to AWS, without having to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations.

AWS

Glacier Definition

ZOOM TECHNOLOGIES

- Data which are not used frequently should be uploaded in glacier, minimum retention period is 90 days, If any data is retrieved or deleted before 90 days extra charges are applied.
- When the data is uploaded it cannot be accessed immediately it takes minimum 3 to 5 hr. to retrieve data from standard Glacier.
- Amazon does not provides direct access to glacier storage, either should be uploaded from s3 using lifecycle properties or use third party software's like fastglacier or blackberry.

Components of Glacier

ZOOM TECHNOLOGIES

- Components of Glacier
  - Vault
  - Archive

Vault

ZOOM TECHNOLOGIES

- Vault

  It is logical container where data i.e. archives are stored, similar to bucket in s3.

  It is region specific.

  Max 1000 vaults can be created per account

  The largest archive that can be uploaded in a single Upload request is 4 gigabytes. For items larger than 100 megabytes, customers should consider using the Multipart upload capability.

  Vault can be deleted, but before deleting remove all archives in it.

AWS

Archives

ZOOM TECHNOLOGIES

- Archives

  A file or object stored in Vault is called as archive.

  The total volume of data and number of archives you can store are unlimited.

  Individual Amazon Glacier archives can range in size from 1 byte to 40 terabytes

AWS

S3 vs Glacier

ZOOM TECHNOLOGIES

Reference Point	S3	Glacier
Data are stored in.	Bucket	Vault
Object	Key	Archive
Total number	100 Bucket per account	1000 Vault per account
Redundancy	99.999999999 %	99.999999999 %
Object size	128 KB	Not applicable
Minimum storage retrieval	Immediate	3-5 hrs.
Cost	$0.005 per GB put $0.004 per GB get	$0.005 per GB put $0.012 per GB get
Max file size in single upload	Earlier 5 GB now 5 TB	4 GB up to 40 TB (multipart upload 4 GB)
Free tier	5GB	10GB

AWS

Elastic Load Balancer (ELB)

ZOOM TECHNOLOGIES

DAY 6

Elastic Load Balancer (ELB)

AWS

Elastic Load Balancer (ELB)

Agenda

- Cluster
- Types of Cluster
- What is Elastic Load Balancer (ELB)
- Types of Load Balancer
- Features
- Advantage of Load Balancer

ZOOM TECHNOLOGIES

Cluster

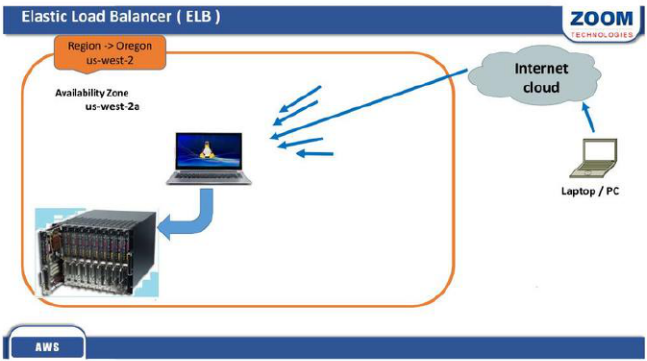
- In a computer system, a cluster is a group of servers and other resources that act like a single system and enable high availability and load balancing or parallel processing

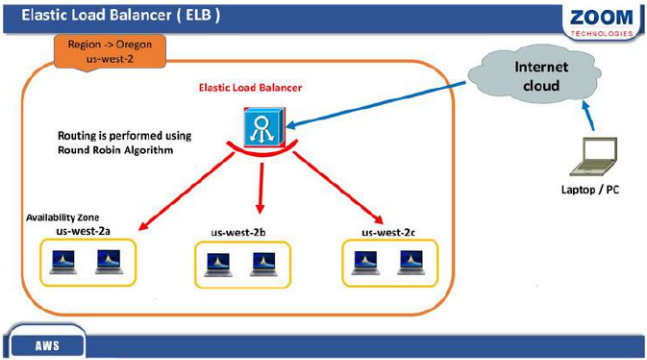
ZOOM TECHNOLOGIES

Types of Cluster

- **Load Balancing**
  - Multiple Nodes are added and scales horizontally
  - Used with Front End Application servers i.e web servers
    - IIS, Apache, NginX, Wordpress, Tomcat , MiddleWare

- **High Availability**
  - More Compute and Memory is added scales vertically
  - Used with Backend Application servers i.e data base servers
    - Oracle , MS-SQL, mysql, mariadb, PostgreSQL etc.


Elastic Load Balancer (ELB)
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Availability Zone
us-west-2a
Internet
cloud
Laptop / PC
AWS


Elastic Load Balancer (ELB)
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
Elastic Load Balancer
Routing is performed using
Round Robin Algorithm
Internet
cloud
Laptop / PC
Availability Zone
us-west-2a
us-west-2b
us-west-2c
AWS

Definition

ZOOM TECHNOLOGIES

Elastic Load Balancer

- Elastic Load Balancer (ELB) is one of the key architecture component inside the AWS cloud.
- Elastic Load Balancing automatically distributes incoming web traffic across multiple applications and containers hosted on Amazon EC2 instances
- With Elastic Load Balancing, you can add and remove EC2 instances as your needs change without disrupting the overall flow of information

Definition

ZOOM TECHNOLOGIES

- Scaling up and down can be automated by integrating with AutoScaling
- If an EC2 instance fails, ELB automatically reroutes the traffic to the remaining running healthy EC2 instances.
- If a failed EC2 instance is restored, Elastic Load Balancing restores the traffic to that instance.
- It is elastic, which means that it will automatically scale to meet your incoming traffic.
- Load Balancers only work across AZs within a region

ELB

ZOOM TECHNOLOGIES

Type of Load Balancer

- **Internet Load Balancer**
  - An Internet-facing load balancer takes requests from clients over the Internet and distributes them across the EC2 instances that are registered with the load balancer
- **Internal Load Balancer**
  - Internal load balancer routes traffic to EC2 instances in private subnets

ELB

ZOOM TECHNOLOGIES

Routing Algorithm

- Routing is performed using the round robin routing algorithm

Features of ELB

ZOOM TECHNOLOGIES

Main Features of Load Balancer

- **Failover Handling**
  - Avoid single point of failure by hosting multiple instances of a given service.
- **Auto-scaling**
  - Manage number of instances of an application according to the incoming traffic.

Advantage of ELB

ZOOM TECHNOLOGIES

Advantage of Load Balancer

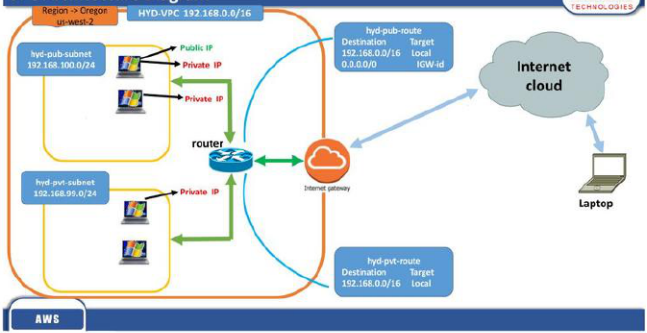
- Optimize resource usage
  - Start and stop resources on demand.
- Maximize the throughput
  - Increase the average rate of successful message delivery.
- Minimize the response time
  - Reduce the time it takes to process a message and send a response back

DAY 7,8

Amazon VPC (Virtual Private Cloud)

Introduction to
Amazon
Virtual Private Cloud (VPC)

VPC Architecture Diagram



VPC Definition

- Amazon VPC is a network infrastructure architecture within the AWS cloud, which closely resembles a traditional network. It isolates your network infrastructure under your account from others account, other wise all network will conflict with each other.
- It is Based on CIDR/ VLSM subnet networking concept.
  - CIDR [Classless Inter Domain Routing]
  - VLSM [Variable Length Subnet Mask]
- A user can create his own VPC which is highly customizable.
- By default every Region will have Default VPC with predefined subnets in each zone.
- As an extension of the corporate network – access through a VPN

AWS

VPC components

- Subnet
- Route tables
- Internet Gateway
- Nat Gateway
- Network ACLs
- Security Groups
- Peering Connections
- VPN

VPC components

Subnet

A range of IP addresses in your VPC

Type of Subnet

Public Subnet

If a subnet has a route to an AWS Internet Gateway it is called a *public subnet*.

Private Subnet

If there is no route from a subnet to an AWS Internet Gateway it is a *private subnet*

- ***Instances in a VPC communicate based on Route Table, VPC Security Groups and Access Control Lists***

VPC components

ZOOM TECHNOLOGIES

Route tables

Applied to subnet(s) specifying route policies.

VPC automatically comes with a main route table.

Every route table contains a local route for communication within the VPC over IPv4.

IGW

Internet gateway is attached to a VPC.

It provide access to the internet for instances in a VPC subnet.

NAT Gateway

NAT gateway provides Internet to your private instances

VPC components

ZOOM TECHNOLOGIES

Security groups

Specify inbound and outbound access policies for an Amazon EC2 instance

Network ACLs

Network access control lists acts as a firewall for controlling traffic in and out of one or more subnets within the VPC

VPC peering

Enables you to route traffic between two or more VPC within the same region

VPN

Bridge your VPC and your onsite IT infrastructure with private connectivity

VPC Architecture Scenarios

ZOOM TECHNOLOGIES

- VPC with a Public Subnet Only
- VPC with Public and Private Subnets
- VPC with Public and Private Subnets and VPC Peering Access
- VPC with Public and Private Subnets and VPN Access
- VPC with a Private Subnet Only and VPN Access

Amazon VPC Products

ZOOM TECHNOLOGIES

Products currently available in Amazon VPC are

- Amazon EC2
- Amazon RDS
- Auto Scaling
- Elastic Load Balancing
- Elastic Beanstalk
- ElastiCache

Steps to Create VPC infrastructure

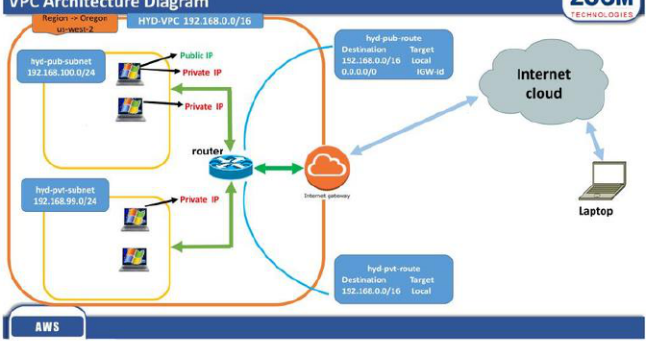
ZOOM TECHNOLOGIES

Step 1) Create VPC with a particular subnet range (max 16 to 28 bit)
Step 2) Create public subnet
Step 3) Create private subnet
Step 4) Create IGW and attach to your VPC
Step 5) Create pub route and Associate respective subnet and add route to IGW
Step 6) Create private route and Associate respective subnet Don't add IGW,
Nat-GW or NAT-instance can be added.
Step 7) Launch VM in Public subnet
Step 8) Launch VM in Pvt subnet
Step 9) Check connectivity

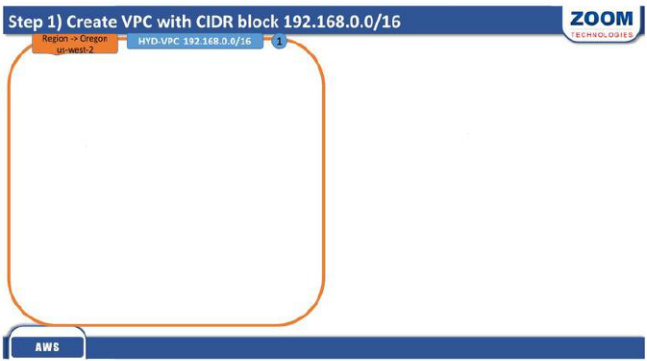
AWS

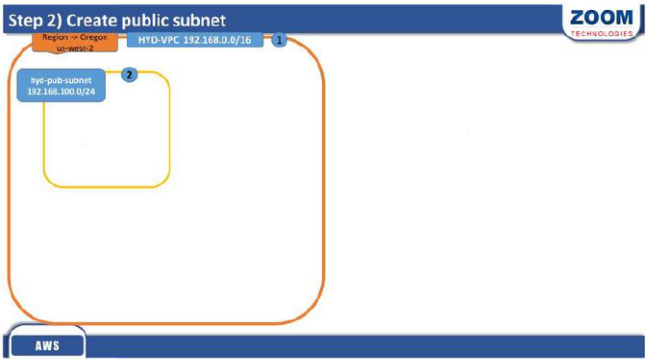
VPC Architecture Diagram

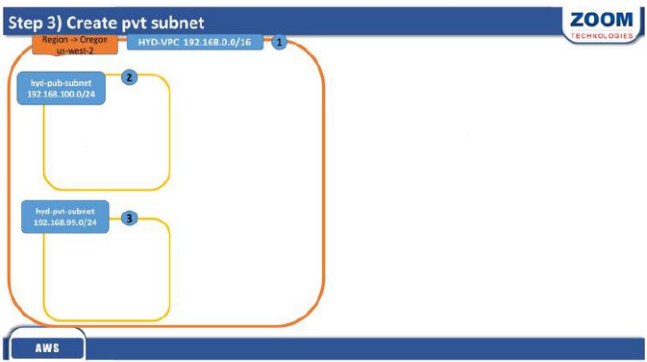
ZOOM TECHNOLOGIES

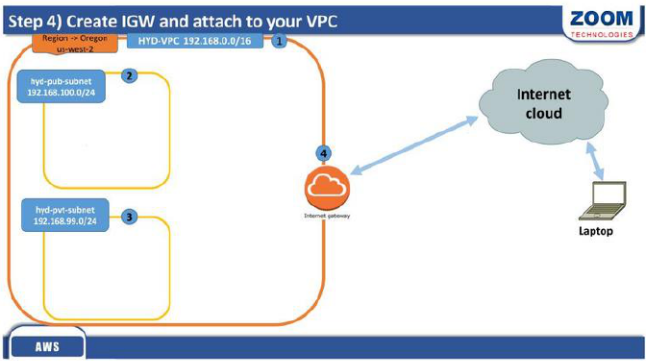


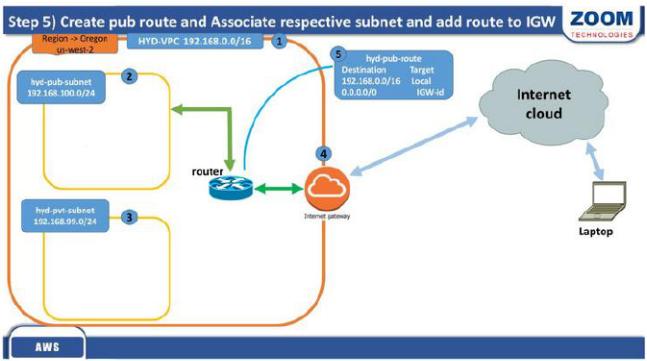
AWS

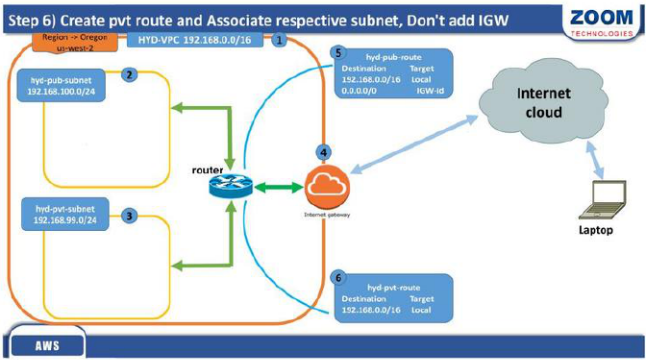

Step 1) Create VPC with CIDR block 192.168.0.0/16
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
AWS

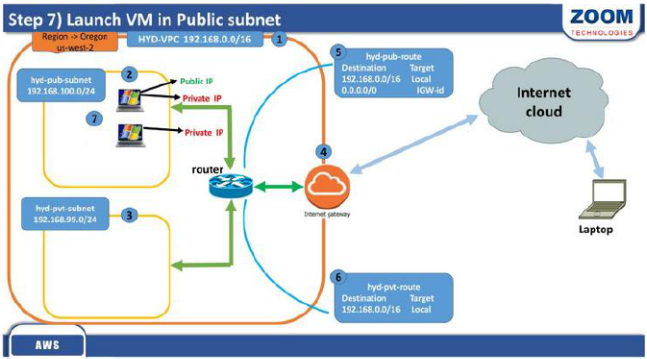

Step 2) Create public subnet
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
AWS

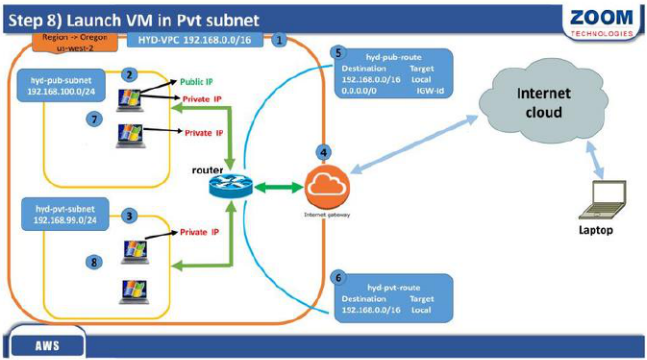

Step 3) Create pvt subnet
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
AWS

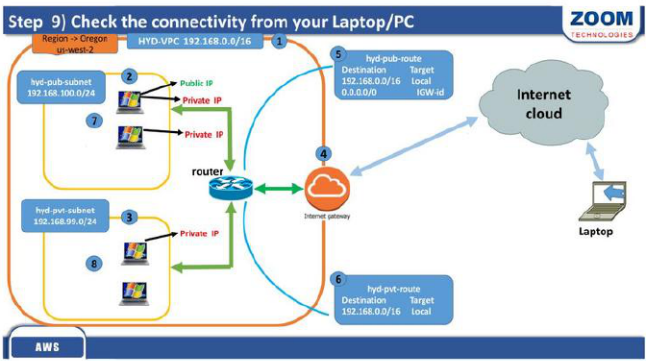

Step 4) Create IGW and attach to your VPC
ZOOM
TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
4
Internet gateway
Internet
cloud
Laptop
AWS

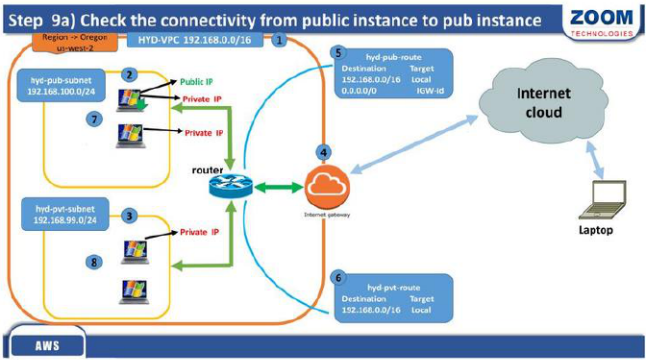

Step 5) Create pub route and Associate respective subnet and add route to IGW
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
router
4
Internet gateway
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
Internet cloud
Laptop
AWS

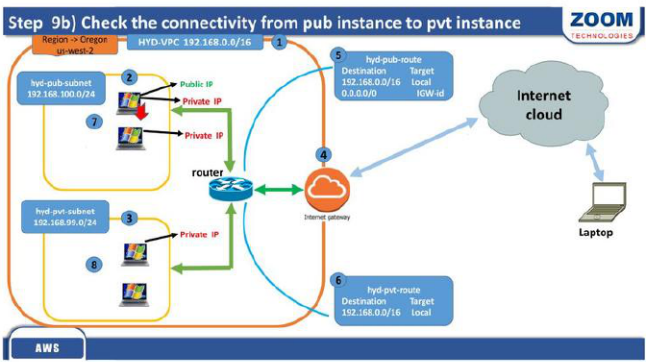

Step 6) Create pvt route and Associate respective subnet, Don't add IGW
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
router
4
Internet gateway
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
Internet cloud
Laptop
AWS

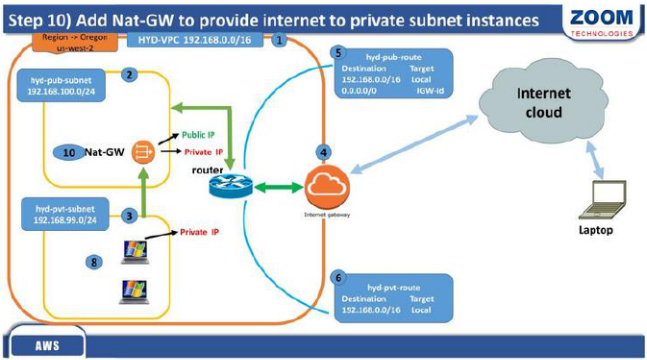

Step 7) Launch VM in Public subnet
ZOOM TECHNOLOGIES
Region -> Oregon us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet 192.168.100.0/24
2
Public IP
Private IP
Private IP
7
router
4
Internet gateway
hyd-pvt-subnet 192.168.99.0/24
3
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
Internet cloud
Laptop
6
hyd-pvt-route
Destination Target
192.168.0.0/16 local
AWS

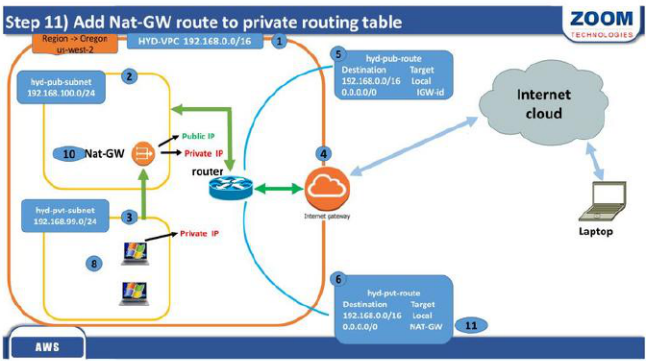

Step 8) Launch VM in Pvt subnet
ZOOM TECHNOLOGIES
Region -> Oregon us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet 192.168.100.0/24
2
Public IP
Private IP
Private IP
7
router
4
Internet gateway
hyd-pvt-subnet 192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
Internet cloud
Laptop
6
hyd-pvt-route
Destination Target
192.168.0.0/16 local
AWS

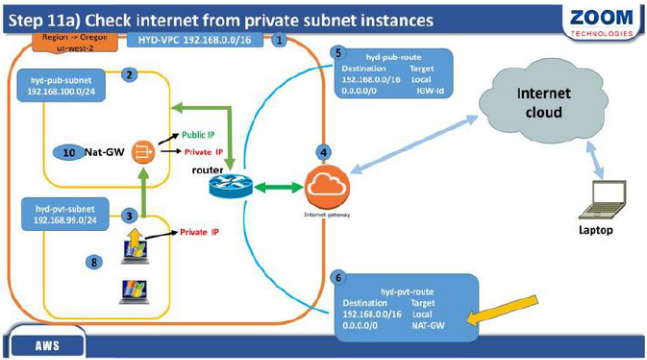

Step 9) Check the connectivity from your Laptop/PC
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
Public IP
Private IP
7
Private IP
router
4
Internet gateway
hyd-pvt-subnet
192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
Internet cloud
Laptop
AWS

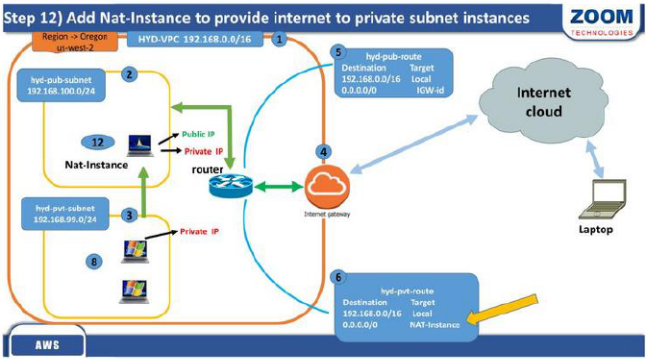

Step 9a) Check the connectivity from public instance to pub instance
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
Public IP
Private IP
7
Private IP
router
4
Internet gateway
hyd-pvt-subnet
192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
Internet cloud
Laptop
AWS

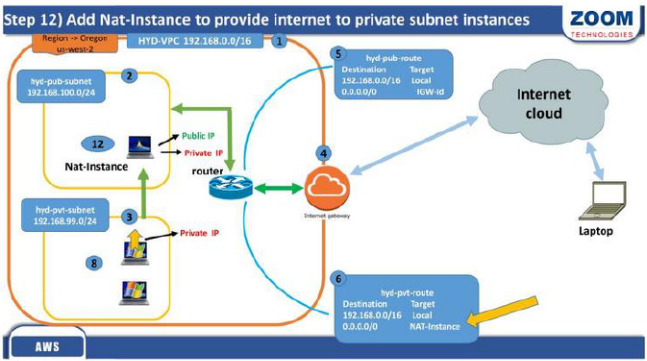

Step 9b) Check the connectivity from pub instance to pvt instance
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
Public IP
Private IP
7
Private IP
router
4
Internet gateway
hyd-pvt-subnet
192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
Internet cloud
Laptop
AWS


Step 10) Add Nat-GW to provide internet to private subnet instances
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
10 Nat-GW
Public IP
Private IP
router
4
Internet gateway
hyd-pvt-subnet
192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
Internet cloud
Laptop
AWS


Step 11) Add Nat-GW route to private routing table
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
10 Nat-GW
Public IP
Private IP
router
4
Internet gateway
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 NAT-GW
11
8
Internet cloud
Laptop
AWS


Step 11a) Check internet from private subnet instances
ZOOM TECHNOLOGIES
Region -> Oregon
us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet
192.168.100.0/24
2
hyd-pvt-subnet
192.168.99.0/24
3
10 Nat-GW
Public IP
Private IP
router
4
Internet gateway
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 NAT-GW
8
Internet cloud
Laptop
AWS


Step 12) Add Nat-Instance to provide internet to private subnet instances
ZOOM TECHNOLOGIES
Region -> Oregon us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet 192.168.100.0/24
2
12
Nat-Instance
Public IP
Private IP
router
4
Internet gateway
hyd-pvt-subnet 192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
Internet cloud
Laptop
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 NAT-Instance
AWS


Step 12) Add Nat-Instance to provide internet to private subnet instances
ZOOM TECHNOLOGIES
Region -> Oregon us-west-2
HYD-VPC 192.168.0.0/16
1
hyd-pub-subnet 192.168.100.0/24
2
12
Nat-Instance
Public IP
Private IP
router
4
Internet gateway
hyd-pvt-subnet 192.168.99.0/24
3
Private IP
8
5
hyd-pub-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 IGW-id
Internet cloud
Laptop
6
hyd-pvt-route
Destination Target
192.168.0.0/16 Local
0.0.0.0/0 NAT-Instance
AWS

VPC Peering

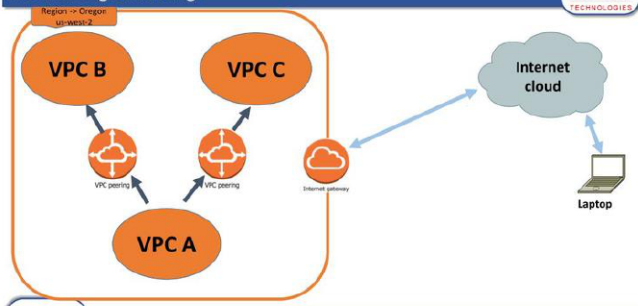
ZOOM TECHNOLOGIES

- VPC peering is used to have communication across multiple VPC's within the same or different region.
- Peering can be done within your own account or other AWS account.
- Transitive peering is not supported.

AWS

VPC Inter Region Peering

ZOOM TECHNOLOGIES



AWS

VPC Cross Region Peering

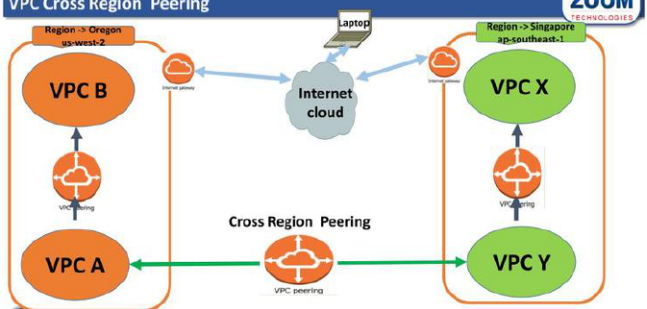
ZOOM TECHNOLOGIES

- Cross Region peering is used to have communication across multiple VPC's across two or more different regions.

AWS

VPC Cross Region Peering

ZOOM TECHNOLOGIES



AWS

DAY 9

Amazon Route53

Amazon Route53

Agenda

ZOOM TECHNOLOGIES

- **What is Route53**
- **Key Features**
- **Routing Policies**

AWS

Amazon Route53 ?

ZOOM TECHNOLOGIES

- DNS is a client/server network communication systems.
- The Domain Name System (DNS) translates Internet domain and host names to IP addresses and vice versa.
- Amazon route 53 is a DNS service Provided by AWS.
- It is an authoritative DNS service.
- **Route 53 is built using AWS's highly available and reliable, global infrastructure of amazon.**
- Improves your availability and application performance at lower cost with Amazon Route 53

AWS

Amazon Route53

ZOOM TECHNOLOGIES

- It uses a global anycast network of DNS servers around the world.
- Anycast is a networking and routing technology that helps your end users' DNS queries get answered from the optimal Route 53 location given network conditions. As a result, your users get high availability and improved performance with Route 53.
- Amazon Route 53 is designed to propagate updates within 60 seconds under normal conditions
- Amazon also supports Private DNS, that lets you have authoritative DNS within your VPCs without exposing your DNS records (including the name of the resource and its IP address(es) to the Internet.

AWS

Amazon Route53 record types

ZOOM TECHNOLOGIES

- Amazon Route 53 DNS record types:
  - A (address record)
  - AAAA (IPv6 address record)
  - CNAME (canonical name record)
  - MX (mail exchange record)
  - NS (name server record)
  - PTR (pointer record)
  - SOA (start of authority record)
  - SRV (service locator)
  - TXT (text record)

AWS

Route53 Health check

ZOOM TECHNOLOGIES

Health Check

- To route the traffic to the end points amazon can perform health checks.
- A health check tells Amazon Route 53 how to send requests to the endpoint.
- A health check is performed using (HTTP, HTTPS, or TCP) protocols, over IP address and ports.
- Amazon Route 53 cannot check the health of endpoints for which the IP address is in local, private, nonroutable, or multicast ranges.

AWS

Amazon Route53 Features

ZOOM TECHNOLOGIES

- Reliable
- Fast
- Integrated with AWS
- Easy to use
- Cost Effective
- Flexible

AWS

Amazon Route 53 Routing Policies

ZOOM TECHNOLOGIES

- **Simple Routing:**
  - With simple routing, Amazon Route 53 responds to DNS queries based only on the values in the resource record set (i.e., the IP).
- **Weighted routing policy**
  - Weighted routing policy is used when multiple resources performs the same function, and you want Amazon Route 53 to route traffic to those resource6 in proportions that you specify. For example, sending 30% of queries to one server, and 70% to the other.
  - For example while testing new versions of software or under load balancer
- **Latency routing policy**
  - Use when you have resources in multiple locations and you want to route traffic to the resource that provides the best latency.

AWS

Amazon Route 53 Routing Policies

ZOOM TECHNOLOGIES

- **Failover Routing:**
  - In Failover routing Route 53 performs the health check , and route traffic to a primary and secondary resource record set.
  - If Primary resource is down the it sends the traffic to secondary resource record set.
- **Geolocation Routing**
  - Geolocation works by mapping IP addresses to locations from where the DNS queries originated from.
  - Example If you have a website on different language then from that region that website can be access
  - To improve the accuracy of geolocation routing, Amazon Route 53 supports the edns-client-subnet extension of EDNS0 (Extension Mechanisms for **DNS** (**EDNS0**).

AWS

Amazon Route 53 Pricing

ZOOM TECHNOLOGIES

- $0.50 per hosted zone / month for the first 25 hosted zones
- $0.10 per hosted zone / month for additional hosted zones

Standard Queries

- $0.400 per million queries – first 1 Billion queries / month
- $0.200 per million queries – over 1 Billion queries / month

AWS

Steps to host a domain in Route 53

ZOOM TECHNOLOGIES

Step 1) Register your domain name with local ISP.

Eg. godaddy.com

Step 2) Host your domain name in Route 53, it adds minimum 4 AWS DNS server of amazon.

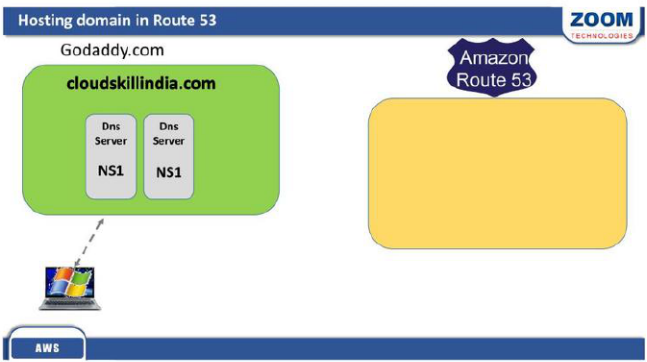
Step 3) Remove the DNS NS record from local ISP and replace with AWS DNS NS record.

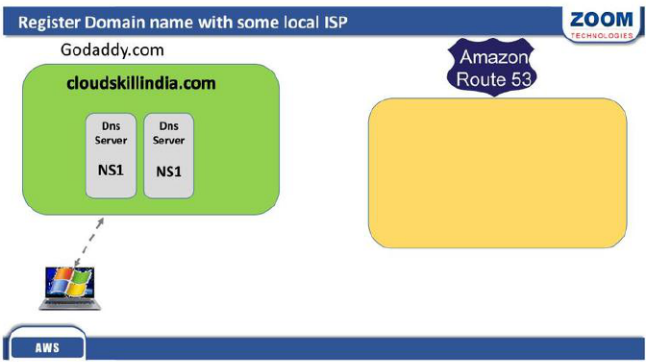
Step 4) Now configure a instance with web server and elastic IP.

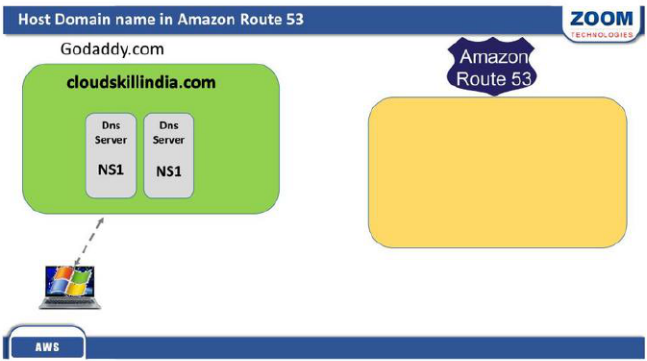
Step 5) Now add your record set (A record, CNAME record) in Route 53.

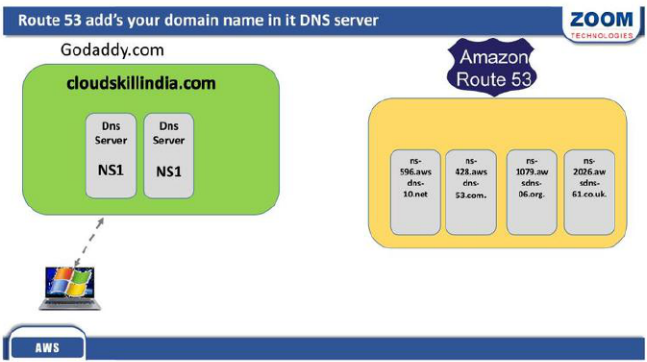
Step 6) Check the site with name instead of IP.

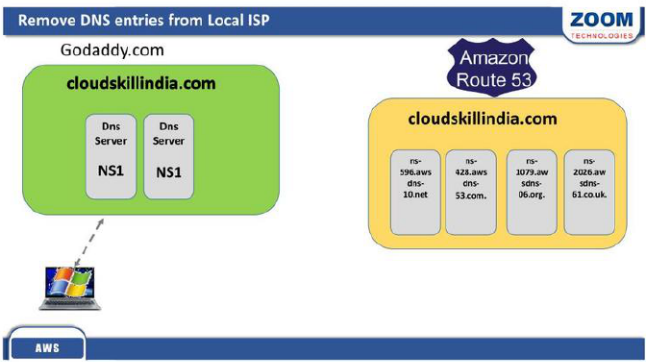
AWS

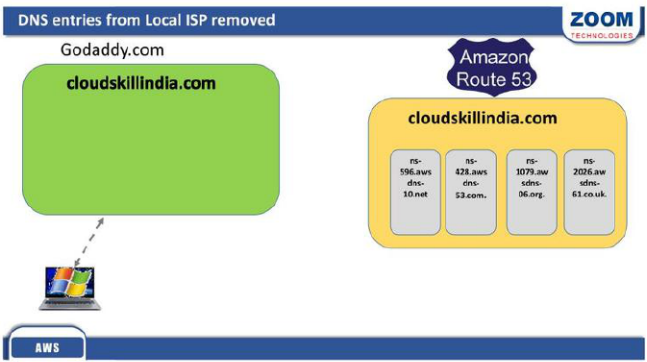

Hosting domain in Route 53
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Dns Server
NS1
Dns Server
NS1
Amazon Route 53
AWS

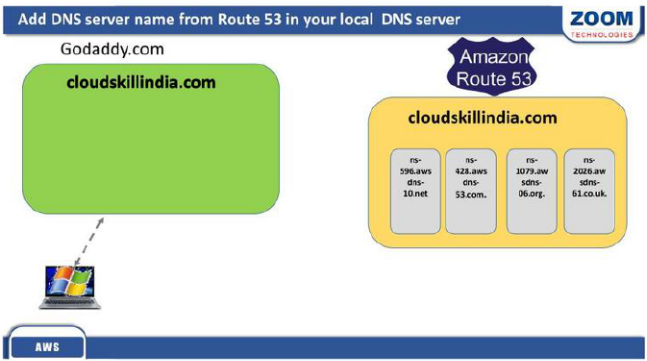

Register Domain name with some local ISP
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Dns Server
NS1
Dns Server
NS1
Amazon Route 53
AWS

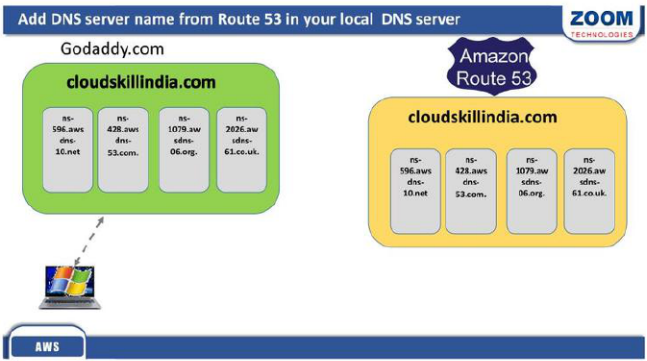

Host Domain name in Amazon Route 53
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Dns Server
NS1
Dns Server
NS1
Amazon Route 53
AWS

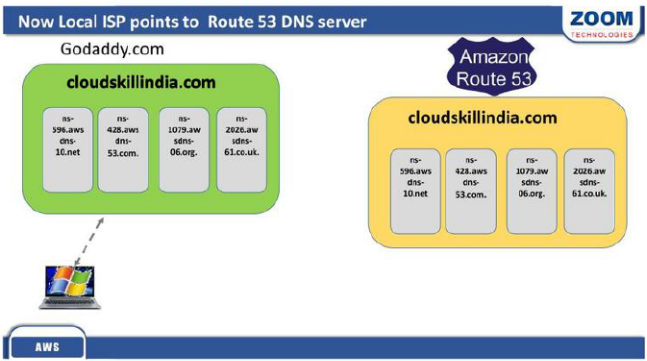

Route 53 add's your domain name in it DNS server
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Dns Server
NS1
Dns Server
NS1
Amazon Route 53
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
AWS

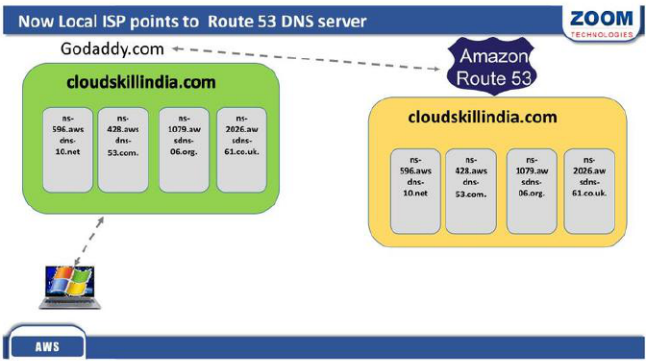

Remove DNS entries from Local ISP
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Dns Server
NS1
Dns Server
NS1
Amazon Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
AWS


DNS entries from Local ISP removed
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Amazon Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
AWS

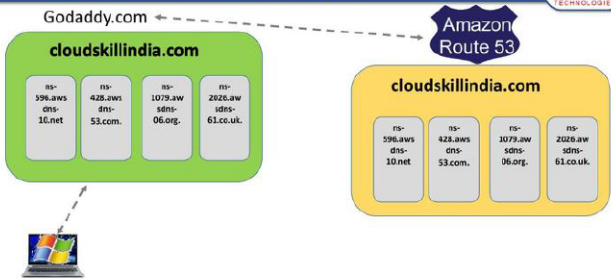

Add DNS server name from Route 53 in your local DNS server
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
Amazon
Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
AWS


Add DNS server name from Route 53 in your local DNS server
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
Amazon
Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2026.aw sdns-61.co.uk.
AWS


Now Local ISP points to Route 53 DNS server
ZOOM
TECHNOLOGIES
Godaddy.com
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2626.aw sdns-61.co.uk.
Amazon Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2626.aw sdns-61.co.uk.
AWS


Now Local ISP points to Route 53 DNS server
ZOOM
TECHNOLOGIES
Godaddy.com
Amazon Route 53
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2626.aw sdns-61.co.uk.
cloudskillindia.com
ns-596.aws dns-10.net
ns-428.aws dns-53.com.
ns-1079.aw sdns-06.org.
ns-2626.aw sdns-61.co.uk.
AWS

Now Local ISP points to Route 53 DNS server



AWS

Amazon VPC (Virtual Private Cloud)

Day 10
SNS (Simple Notification Service)
Cloudwatch
Autoscaling

AWS

AWS SNS
(Simple Notification Service)

- SNS service is used to deliver or sending notification to subscribed endpoints or clients by using push messaging mechanism.

- Service like CloudWatch, Load Balancer, RDS, dynamodb and other aws services uses SNS to send alerts and alarms to the endpoints i.e. through API, HTTP/HTTPS, SQS, EMAIL, AWS Lambda, Mobile Push Notifications, Email, Email-JSON.

AWS Simple Notification Service(SNS)

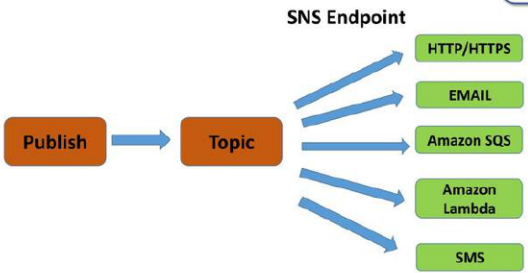
ZOOM TECHNOLOGIES

- Topics are created which is a logical access point.
- Defines Subscriber to whom messages should be published.
- SNS can only guarantee a single delivery to each subscriber of a given topic. This means that if there was a bug or a problem processing the message and there was no specific code to save it somewhere, then the message lost.

AWS

SNS WORK FLOW

ZOOM TECHNOLOGIES



AWS

AWS Simple Notification Service(SNS)

ZOOM TECHNOLOGIES

- Topic names are limited to 256 characters.
- By default, SNS offers 10 million subscriptions per topic, and 100,000 topics per account.
- Amazon SNS messages can contain up to 256 KB of text data, including XML, JSON and unformatted text.
- Each 64KB chunk of published data is billed as 1 request.
- Each SMS message can contain up to 140 bytes,

AWS

Amazon SNS Pricing

ZOOM TECHNOLOGIES

Endpoint Type	Free Tier	Price
Mobile Push Notifications	million	$0.50 per million
Worldwide SMS	100 (US)	Learn more [Charges are applied countries wise]
email/email-JSON	1,000	$2.00 per 100,000
HTTP/s	100,000	$0.60 per million
Simple Queue Service (SQS)	No charge for deliveries to SQS Queues	
Lambda functions	No charge for deliveries to Lambda	

AWS

Amazon CloudWatch

Cloud watch is not going to monitor your on premises Data Center infrastructure. For that we use traditional monitoring tools like :

- Nagios
- Zabbix
- Bigbrother
- MRTG , CACTI
- Airwatch
- Wireshark
- Zenoss
- ps, kill, nice, renice
- vmstat, iostat , Syslog
- Iptraf, netcool
- HPserviceManager
- Windows Task Manager

What Cloud Watch is going to do ?

ZOOM TECHNOLOGIES

- Cloud watch is going to monitor only Service and Resource of AWS infrastructure.
- Monitoring is done based on Metrics.
- Metrics is collection of data through which amazon keeps track of all services and resources.
- Each region contains its own metrics, and are stored for only 14 days, then it gets expire automatically.

AWS

Retention period changd

ZOOM TECHNOLOGIES

- From November 1, 2016 retention period of all metrics changed from 14 days to 15 months.
- Data points with a period of
  - Less than 60 sec — 3 hrs.
  - 1 min — 16 days
  - 5 min — 63 days
  - 1 hr — 455 days (15 months)

AWS