

Intro

Tuesday, October 23, 2018 3:14 PM

Cloud Computing models

1. IaaS (eg : VPC,EC2,EBS)
2. PaaS (eg : RDS, EMR, Elasticsearch, Beanstalk)
3. SaaS (eg : Web based email , office 365,salesforce)
4. Func as a service (server less computing eg:S3,lambda,SNS,DynamoDB)

Advantages and benefits of cloud computing

1. Trade capital expense for variable expense
2. Benefit from massive economies of scale
3. Stop guessing capacity
4. Increase speed and agility
5. Stop spending money on running and maintaining data centers
6. Go global in minutes

Although you are charged for data transfer out, there is no charge for inbound data transfer or for data transfer between other Amazon Web Services within the same region. The outbound data transfer is aggregated across Amazon EC2, Amazon S3, Amazon RDS, Amazon SimpleDB, Amazon SQS, Amazon SNS, and Amazon VPC and then charged at the outbound data transfer rate. This charge appears on the monthly statement as AWS Data Transfer Out.

Need to find out :

bucket url format : <https://s3-ap-southeast-1.amazonaws.com/first-bucket.nauty/background.png>

Arn format :

arn:*partition:service:region:account-id:resource*

Eg :

arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/My App/MyEnvironment

arn:aws:iam::123456789012:user/David

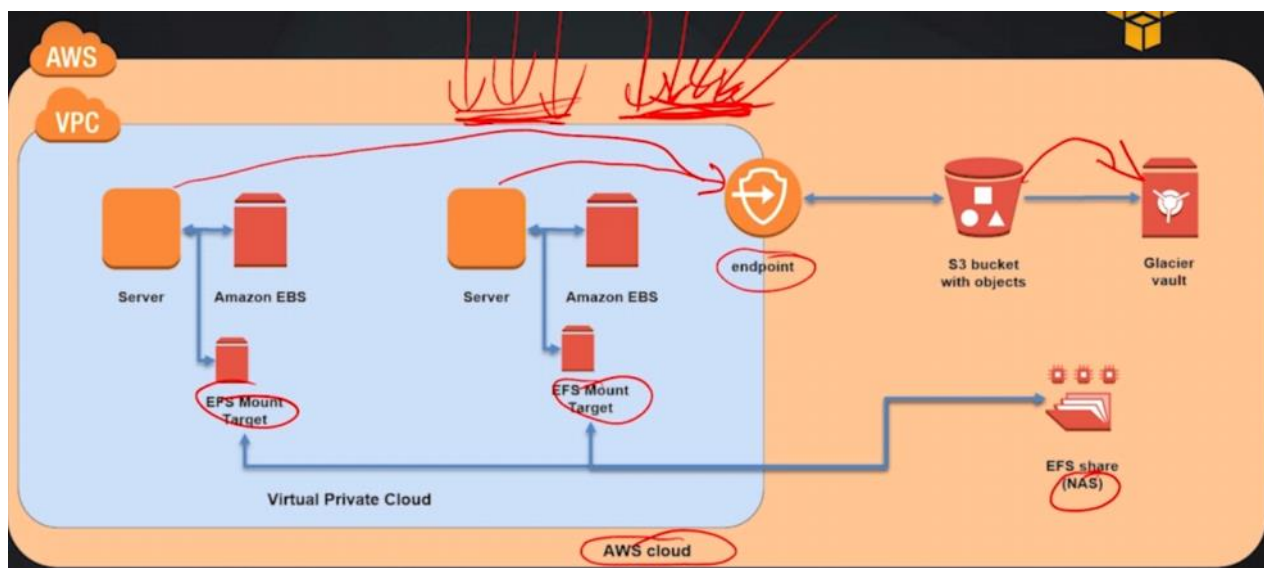
arn:aws:rds:eu-west-1:123456789012:db:mysql-db

arn:aws:s3::my_corporate_bucket/exampleobject.png

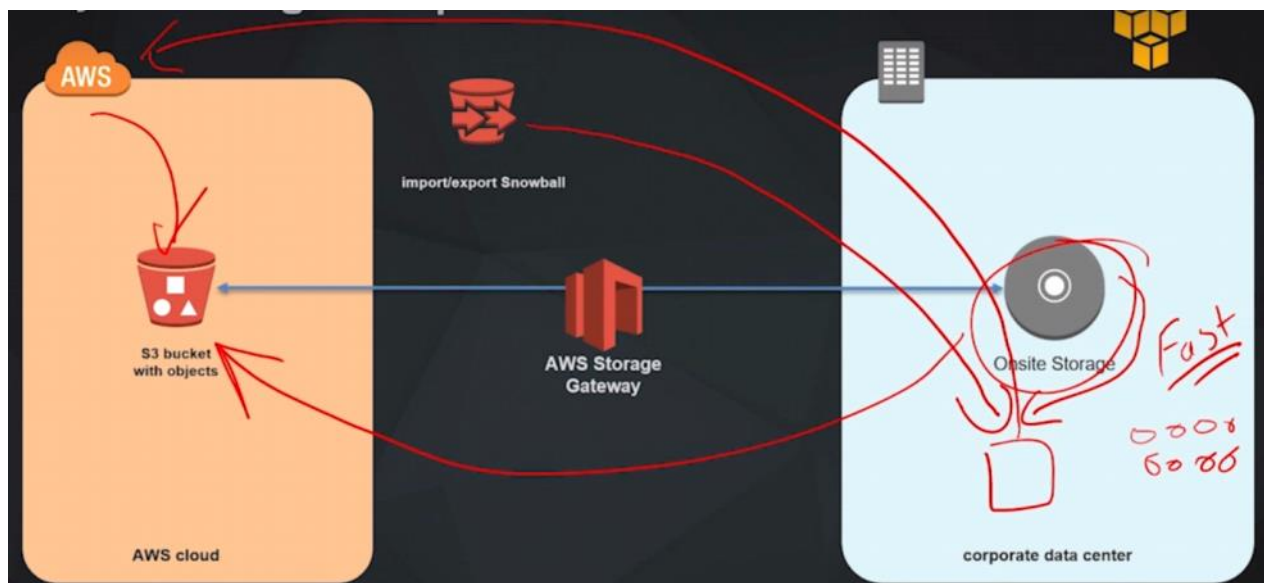
AWS Storage Services

Tuesday, October 30, 2018 2:36 PM

1. S3 -- server less service
2. Glacier - cheapest -- can setup lifecycle rules to move files from s3 to glacier
3. elastic block storage-EBS -- storage for EC2 services
4. Elastic file system - EFS -- Network attach storage -- multiple servers can access this.
5. Storage Gateway -- enables hybrid storage between AWS and on premises Env. Low latency by caching frequently used data.
6. Snowball -- portable petabyte scale datastorage device , used to migrate data from onpremises to AWS.



Hybrid model



AWS Database Services

Tuesday, October 30, 2018 3:42 PM

Relational Database Services (RDS)

DynamoDB -- (Server less service)

RedShift -- cloud warehouse

Aws aurora

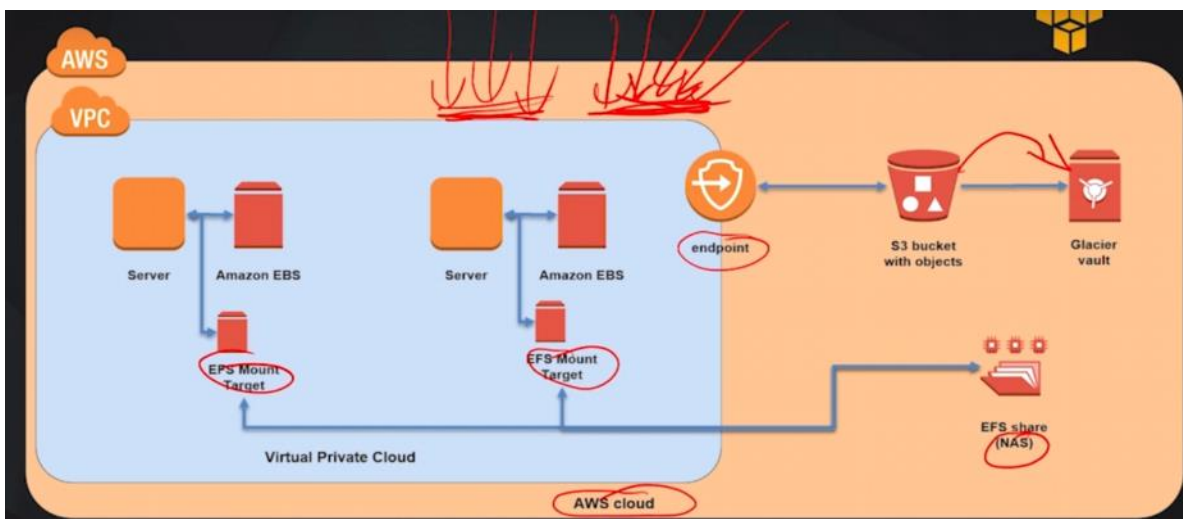
ElastiCache

Database migration Services (DMS)

- help is migrating databases to AWS

- can transfer data from one type of database engine to another type

Neptune -- graph database



AWS Compute service

Wednesday, October 31, 2018 9:38 AM

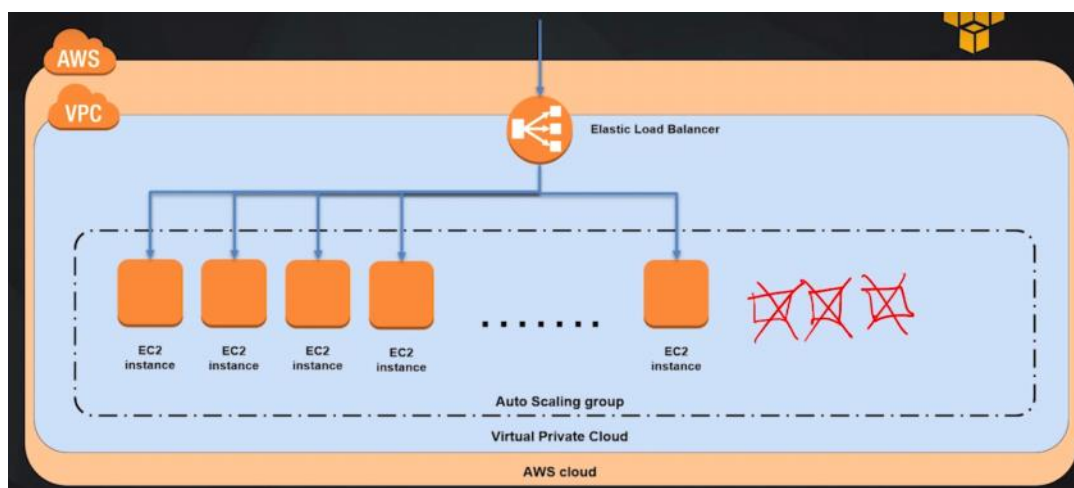
EC2
EC2 autos scaling
EC2 LightSail
Elastic container service
AWS lambda

Auto Scaling :

- automatically creates or removes ec2 instances as per the request volume.
- performs health checks and replaces unhealthy instances with healthy ones



Auto Scaling may cause you to reach limits of other services, such as the default number of Amazon EC2 instances you can currently launch within a region, which is 20

From <<https://www.udemy.com/aws-cloud-certified-practitioner-mock-tests/learn/v4/t/quiz/4466756/results/128191747>>



Auto Scaling Components

The following table describes the key components of Amazon EC2 Auto Scaling.

	<h3>Groups</h3> <p>Your EC2 instances are organized in to <i>groups</i> so that they can be treated as a logical unit for the purposes of scaling and management. When you create a group, you can specify its minimum, maximum, and, desired number of EC2 instances. For more information, see Auto Scaling Groups.</p>
	<h3>Launch configurations</h3> <p>Your group uses a <i>launch configuration</i> as a template for its EC2 instances. When you create a launch configuration, you can specify information such as the AMI ID, instance type, key pair, security groups, and block device mapping for your instances. For more information, see Launch Configurations.</p>



Scaling options

Amazon EC2 Auto Scaling provides several ways for you to scale your Auto Scaling groups. For example, you can configure a group to scale based on the occurrence of specified conditions (dynamic scaling) or on a schedule. For more information, see [Scaling Options](#).

Networking and content delivery services

Wednesday, October 31, 2018 9:49 AM

Amazon CloudFront -- deliver data to edge nodes, protection against Ddos attacks

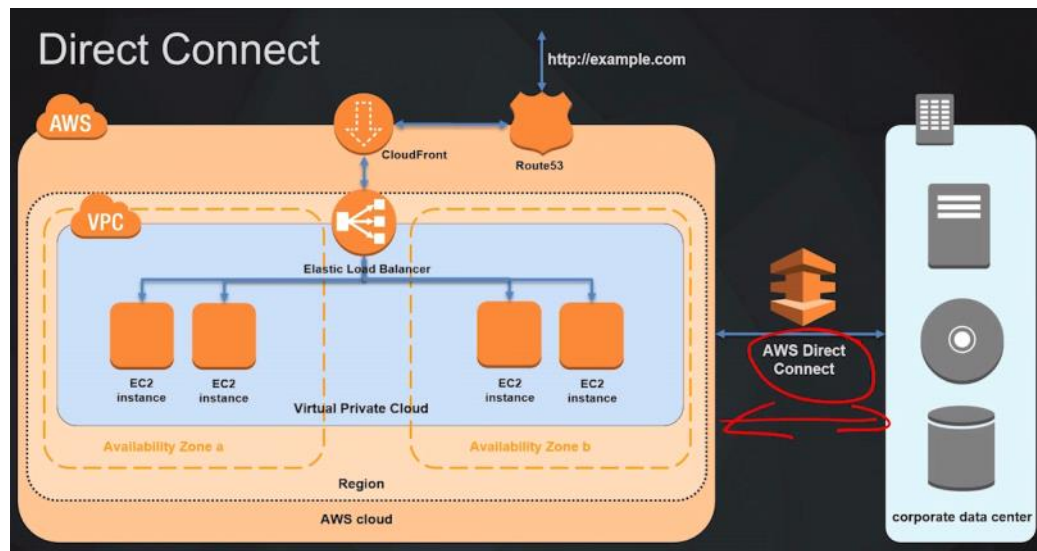
Amazon virtual private cloud (VPC)

Direct connect -- High speed , dedicated network connection to AWS

Elastic load balancer -- distributes incoming request across multiple Ec2 instances also across multiple AZs

Route53 -- DNS (domain name system)

API gateway -- server less service , help developers create and manage APIs



Load Balancer Types

Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. Amazon ECS services can use either type of load balancer.

Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic.

Network Load Balancers and Classic Load Balancers are used to route TCP (or Layer 4) traffic.

Application Load Balancer

- makes routing decisions at the application layer (HTTP/HTTPS)
- supports path-based routing
- can route requests to one or more ports on each container instance in your cluster.
- support dynamic host port mapping.

Network Load Balancer

- makes routing decisions at the transport layer (TCP/SSL).
- It can handle millions of requests per second.

Classic Load Balancer

- makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS).
- currently require a fixed relationship between the load balancer port and the container instance port.

Application Integration services

Wednesday, October 31, 2018

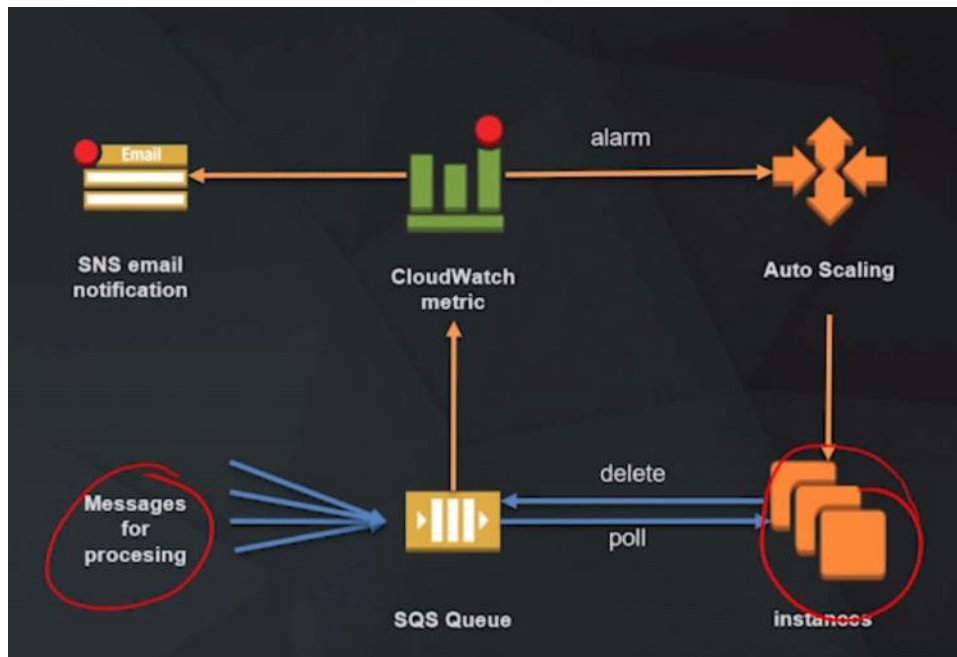
4:36 PM

Step function -- ETL tool

Simple workflow function -- similar to step function

SNS (simple notification service) -- PUB-SUB

SQS (Simple que service)



Customer Engagement Services

Wednesday, October 31, 2018

4:46 PM

Amazon Connect -->

- self service contact center

- Pay as you go model

- Drag - drop Interface

Amazon Pinpoint -->

- Allows you to send email , sms etc to customers

Amazon Simple Email Service -->

Analytics and Hadoop services

Wednesday, October 31, 2018

5:08 PM

Amazon EMR -->

- Hadoop framework as a service

- Can run spark etc

Amazon Athena --> help in analyzing data stored in s3 using standard sql

Amazon elastic search --> like solr

Amazon kinesis --> collect , process and analyses streaming data

QuickSight --> similar to tableau

ML

Wednesday, October 31, 2018 5:13 PM

AWS deepLense --> Deep learning vdo camera

sageMaker --> Flagship ML product, build and train ML model and deploy to AWS

Recognition --> deep learning bases vdo and photo recognition

Lex --> chatbots.

Polly --> text to speech

Comprehend --> uses deeplearning to analyse text to find out relationships

Translate --> uses ML to translate text to number of different languages

Transcribe --> speech recognition service , can analysis audio files stored on S3.

Management Tools

Wednesday, October 31, 2018 2:34 PM

cloud formation --> uses a text file to define our infra (Infra as a code)

AWS service catalog --> allows companies to catalog resources that can be deployed on **AWS**.

Cloudwatch --> Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications

AWS system manager --> provides a UI that help you in viewing operation data from multiple aws services.can also automate tasks across AWS cluster

Aws cloud trail --> logger

Trusted advisor --> online expert system

AWS config --> help in asses , enable and audit of AWS resources

Aws opsWorks --> helps in configuring and automating the deployment of resource in aws.

Security , Identity and Compliance

Wednesday, October 31, 2018

8:51 PM

AWS Artifact --> contains AWS audit and compliance documentation.

AWS Certificate manager --> issues SSL certificates for https communication with our website , it integrates with services like route53 and cloud front , certificates are free.

Amazon cloud directory --> cloud based directory service .unlike LDAP it has multiple hierarchy.

AWS directory service --> fully manages Microsoft Active directory service.

AWS cloud HSM --> hardware security module. Used for regulatory compliance.

Cognito --> provides sign in and signup capability for you mobile and web application. Can integrate with Facebook and google .

IAM --> manages user/user groups access to your resources in your account.

AWS organizations --> allows policy based management for multiple accounts.

Amazon Inspector --> Automated security assessment service.

AWS key management service --> helps in creating and managing encryption keys for the encrypted data

AWS shield --> provides protection against DDOS. Standard version is by default applicable on all accounts.

WEB application firewall -->

Developer tools

Thursday, November 1, 2018 10:36 AM

Cloud 9 -- dev env(IDE) , help in deploying servers directly to aws from IDE

Codestar -- help in develop and deploy application , project management dashboard , issues tracking dashboard

X ray -- debug application

Code comit -- like github

Code pipeline -- help in build , test and deploy code every time the code changes

Code build -- compiles build and makes packages

Code deploy -- service to automate the deployment of packages.

AWS migration services

Thursday, November 1, 2018 10:51 AM

Application discovery services -- gathers information about all the datacenters in an on premises network and help in planning migration to AWS. Data is retained and encrypted .

AWS database migration service --

AWS server migration service -- automate migration of on premises workloads to AWS

Aws snowball

Business productivity and App streaming

Thursday, November 1, 2018 10:53 AM

Amazon workDocs -- secure , fully managed , file collaboration and management service.

Amazon workmail -- business email and calendar service.

Amazon chime -- online meeting service.

Amazon workspace -- remote desktop

Amazon app stream -- streams desktop application from aws to html 5 compatible browsers.

Media services

Thursday, November 1, 2018 10:46 AM

Elemental media convert -- file based vdo transcoding service

Elemental media package -- prepared media package for delivery over the internet , has digital rights management

Elemental media tailor -- insert targeted vdo adds into vdo streams.

Elemental media live -- for creating vdo streams to diliver to tv devises and internet connected devises.

Elemental media store -- storage devise for media

Kinesis vdo stream -- streams vdo through AWS for machine learning.

Mobile services

Thursday, November 1, 2018 10:49 AM

Aws mobile Hub -- allows you to configure your AWS services for mobile applications in one place.

Aws device farm -- App testing service

AWS app sync -- graph QL for mobile.

IOT

Thursday, November 1, 2018 10:55 AM

AWS IOT -- helps in creating an interface between embedded devices and AWS cloud applications

Amazon FreeRTOS -- free OS for microcontrollers

AWS greengrass -- software that lets you run local aws lambda functions etc on AWS connected IOT devices.

Game Dev

Thursday, November 1, 2018 10:57 AM

Amazon gamelift -- deploy , manage , scale dedicated game server on AWS.
Amazon lumberyard -- game dev env , game engine on the cloud

AWS Elastic Beanstalk

Friday, November 2, 2018 10:20 AM

Deployment service

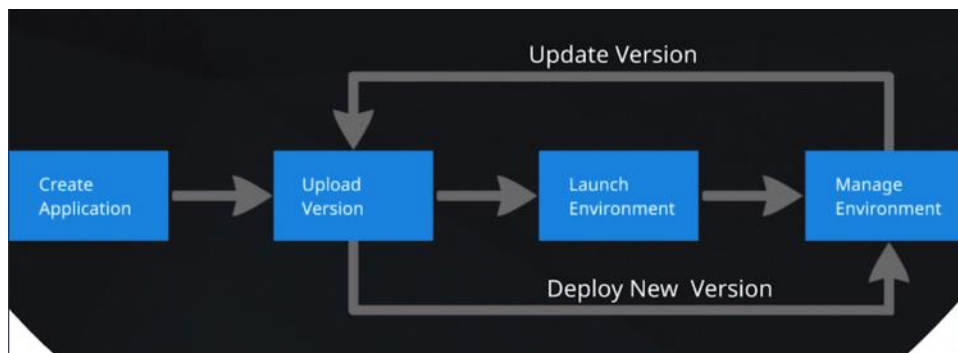
Quickly deploy and manage applications on environments

Automatically handles capacity provisioning , load balancing , scaling and health monitoring

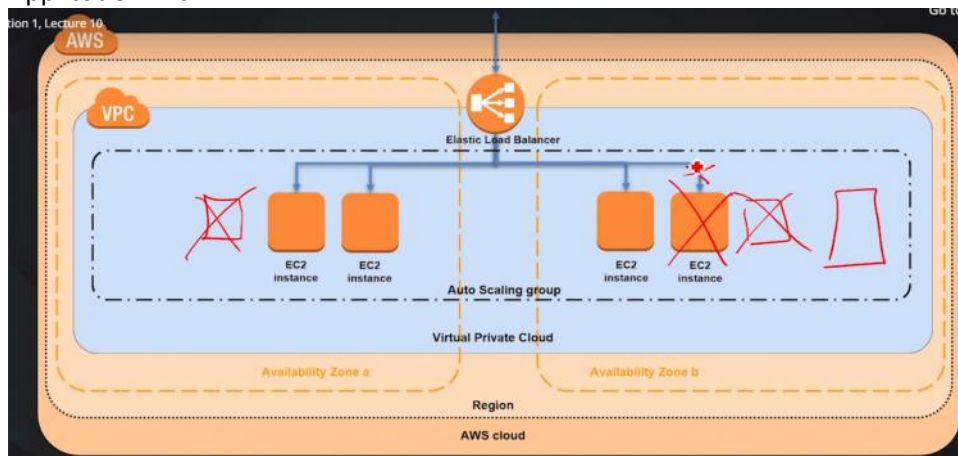
Deployment Options :

- All at once
- Rolling -- a batch at a time
- Immutable (2 env temporarily)
- blue-green (2 env)

Execution cycle:



Application Arch.



Simple monthly calculator

Friday, November 2, 2018 5:39 PM

Input - put in all the service usage , data transfers

Output - it will tell you the estimated monthly cost

Has sample customer samples

Total cost of ownership (TCO)

Friday, November 2, 2018 5:43 PM

Use TCO calculator to compare the cost of running your application in an on-premises to AWS

Takes under consideration the following :

1. Server cost -- hardware , software --> Basic
2. Storage cost -- storage admin cost , storage disks , switches --> Basic
3. Network cost -- bandwidth cost , admin cost
4. IT labor cost

AWS Cost Explorer

Thursday, November 22, 2018 12:29 PM

Investigate where cost are being wasted.

Amazon Inspector

Friday, November 2, 2018 5:52 PM

Automated tool to reduce the cost spent on security.

It is a automated security assessment service

Reduces cost and increases the effectiveness of security assessment and compliance

AWS compliance program

Saturday, November 3, 2018 2:40 PM

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
C5 [Germany]	CISPE	CIS
Cyber Essentials Plus [UK]	EU Model Clauses	CJIS
DoD SRG	FERPA	CSA
FedRAMP	GLBA	ENS [Spain]
FIPS	HIPAA	EU-US Privacy Shield
IRAP [Australia]	HITECH	FFIEC
ISO 9001	IRS 1075	FISC
ISO 27001	ITAR	FISMA
ISO 27017	My Number Act [Japan]	G-Cloud [UK]
ISO 27018	U.K. DPA - 1988	GxP (FDA CFR 21 Part 11)
MTCS [Singapore]	VPAT / Section 508	ICREA
PCI DSS Level 1	EU Data Protection Directive	IT Grundschutz [Germany]
SEC Rule 17-a-4(f)	Privacy Act [Australia]	MITA 3.0
SOC 1	Privacy Act [New Zealand]	MPAA
SOC 2	PDPA - 2010 [Malaysia]	NIST
SOC 3	PDPA - 2012 [Singapore]	PHR
	PIPEDA [Canada]	Uptime Institute Tiers

Compliant

- SOC 1/SSAE 16/ISAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

10 people bookmarked this moment.

Compliance-Enabling

- Criminal Justice Information Services (**CJIS**)
- Cloud Security Alliance (**CSA**)
- Family Educational Rights and Privacy Act (**FERPA**)
- Health Insurance Portability and Accountability Act (**HIPAA**)
- Motion Picture Association of America (**MPAA**)

AWS support plans

Saturday, November 3, 2018

2:43 PM

- Basic
 - Free, Customer service only, No technical support
- Developer
 - Business hours technical support, < 12 business hours response to critical failures
- Business
 - 24/7 technical support, <1 hour response to critical failures
- Enterprise
 - 24/7 technical support from Snr Engineer, <15 minutes response to critical failures

Chat option is available in Business and Enterprise plan only.

Support Concierge -- Enterprise support

If you suspect that AWS resources are being used for abusive purposes, you can contact the AWS Abuse team using the Report Amazon EC2 Abuse form

The AWS Account you want to subscribe for AWS Shield Advanced must have AWS Business Support or AWS Enterprise Support.

Support billing calculations are performed on a per-account basis for all plans. Enterprise Support plan customers have the option to include multiple enabled accounts in an aggregated monthly billing calculation.

AWS security Groups

Monday, November 5, 2018 2:13 PM

Provides instance level security

It provides security at the protocol and port level

It contains a set of rules that filter traffic into and out of an EC2 instance.

Security groups exists within individual VPC.

Security groups Rules

2 types :

1. Inbound
2. Outbound

we do not need the same rules for both outbound traffic and inbound. Therefore any rule that allows traffic **into** an EC2 instance, will allow responses to pass back **out** without an explicit rule in the Outbound rule set.

IAM

Monday, November 5, 2018 3:05 PM

- iam is a global service
- A webservice that allows you to securely control individuals and group access to your AWS resources.
- Create and manage user identities("IAM users") and grant permissions.
- A web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.
- Sample Sign In page url :

A Your sign-in page URL has the following format, by default:

https://Your_AWS_Account_ID.signin.aws.amazon.com/console/

If you forget or lose your credentials, you can't recover them. For security reasons, AWS doesn't allow you to retrieve your passwords or secret access keys and does not store the private keys that are part of a key pair. However, you can create new credentials and then disable or delete the old credentials

IAM permits users to have no more than two active access keys at one time.

Features :

- shared access to your AWS account --> we can give shared access to 1000s of employees
- Granular permissions
- Secure access to AWS resources for applications that run on EC2.
- **identity federation** --> to grant permission for users outside of AWS.
- payment card industry and data security standard compliance
- access log auditing using Cloudtrail
- Eventually consistent
- Free to use

Default : users cant access anything in the account.

Policy : json that define the **effect** , **actions**, **resources** and **optional conditions**.

Eg :

```
Effect = "Allow",
Action="dynamodb:*",
Resources : "arn:XXXXXXXX" (ARN = Amazon resource name)
```

Groups:

Collection of IAM users

Users can belong to multiple groups

Groups can only contain users, cannot be nested.

Roles:

Important if you have people outside of AWS , where we have to assume temp credentials.

-- these are defined permissions that can be assumed by users or resources.

Uses :

- if our EC2 instance wants to access S3 , we can create specific role for the EC2 instance that lets it interact with S3.
- grant access to your resources to users in another AWS account.
- can be used to allow users to temporarily assume a role with least privilege access to critical resources.

IAM Best Practices

Wednesday, November 7, 2018 4:00 PM

- Lock Away Your AWS Account [Root User Access Keys](#)
- Create Individual [IAM Users](#)
- Use [Groups](#) to Assign Permissions to IAM Users
- Use [AWS Defined Policies](#) to Assign Permissions Whenever Possible
- Grant [Least Privilege](#)
- Use [Access Levels](#) to Review IAM Permissions (List, Read, Write, or Permissions management)
- Configure a Strong [Password Policy](#) for Your Users
- Enable [Multi-Factor Authentication \(MFA\)](#) for Privileged Users
- Delegate by Using [Roles](#) Instead of by Sharing Credentials
- Use [Roles for Applications](#) That Run on Amazon EC2 Instances
- [Rotate Credentials](#) Regularly
- Remove [Unnecessary Credentials](#)
- Use [Policy Conditions](#) for Extra Security (eg MFA login)
- [Monitor](#) Activity in Your AWS Account (eg CloudTrail)

AWS organizations

Monday, November 5, 2018 3:06 PM

- Allows multiple AWS accounts used by an organization to be part of an **Organization Unit (OU)**.
- **Service control Policies (SCPs)** allow the whitelisting or blacklisting of services within an organization unit.
- A blacklisted service will not be available even if the **IAM user or group policy allows it**.

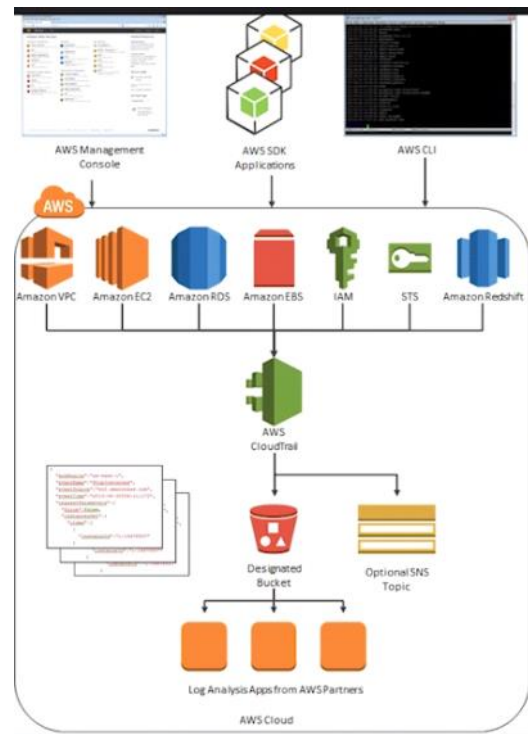
Benefits:

- Centrally manage policies.
- control access to services
- automate account creation and management programmatically with API.
- **consolidate billing**

Cloud Trail

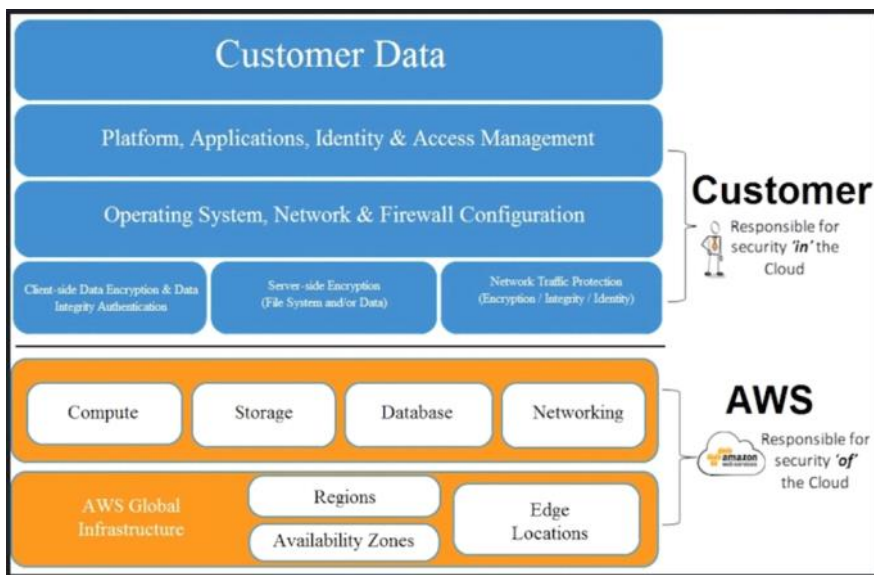
Monday, November 5, 2018

3:06 PM

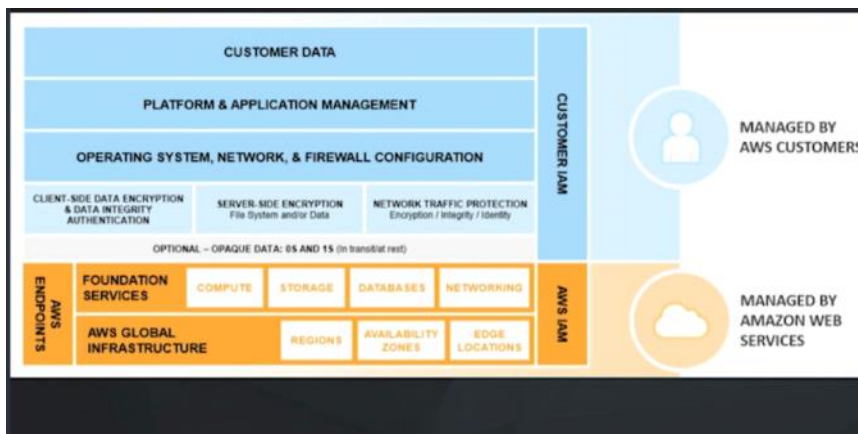


Shared Responsibility model

Monday, November 5, 2018 3:08 PM

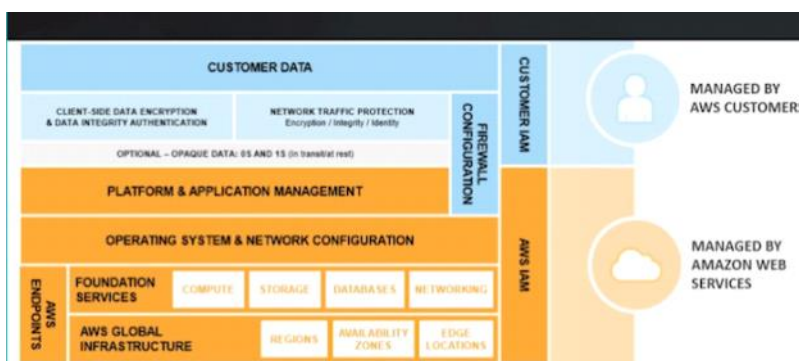


This responsibility model changes , depending on the type of service used



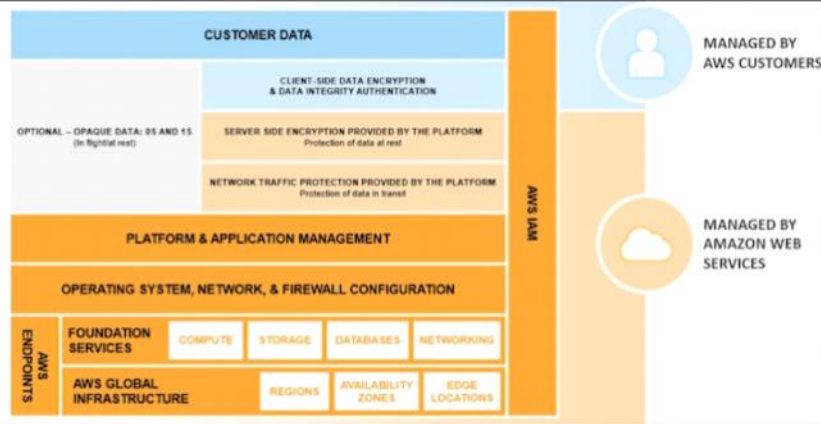
Infrastructure Services e.g.

- Amazon EC2, and related services, such as:
 - Amazon EBS,
 - Auto Scaling, and
 - Amazon VPC.
- You control the operating system,
- You configure and operate IAM



Container Services e.g.

- Amazon RDS
- Amazon EMR,
- AWS Elastic Beanstalk
- AWS provides a managed service
- You are responsible for:
 - network controls eg firewall rules
 - platform-level security separate from IAM



High-level storage, database, and messaging services:

- Amazon S3,
 - Amazon Glacier,
 - DynamoDB,
 - AWS Lambda,
 - Amazon SQS, and Amazon SES
- AWS manages the underlying service components or the operating system on which they reside

AWS Trusted Advisor

Friday, November 9, 2018 9:01 AM

Online service that will audit your infra against best practices.

Categories :

1. Cost optimization
2. Security
3. Performance
4. Service limit
5. Fault tolerant

S3

Friday, November 9, 2018 11:20 AM

Bucket

- containers for objects stored in S3
- total volume of basket is unlimited
- A bucket is owned by the AWS account that created it.
- By default, you can create up to 100 buckets in each of your AWS accounts. If you need additional buckets, you can increase your bucket limit by submitting a service limit increase
- Bucket ownership is not transferable
- After you have created a bucket, you can't change its Region.
- You cannot create a bucket within another bucket.
- If you explicitly specify an AWS Region in your create bucket request that is different from the Region that you specified when you created the client, you might get an error.

The following are the rules for naming S3 buckets in all AWS Regions:

- Bucket names must be unique across all existing bucket names in Amazon S3.
- Bucket names must comply with DNS naming conventions.
- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must not contain uppercase characters or underscores.
- Bucket names must start with a lowercase letter or number.
- Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number.
- Bucket names must not be formatted as an IP address (for example, 192.168.5.4).

Objects

- entities stored in bucket
- 0 byte to 5 TB
- largest object upload is 5 GB
- Multi-part upload for 100 MB to 5 TB

- Improved throughput

Using multipart upload provides the following advantage:

- Quick recovery from any network issues
- Pause and resume object uploads
- Begin an upload before you know the final object size

An object consists of the following:

- Key
- Version
- Value
- Metadata
- Subresources
- Access Control

examples of valid object key names:

4my-organization
my.great_photos-2014/jan/myvacation.jpg
videos/2014/birthday/video1.wmv

Objects consist of **object data** and **metadata**. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata, such as the date last modified, and standard HTTP metadata, such as Content-Type. You can also specify custom metadata at the time the object is stored.

Every object is contained in a bucket. For example, if the object named photos/puppy.jpg is stored in the johnsmith bucket, then it is addressable using the URL

<http://johnsmith.s3.amazonaws.com/photos/puppy.jpg>

An object is uniquely identified within a bucket by a **key (name)** and a **version ID**

In a path-style URL, the **bucket name is not part of the domain** (unless you use a Region-specific endpoint).

For example:

US East (N. Virginia) Region endpoint : <http://s3.amazonaws.com/bucket>.

Region-specific endpoint : <http://s3-aws-region.amazonaws.com/bucket>.

To track the storage cost or other criteria for individual projects or groups of projects, **label** your Amazon S3 buckets using **cost allocation tags**. A cost allocation tag is a key-value pair that you associate with an S3 bucket. After you activate cost allocation tags, AWS uses the tags to organize your resource costs on your cost allocation

Each S3 bucket has a tag set. A tag set contains all of the tags that are assigned to that bucket. A tag set can contain as many as **10 tags**, or it can be empty. Keys must be unique within a tag set, but values in a tag set don't have to be unique

Amazon S3 Data Consistency Model

-- provides read-after-write consistency for PUTS in your S3 bucket in all regions with one caveat.

Note : The caveat is that if you make a HEAD or GET request to the key name (to find if the object exists) before creating the object, Amazon S3 provides eventual consistency for read-after-write.

-- Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all regions.

Updates to a single key are atomic. For example, if you PUT to an existing key, a subsequent read might return the old data or the updated data, but it will never return corrupted or partial data.

-- Amazon S3 achieves high availability by replicating data across multiple servers within Amazon's data centers. If a PUT request is successful, your data is safely stored. However, information about the changes must replicate across Amazon S3, which can take some time

Note

Amazon S3 does not currently support object locking.

The following table describes the characteristics of eventually consistent read and consistent read.

Eventually Consistent Read	Consistent Read
----------------------------	-----------------

Stale reads possible	No stale reads
Lowest read latency	Potential higher read latency
Highest read throughput	Potential lower read throughput

pre-signed URL

A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.

Transfer Acceleration

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. For more information on Reserved Instances, please visit the Link: <http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.htm>

Security

Friday, November 9, 2018 11:20 AM

S3 is secure by default.
Everything is private by default

Security can be modified through :

- IAM roles , users and groups (fine grained control).
- **Bucket policies** applied at the bucket level.
- **access control Lists (ACL)** applied at the bucket and/or object level.

Unlike **access control lists**, which can add (grant) permissions only on individual objects, **Bucket policies** can either add or deny permissions across all (or a subset) of objects within a bucket.

Data protection

Amazon S3 uses a combination of Content-MD5 checksums and cyclic redundancy checks (CRCs) to detect data corruption. Amazon S3 performs these checksums on data at rest and repairs any corruption using redundant data. In addition, the service calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data

Storage classes

Friday, November 9, 2018 11:33 AM

Standard

- 99.9999(11 9s) % durability (multi AZ)
- 99.99% availability
- Supports SSL encryption in transit and at rest.
- Lifecycle management.

Standard - Infrequent Access (IA)

- Same features as S3 standard,
- Lower per GB storage price than standard
- To get the data need to pay per GB retrieval fee.
- Something between **S3** and **glacier**

Standard - One zone IA

- 99.9999(11 9s) % durability (single AZ)
- 99.5 availability
- Lower per GB storage price than standard IA
- To get the data need to pay per GB retrieval fee.

Reduced Redundancy Storage (RRS)

- Old storage class
- 99.99 % durable
- 99.99 availability
- Going to be deprecated
- RRS is not designed to sustain the concurrent loss of data in two facilities. It can sustain the loss of one only.

By default, you can create up to 100 buckets in each of your AWS accounts. If you need additional buckets, you can increase your bucket limit by submitting a service limit increase.

Versioning

Friday, November 9, 2018 11:49 AM

Preserves copies of object inside a basket.
Individual objects can be restored to previous versions
Deleted objects can be recovered.

EC2

Friday, November 9, 2018 9:05 AM

Features :

- A. Instances & Instance types & Tags
- B. Amazon Machine Images (AMIs)
- C. Secure login information for your instances using key pairs
- D. Instance store & EBS volumes
- E. Hosting in Regions & Availability Zones
- F. Security groups
- G. Elastic IP addresses

AMIs are region specific

Placement groups are a clustering of EC2 instances in one Availability Zone with fast (10Gbps) connections between them. This service is used for applications that need extremely low-latency connections between instances.

Purchasing options

Friday, November 9, 2018 9:06 AM

1. On-demand
 - a. Pay by the second with no upfront or terminating cost
2. Reserved Instances
 - a. Purchase at a significant discount, instances that are always available
 - b. Term is 1 -3 years.
3. Scheduled instances
 - a. Purchase instance that are always available on the specified recurring schedule
 - b. Term - 1 year
4. Spot instances
 - a. Request unused EC2 instance , which can lower cost significantly
 - b. Generally cheapest option
5. Dedicated instances
 - a. Pay by the hour
 - b. Instances run on a single tenant hardware
6. Dedicated Hosts
 - a. Pay for a host that is fully dedicated to running your instance.

Note :

The only difference between On-Demand instances and Spot Instances is that Spot instances can be interrupted by EC2 with two minutes of notification when the EC2 needs the capacity back.

<https://aws.amazon.com/ec2/pricing/>

Pricing :

On Demand :

per hour or per second depending on which instances you run.
No longer-term commitments or upfront payments are needed.

recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

Spot Instance :

spare Amazon EC2 computing capacity for up to 90% off the On-Demand price.

recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

Reserved instances :

discount (up to 75%) compared to On-Demand instance pricing.

In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances.

recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

Dedicated Hosts :

A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements.

- Can be purchased On-Demand (hourly).
- Can be purchased as a Reservation for up to 70% off the On-Demand price.

Per Second Billing :

With per-second billing, you pay for only what you use. It takes cost of unused minutes and seconds in an hour off of the bill,

EC2 usage are billed on one second increments, with a minimum of 60 seconds. Similarly, provisioned storage for EBS volumes will be billed per-second increments, with a 60 second minimum.

Per-second billing is available for instances launched in:

- On-Demand, Reserved and Spot forms
- All regions and Availability Zones
- Amazon Linux and Ubuntu

Ec2 Instance Types

Friday, November 9, 2018 9:23 AM

1. General Purpose --> for simple applications (T2,M3,M4)
2. Compute optimized --> High performance servers , eg : video encoding (C3,C4)
3. Memory optimized --> for high performance databases , distributed memory cache (X1,R3,R4)
4. GPU(graphic processing unit)/accelerated computing -- for 3d application , machine learning (G3,G2)
5. Storage optimized --> for NoSQL databases,big data (I3,I2,D2)

Storage options

Friday, November 9, 2018 9:34 AM

Elastic block store (EBS)

- Most common
- replicated within AZ , but if the AZ goes down the data is lost.
- EBS volumes attached at instance launch are **deleted when instance terminated**.
- EBS volumes attached to a running instance are **not deleted** when instance is terminated **but are detached with data intact**.

Instance store

- Physically attached to the host server
- **Data not lost** when OS is rebooted.
- **Data lost** when:
 - # underlying drive fails
 - # instance is stopped
 - # instance is terminated
- Do not rely for valuable , long term data
- cant detach and attach to another instance.
- high speed access.

EBS volumes cannot be used across Availability Zones; however, since snapshots are stored in S3, new volumes can be created from a snapshot and placed into any Availability Zone.

With Amazon EBS, you can create point-in-time snapshots of volumes, which we store for you in Amazon S3. After you've created a snapshot and it has finished copying to Amazon S3 (when the snapshot status is completed), you can copy it from one AWS region to another, or within the same region.

RDS

Sunday, November 11, 2018 12:16 PM

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need

RDS supports the following database products:

- MySQL
- PostgreSQL
- Oracle
- Microsoft SQL Server
- Aurora DB
- MariaDB

Managed RDBMs

It is a container service and handles the following :

- routine db task
- provisioning
- patching
- backup
- recovery
- failure detection
- repair

You are billed with RDS according to the following criteria.

- Instance class & Storage
- Running time
- I/O requests per month & Data transfer
- Backup storage

Amazon RDS uses DB security groups, VPC security groups, and EC2 security groups. In simple terms, a DB security group controls access to a DB instance that is not in a VPC, a VPC security group controls access to a DB instance inside a VPC, and an Amazon EC2 security group controls access to an EC2 instance and can be used with a DB instance.

Each DB instance runs a DB engine. Amazon RDS currently supports the MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server DB engines. Each DB engine has its own supported features, and each version of a DB engine may include specific features. Additionally, each DB engine has a set of parameters in a **DB parameter group** that control the behaviour of the databases that it manages.

The Amazon RDS Service Level Agreement requires that you follow these guidelines:

1. Monitor your memory, CPU, and storage usage.
2. Enable Automatic Backups and Test failover for your DB instance.
3. Do not create more than 10,000 tables using Provisioned IOPS or 1000 tables using standard storage on one MySQL DB instance.
4. Ensure your database workload is less than the I/O than you have provisioned.
5. If your client application is caching the DNS data of your DB instances, set a TTL of less than 30

seconds

InnoDB is the recommended and supported storage engine for MySQL DB instances on Amazon RDS. InnoDB instances can also be migrated to Aurora, while **MyISAM** instances can't be migrated. However, **MyISAM** performs better than InnoDB if you require **intense, full-text search capability**.

We recommend that you do not enable the following modes because they turn off transaction logging, which is required for Multi-AZ:

- Simple recover mode
- Offline mode
- Read-only mode.

Licence:

<https://aws.amazon.com/rds/oracle/faqs/>

We can use the **Read Replica** feature of the database to ensure the data is replicated to another **region**. For more information on an example of Read Replica's

Multi Azs feature

Sunday, November 11, 2018 12:28 PM

--> not available to free tier

--> in this there is another instance of the DB created in a different AZ and is kept in sync with the main DB.

In case the main DB goes down the route 53 service will start pointing to the standby db.

RDS backup

Sunday, November 11, 2018 12:22 PM

- user initiated db snapshots
- automated db backup to S3
- snapshot can be encrypted at rest

Cloud Formation

Monday, November 12, 2018 3:27 PM

There are no limits to the number of templates. Each AWS CloudFormation account is limited to a maximum of 200 stacks.

Template, Parameter, Output, and Resource description fields are limited to **4096** characters.

You can include up to 60 parameters and 60 outputs in a template.

When you use AWS CloudFormation, you manage related resources as a single unit called a stack. You create, update, and delete a collection of resources by creating, updating, and deleting stacks. All the resources in a stack are defined by the stack's AWS CloudFormation template.

Reads Text files (called templets) and interprets them to deploy resources in AWS.

- Infra as code (JSON or YAML templates).
- version control
- template describe all the AWS resources and Cloud Formation takes care of provisioning and configuring.

AWS Cloud Formation templates are text files with extension:

- A. .json
- B. .yaml
- C. .txt
- D. .template

Template Sections

- **Format Version** = version of the cloud formation interpreter
- **Description** = must always follow version.
- **Metadata** = Json and keys that provide additional info.
- **Parameters** = allows values to be passed to cloud formation during stack creation.
- **Mapping** = match parameters to a corresponding name value pairs.
- **Transform** =
 - two purposes :
 1. Can be used to define the server less application model (SAM) to use.
 2. Can be used to include template snippets from Cloud formation to your cloud formation template
- **Outputs** = declare the output values.
- **Resources** = compulsory , declare the resource that we are going to deploy.
- **conditions** = Define when a resource can be created or a property defined.

When AWS CloudFormation creates a resource, it generates a physical name that is based on the combination of the logical name, the stack name, and a unique ID.

For sensitive information, you can use the NoEcho attribute to prevent a parameter value from being displayed in the console, command line tools, or API. If you set the NoEcho attribute to true, the parameter value is returned as asterisks (*****).

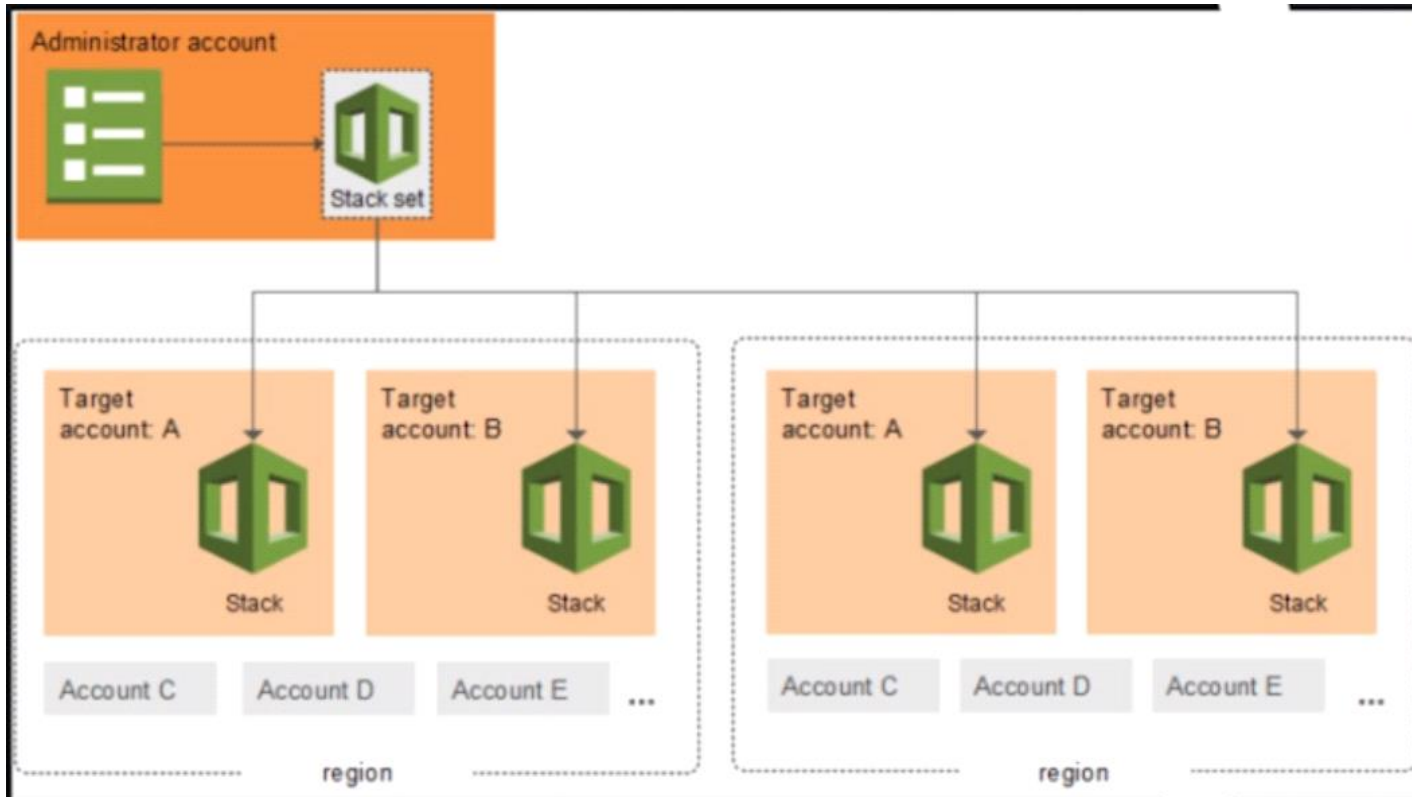
By default, the “**automatic rollback on error**” feature is enabled. This will cause all AWS resources

that AWS CloudFormation created successfully for a stack up to the point where an error occurred to be deleted. This is useful when, for example, you accidentally exceed your default limit of Elastic IP addresses, or you don't have access to an EC2 AMI you're trying to run. This feature enables you to rely on the fact that stacks are either fully created, or not at all, which simplifies system administration and layered solutions built on top of AWS CloudFormation.

Stack Sets

Monday, November 12, 2018 4:08 PM

Allows you to create stacks across regions and in multiple accounts.



Cloud Former

Monday, November 12, 2018 4:10 PM

- creates an AWS cloud Formation template from existing AWS resources in your account.
- you select resources from your account.

CloudFormation Designer

Monday, November 12, 2018 4:12 PM

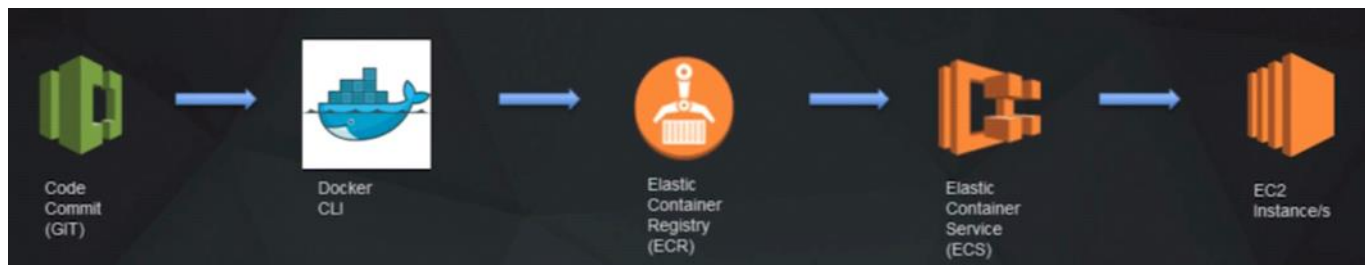
- Visual tool that provides a drag and drop interface for adding resources to templates.
- supports JSON and YAML

ECS - Elastic Container Service

Friday, November 9, 2018 10:08 AM

This uses Ec2 instance to run Docker containers .

Docker : Docker containers wrap up a piece of software in a complete filesystem that contains everything it needs to run: code , runtime , system tools , system libraries - anything you can install on a server. This guarantees that it will always run the same , regardless of the environment it is running in .



Amazon Glacier

Friday, November 9, 2018 11:45 AM

- Archiving solution
- Lowest cost AWS
- 11 9 durability across 3 AZs
- 3 retrieval options
 - # **Expedite** (1 -5 mins)
 - # **Standard** (3-5 hours)
 - # **Bulk** (5-12 hours)

Note that the **AWS Console cannot be used to upload data onto Glacier**. The console can only be used to create a Glacier vault which can be used to upload the data. For more information on uploading data onto Glacier. For more details please refer to link- <https://aws.amazon.com/glacier/>

There is no maximum limit to the total amount of data that can be stored in Amazon Glacier. Individual archives are limited to a maximum size of 40 terabytes.

Dynamo DB

Sunday, November 11, 2018 12:35 PM

Amazons NoSQL DB.

Consists of :

- Tables

- Table has attributes (cols)

- Items (rows)

- Partition key and sort key(optional) -- to search for a data and sort it.

Dynamo Db secondary Indexes:

--> Efficient access to data with attributes other than the primary key.

2 types

- **Local secondary index** -- same partition key but different sort key

- **global secondary index** -- different partition and sort key

Amazon Neptune

Sunday, November 11, 2018 12:44 PM

Graph database

Purpose : build to store and navigate relationships.

Graph Structure :

- nodes
- edges
- properties

Graph query languages:

- Gremlin
- SPARQL

Amazon RedShift

Sunday, November 11, 2018 12:50 PM

Fully managed big data warehouse service.

Designed for OLAP and BI applications

Cluster is a set of nodes ,
1 leader and many compute nodes.

Elastic cache

Sunday, November 11, 2018 12:55 PM

Fully managed , in memory data store service.

Low latency data access.

Redis and **Memcached** engine

VPC

Sunday, November 11, 2018 2:32 PM

Default maximum VPCs per region = 5

Maximum subnets per VPC = 200

Maximum VPN connections per region = 50

The minimum size of a subnet is a /28 (or 14 IP addresses.) for IPv4. Subnets cannot be larger than the VPC in which they are created

It is a virtual cloud area in the AWS.

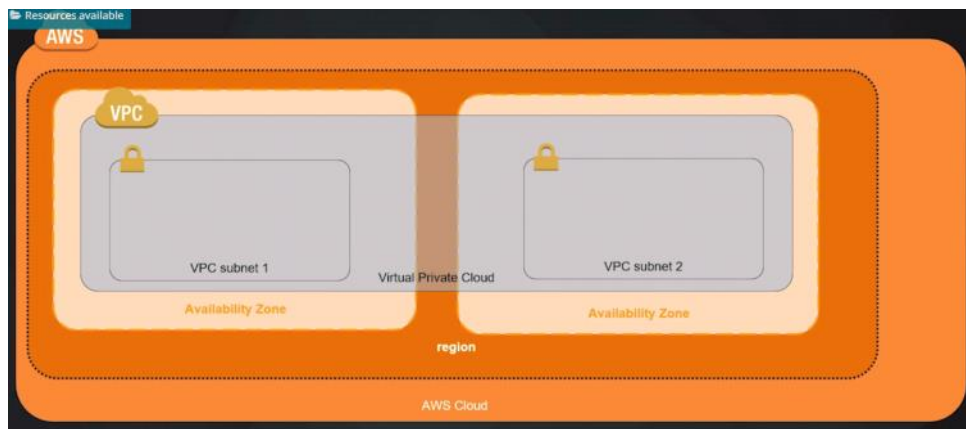
Primary private IP addresses retained for the instance's or interface's lifetime.

Secondary private IP addresses can be assigned, unassigned, or moved between interfaces or instances at any time



Each VPC has at least one VPC subnet.

By having multiple subnets across multiple AZ we can launch multiple EC2 instances across different AZs



Connection types :

- Internet gateway.
- virtual private gateway.
- AWS direct connect.

Requirement for internet connectivity:

1. EC2 instance has a public IP address
2. VPC has a internet gateway
3. Route defined in a route table from subnet to IGW(internet gateway).

SUBNET

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.

NAT (network address translation)

NAT maps multiple private IPv4 addresses to a single public IPv4 address. A NAT device has an **Elastic IP address** and is connected to the internet through an internet gateway. You can connect an instance in a private subnet to the internet through the NAT device, which routes traffic from the instance to the internet gateway, and routes any responses to the instance.

A NAT gateway provides the most secure solution for granting EC2 instances in private subnet the ability to download software packages. However, the NAT gateway **MUST** be placed in a public subnet, and a route to it must be created in the route table associated with the private subnets.

VPN

A VPN connection consists of a **virtual private gateway** attached to your VPC and a customer gateway located in your data center. A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection. A customer gateway is a physical device or software appliance on your side of the VPN connection

Billing

There are **no additional charges** for creating and using the VPC itself. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges. If you connect your VPC to your corporate datacenter using the optional hardware VPN connection, **pricing is per VPN connection-hour** (the amount of time you have a VPN connection in the "available" state.) Partial hours are billed as full hours. **Data transferred over VPN connections will be charged at standard AWS Data Transfer rates.**

VPC security

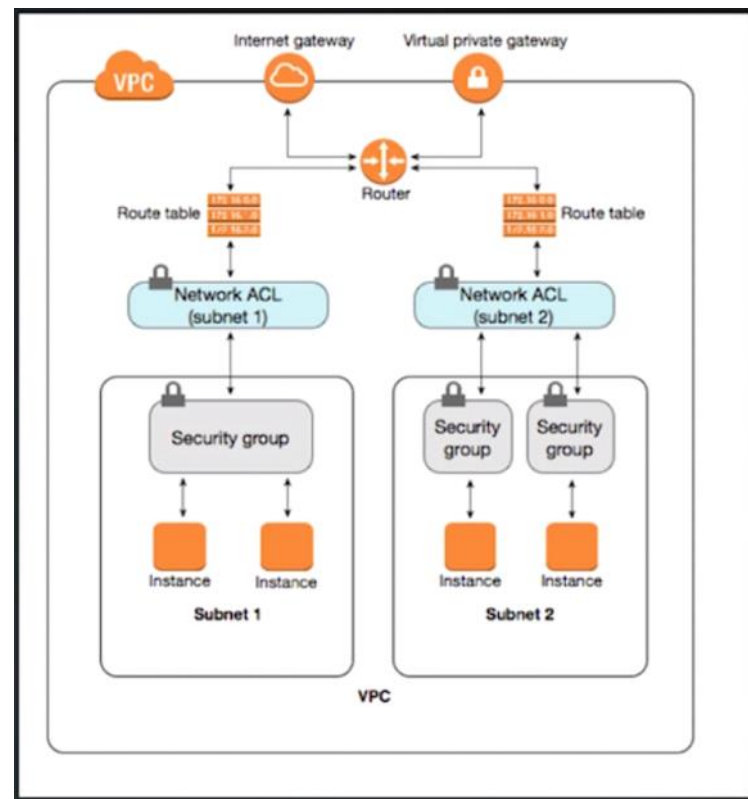
Sunday, November 11, 2018 3:16 PM

Security groups :

- firewall at instance level
- State full

Network Access control List (ACL):

- firewall at subnet level
- it is as a second level of defense
- Stateless



Cloud Watch

Tuesday, November 13, 2018 11:23 AM

The metrics are not all available in all regions.

Eg :

1. Billing
2. Dynamo DB
3. EC2 , EBS
4. Etc

We can get the cloud watch using 3 ways :

1. CLI
 - a. Max number of data points : 50,850
 - b. Max data points in a single req : 1440
2. API
3. Management console

Alarms 3 stats :

1. OK
2. ALARM
3. INSUFFICIENT_DATA

Metrics produced by AWS services are **standard resolution** (1 minute) by default. Only custom metrics that you define with a **storage resolution** of 1 second support sub-minute periods.

Basic Monitoring metrics (at 5 minute frequency) for Amazon EC2 instances are free of charge, as are all metrics for Amazon **EBS volumes, Elastic Load Balancers, and Amazon RDS DB instances.**

Memory Utilization is not included as part of EC2 Cloud Watch **basic monitoring**

Aggregate statistics are only available with **detailed monitoring**

Cloud watch Logs

Tuesday, November 13, 2018 11:38 AM



- This can store , monitor and access your logs files from EC2, cloud trail or other sources.
- Allows to monitor our logs in Realtime.
 - Log Streams - seq of log events from a source
 - log groups - streams the same retention , monitoring and access control settings.
- Metric filters -- this help cloud watch to define how info is extracted to create data points.
- Retention settings -- defines how long log events are kept in cloud watch logs.

Cloud watch events

Tuesday, November 13, 2018 11:46 AM

Events :

1. Occur when resources change state
2. Cloud trail integration

Rules :

1. Help us in matching the events and routing them to one or more targets.

Targets :

1. The action that needs to be performed eg : AWS lambda function , amazon SNS , SQS, etc.

AWS Glue

Tuesday, November 27, 2018 12:29 PM

is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue is serverless, so there is no infrastructure to buy, set up, or manage. It automatically provisions the environment needed to complete the job, and customers pay only for the compute resources consumed while running ETL jobs. For more details please refer the following link: <https://aws.amazon.com/glue/>

AWS Budgets

Wednesday, November 28, 2018 4:41 PM

Set custom budgets that alert you when you exceed your budgeted thresholds. AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

You can also use AWS Budgets to set RI utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. RI alerts support Amazon EC2, Amazon RDS, Amazon Redshift, and Amazon ElastiCache reservations.

Budgets can be tracked at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic.

Budgets can be created and tracked from the AWS Budgets dashboard or via the Budgets API.

AWS Cost Explorer

Wednesday, November 28, 2018 4:45 PM

AWS Cost Explorer lets you dive deeper into your cost and usage data to identify trends, pinpoint cost drivers, and detect anomalies.

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. Get started quickly by creating custom reports (including charts and tabular data) that analyze cost and usage data, both at a high level (e.g., total costs and usage across all accounts) and for highly-specific requests (e.g., m2.2xlarge costs within account Y that are tagged “project: secretProject”).

Guard Duty

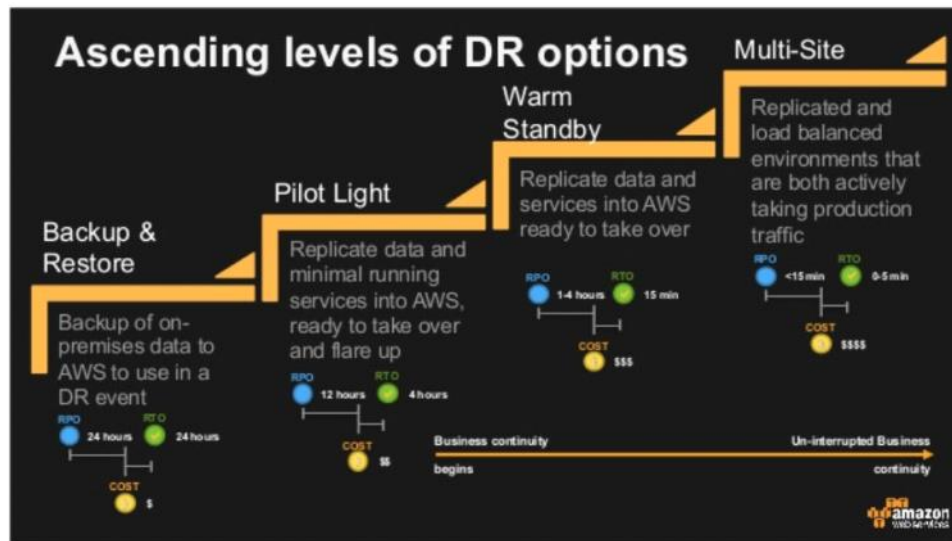
Wednesday, November 28, 2018 4:47 PM

Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behaviour to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

Deployment

Tuesday, November 13, 2018

11:52 AM



Infra as Code

Tuesday, November 13, 2018 11:53 AM

Allows infra to be managed in the same way as software.

Eg : cloud formation

Continuous Deployment - Application

Tuesday, November 13, 2018 11:55 AM

Automated delivery of production ready code.
Allows rapid deployment and roll back if necessary.

Eg :

- code commit
- code pipeline
- Elastic beanstalk
- Etc...

Application Updating options

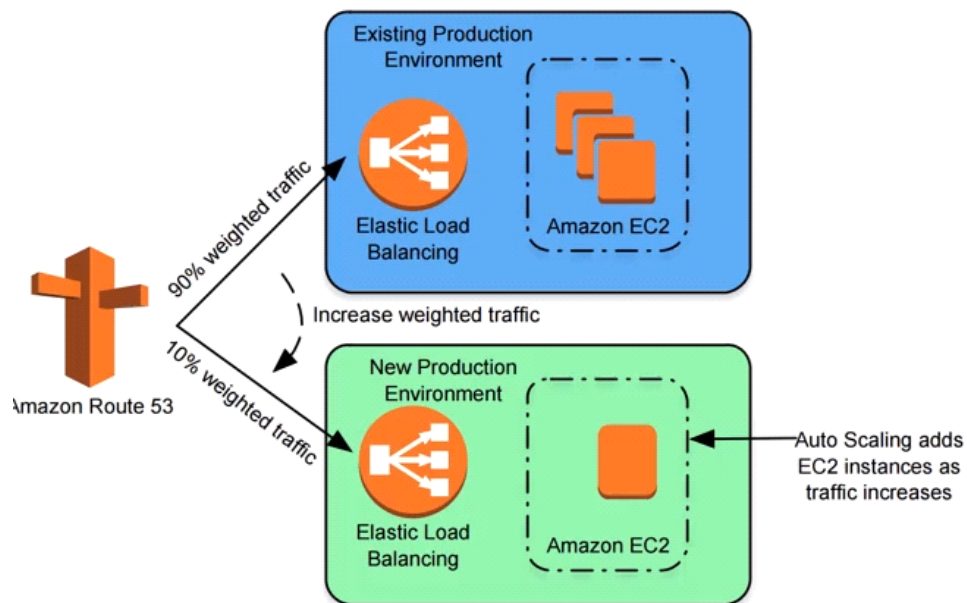
Tuesday, November 13, 2018 12:00 PM

1. Prebaking AMIs -- slow and expensive option
2. In place Upgrade -- application updates on live Amazon EC2 instances
3. Disposable Upgrade -- Rolling out new EC2 instances and terminating older instances
-- Allows staged deployment

Blue green Deployment

Tuesday, November 13, 2018

12:03 PM



What you should review

Thursday, November 22, 2018

1:08 PM

- [You have an application that sends push messages to mobile devices. Which service should you use?](#) -- SNS
- [A _____ tells Auto Scaling when and how to scale. You can create a _____ based on the occurrence of specified conditions \(dynamic scaling\) or you can create one based on a specific schedule.](#) -- scaling options
- [What happens, by default, when one of the resources in a CloudFormation stack cannot be created?](#) -- either all are created or rollback
- [You have an application that requires ad-hoc data mining and analytics of manufacturing data. What is best suited for this application?](#) -- EMR
- [You would like to be able to check department costs have not exceeded budget for the month. What is the best way to achieve this?](#) --
- [In the shared responsibility model, updates and security patches to EC2 instances is the responsibility of AWS.](#)
- [What licensing options are available for RDS Oracle?](#)

Partial upfront cost reserved etc

Which of the following disaster recovery deployment mechanisms has the lowest downtime?

- Devops

Warm standby

Pilot light

Backup restore

<https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/>

AWS Guard Duty