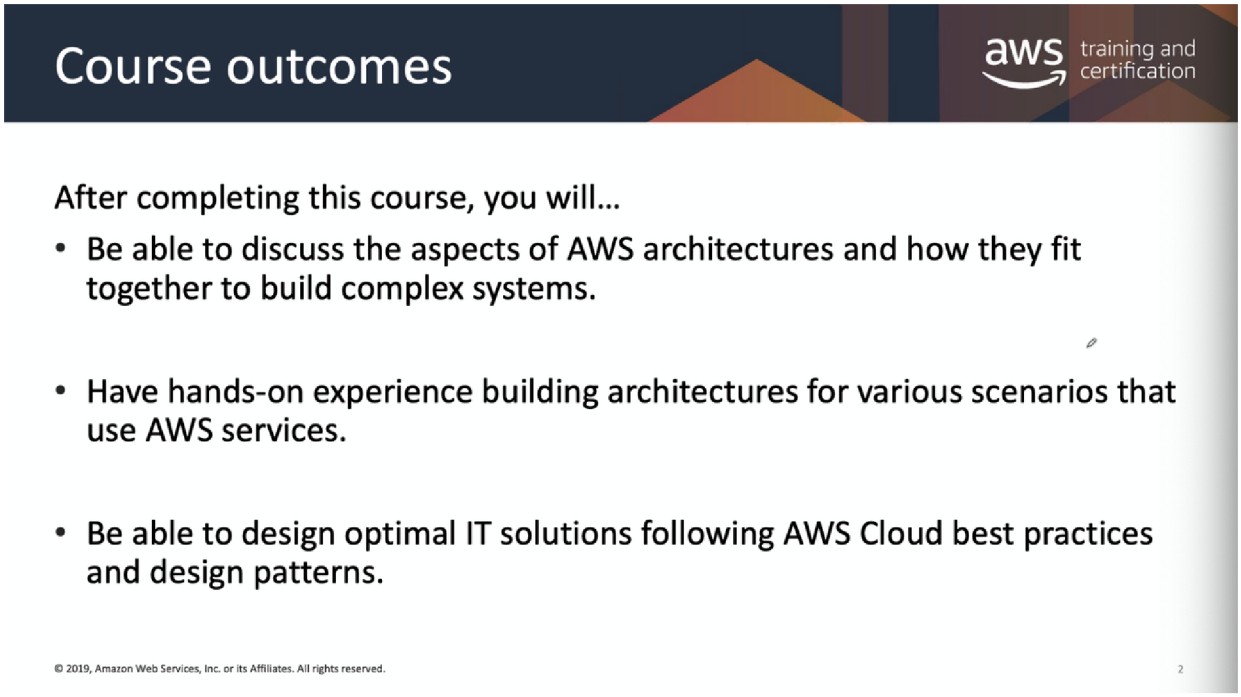
Architecting on AWS

day 3
https://www.youtube.com/watch?v=LCjX2rsQ2wA
https://aws.amazon.com/blogs/security/discover-sensitive-data-by-using-custom-data-identifiers-with-amazon-macie/

https://www.normkean.com/arcacc/arcacc_day1.html
☎9/14
Module 1: Introduction



Amazon.com

aws training and certification

Amazon.com's e-commerce tools were a " jumbled mess:"

- Applications and architectures were built without proper planning.
- Services had to be separated from each other.

Solution: Tools became a set of well documented APIs, which became the standard for service development at Amazon.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Problems persisted

aws training and certification

Amazon.com still struggled to build applications quickly.

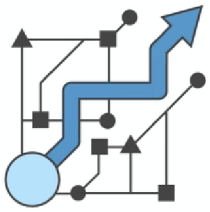
- Database, compute, and storage components took 3 months to build.
- Each team built their own resources, with no planning for scale or re-usability.

Solution: Built internal services to create highly available, scalable, and reliable architectures on top of their infrastructure. In 2006, Amazon started selling these services as Amazon Web Services (AWS).

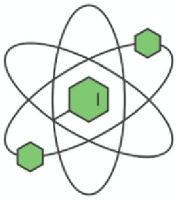
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

What is the cloud? What is AWS?

aws training and certification



Programmable resources



Dynamic abilities

Pay as you go

What other advantages does the cloud offer?

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Six advantages of cloud computing

aws training and certification

Trade capital expense for variable expense

Benefit from massive economies of scale

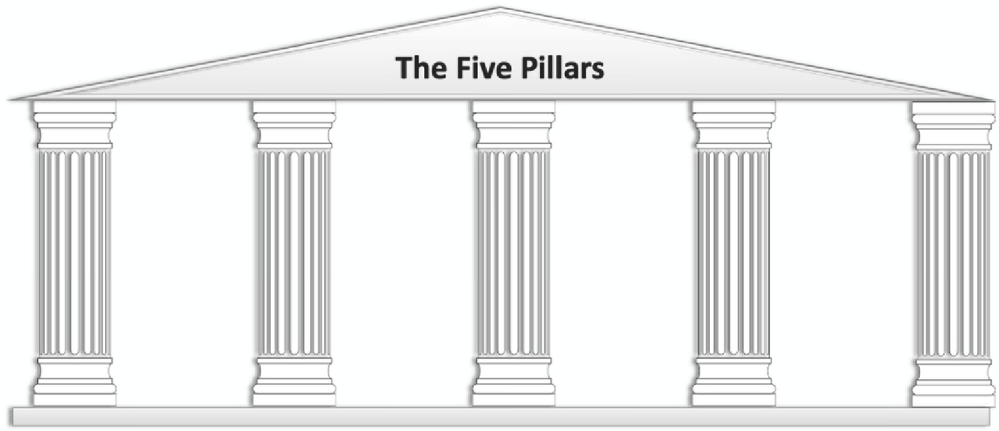
Stop guessing about capacity

Increase speed and agility

Focus on what matters

Go global in minutes

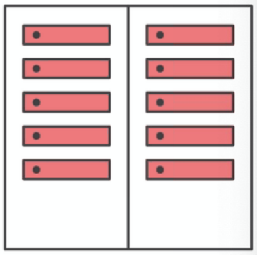
The AWS Well-Architected Framework



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Reliability

- Dynamically acquire computing resources to meet demand
- Recover quickly from infrastructure or service failures
- Mitigate disruptions such as:
  - Misconfigurations
  - Transient network issues



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Cost optimization

aws training and certification

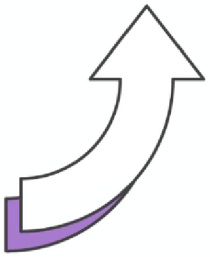
- Measure efficiency
- Eliminate unneeded expense
- Consider using managed services

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Performance efficiency

aws training and certification

- Choose efficient resources and maintain their efficiency as demand changes
- Democratize advanced technologies
- Mechanical sympathy



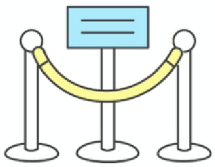
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Operational excellence

- The ability to run and monitor systems
- Continually improve supporting process and procedures

Deployed

Updated



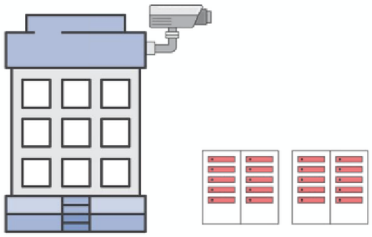
Operated

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc

AWS data centers

- A single data center typically houses tens of thousands of servers
- All data centers are online, not “cold”
- AWS custom network equipment:
  - Multi-ODM sourced
  - Customized network protocol stack



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Availability Zones

aws training and certification

Each Availability Zone is:

- Made up of one or more data centers
- Designed for fault isolation
- Interconnected with other Availability Zones using high-speed private links

- You can choose your Availability Zones
- AWS recommends replicating across Availability Zones for resiliency

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

77 AZs!

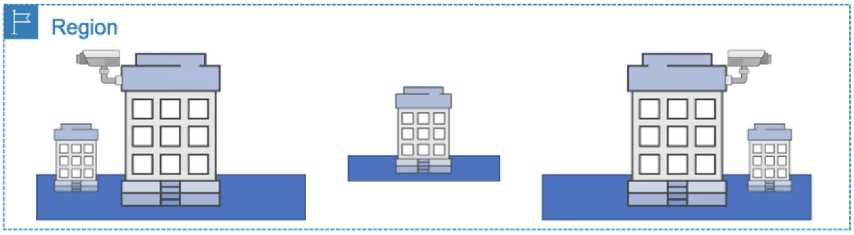
AWS Regions

aws training and certification

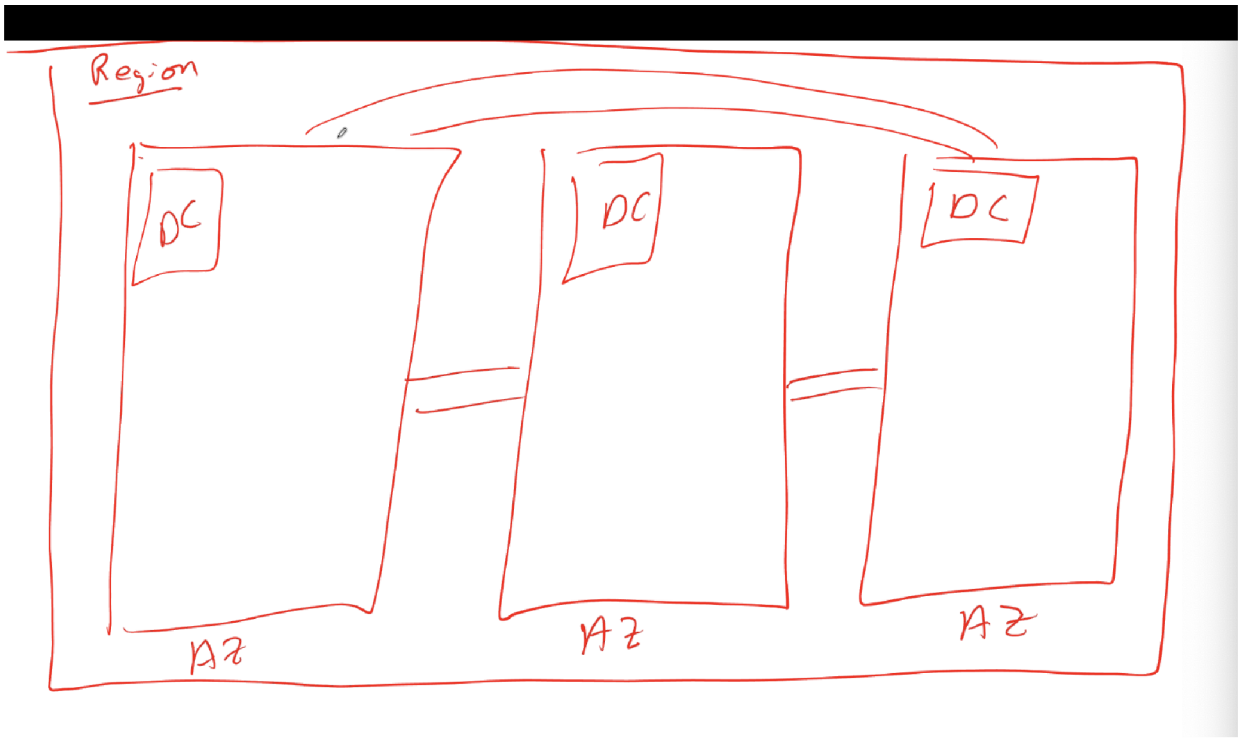
Each AWS Region is made up of two or more Availability Zones.

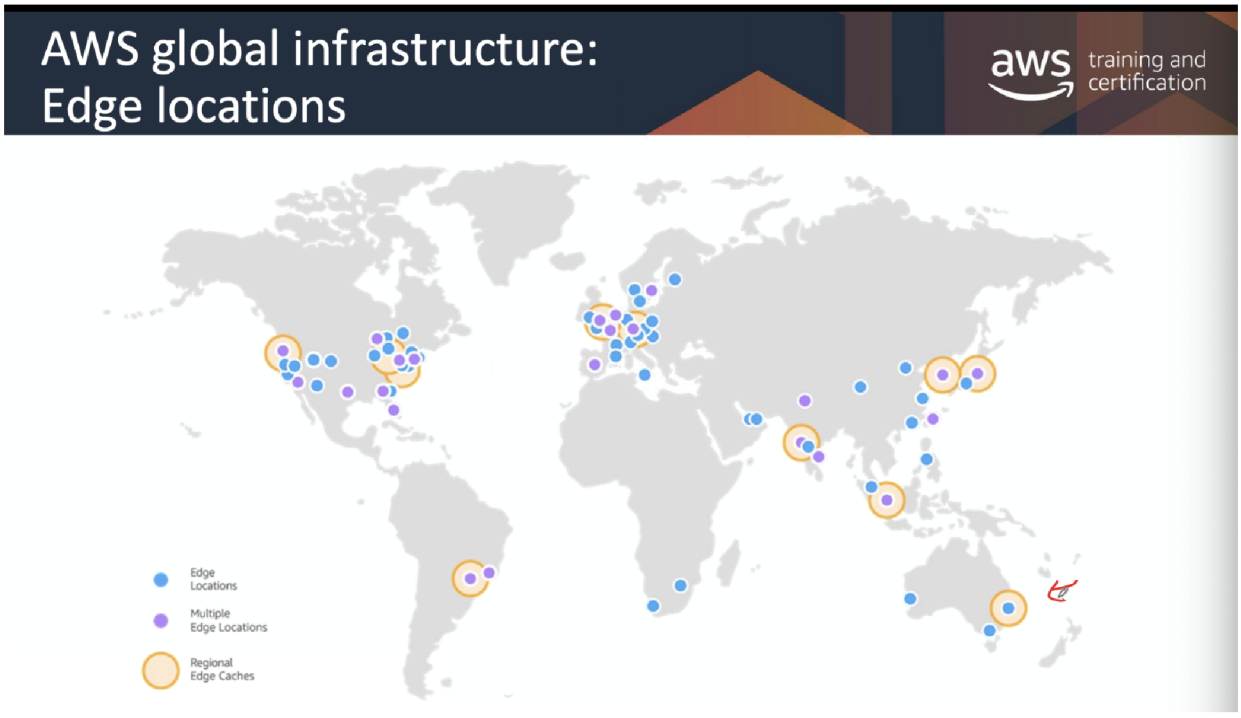
24

- AWS has ~~22~~ Regions worldwide.
- You enable and control data replication across Regions.
- Communication between Regions uses AWS backbone network infrastructure.

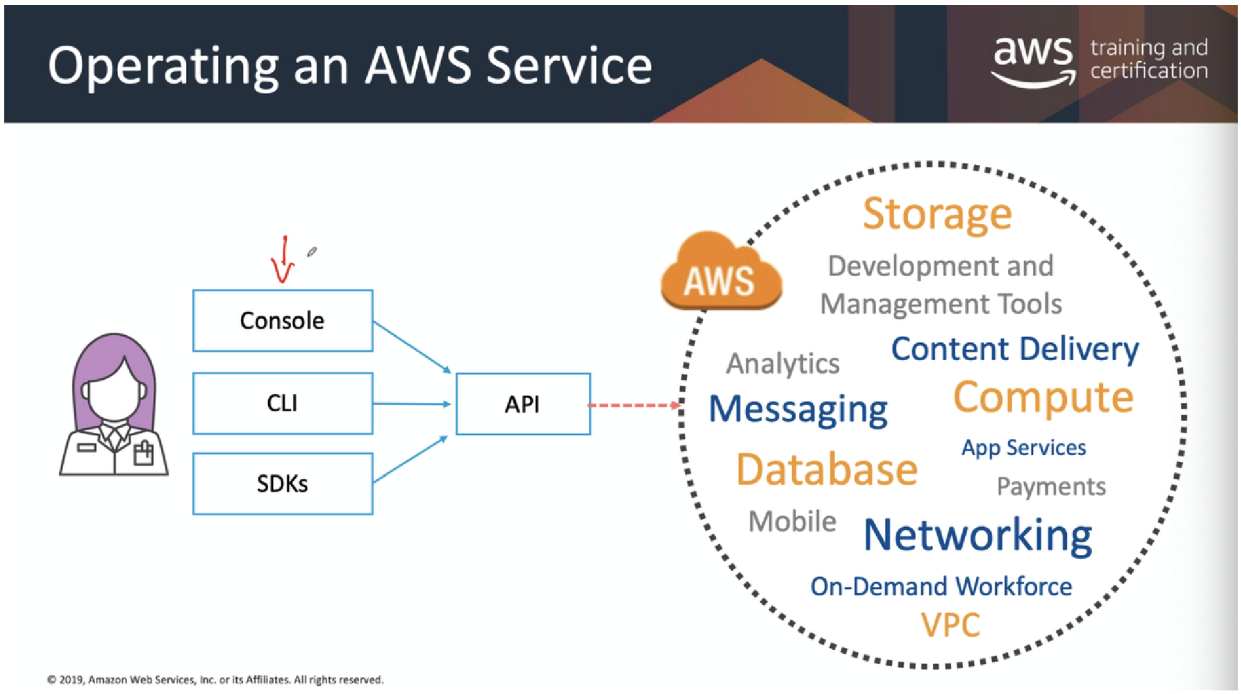


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

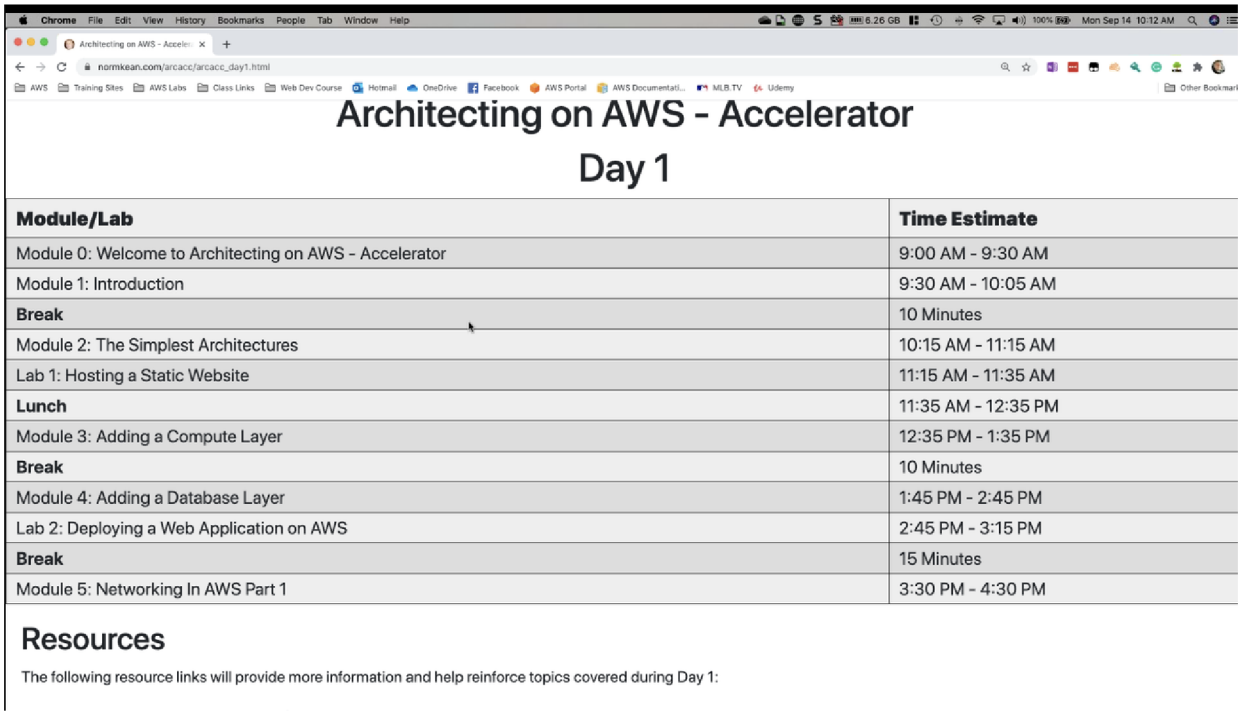




https://infrastructure.aws/
https://aws.amazon.com/about-aws/global-infrastructure/
Great video from re:invent 2016 on AWS global network: https://www.youtube.com/watch?v=uj7Ting6Ckk



end points are outside of regions, but do serve as caching points. They are there to push out contents to larger place



Architecting on AWS - Accelerator

Day 1

Module/Lab	Time Estimate
Module 0: Welcome to Architecting on AWS - Accelerator	9:00 AM - 9:30 AM
Module 1: Introduction	9:30 AM - 10:05 AM
Break	10 Minutes
Module 2: The Simplest Architectures	10:15 AM - 11:15 AM
Lab 1: Hosting a Static Website	11:15 AM - 11:35 AM
Lunch	11:35 AM - 12:35 PM
Module 3: Adding a Compute Layer	12:35 PM - 1:35 PM
Break	10 Minutes
Module 4: Adding a Database Layer	1:45 PM - 2:45 PM
Lab 2: Deploying a Web Application on AWS	2:45 PM - 3:15 PM
Break	15 Minutes
Module 5: Networking In AWS Part 1	3:30 PM - 4:30 PM

Resources

The following resource links will provide more information and help reinforce topics covered during Day 1:

Amazon S3 use case 1

aws training and certification

Storing and distributing static web content and media

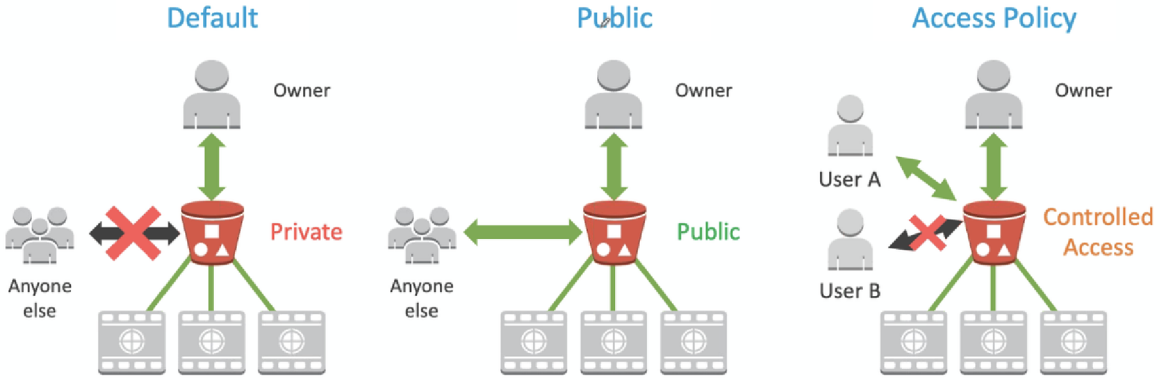
https://[BucketName].s3.[aws-region].amazonaws.com

https://[BucketName].s3.[aws-region].amazonaws.com/homepage.html

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon S3 access control - general

aws training and certification



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon S3 use case 2

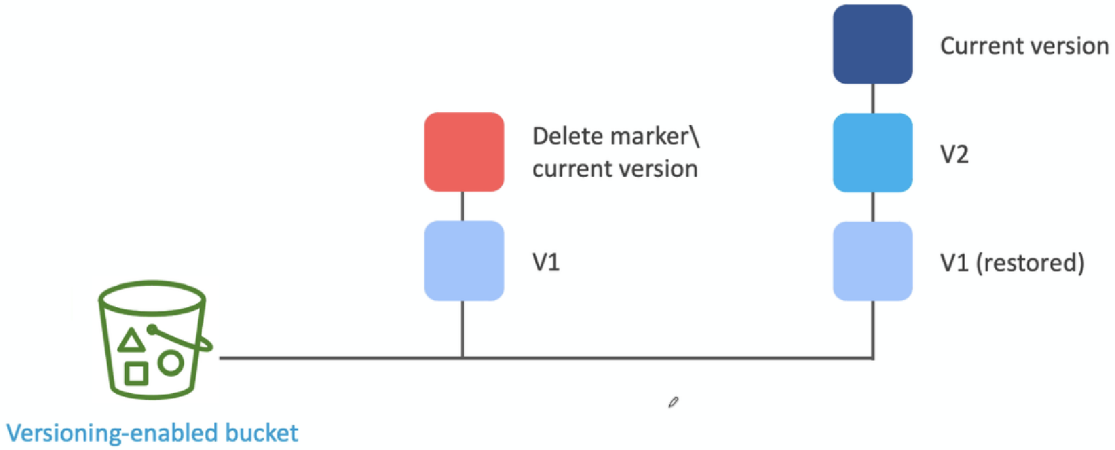
aws training and certification

Host entire static websites

HTML files, images, videos, and client-side scripts

Amazon S3 versioning

aws training and certification

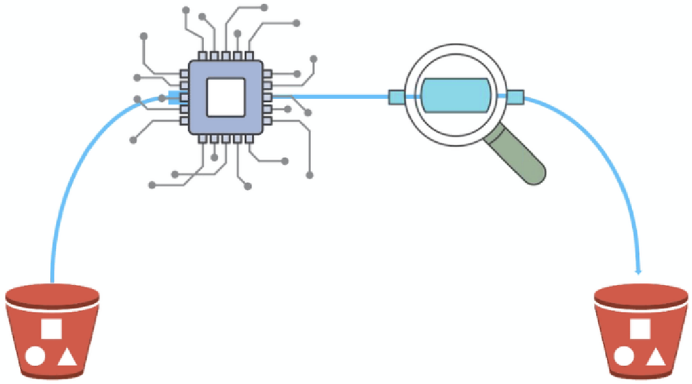


can't disable versioning. pay for each of the versions

Amazon S3 use case 3

aws training and certification

Data store for computation and large-scale analytics



Financial transaction analysis

Clickstream analytics

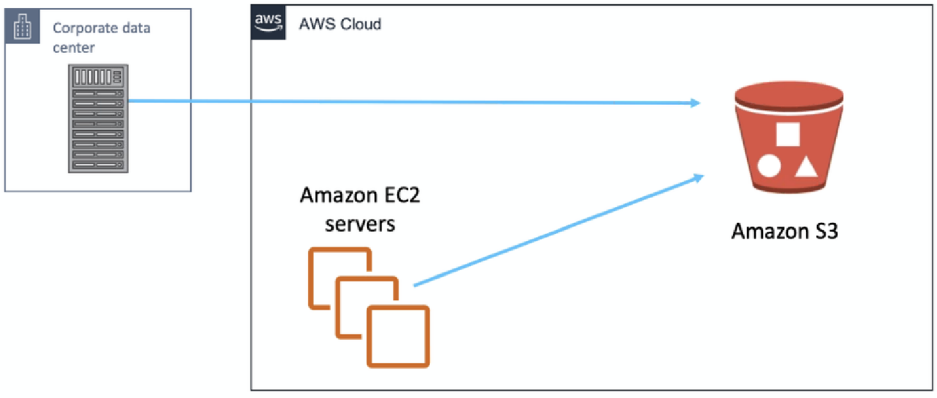
Media transcoding

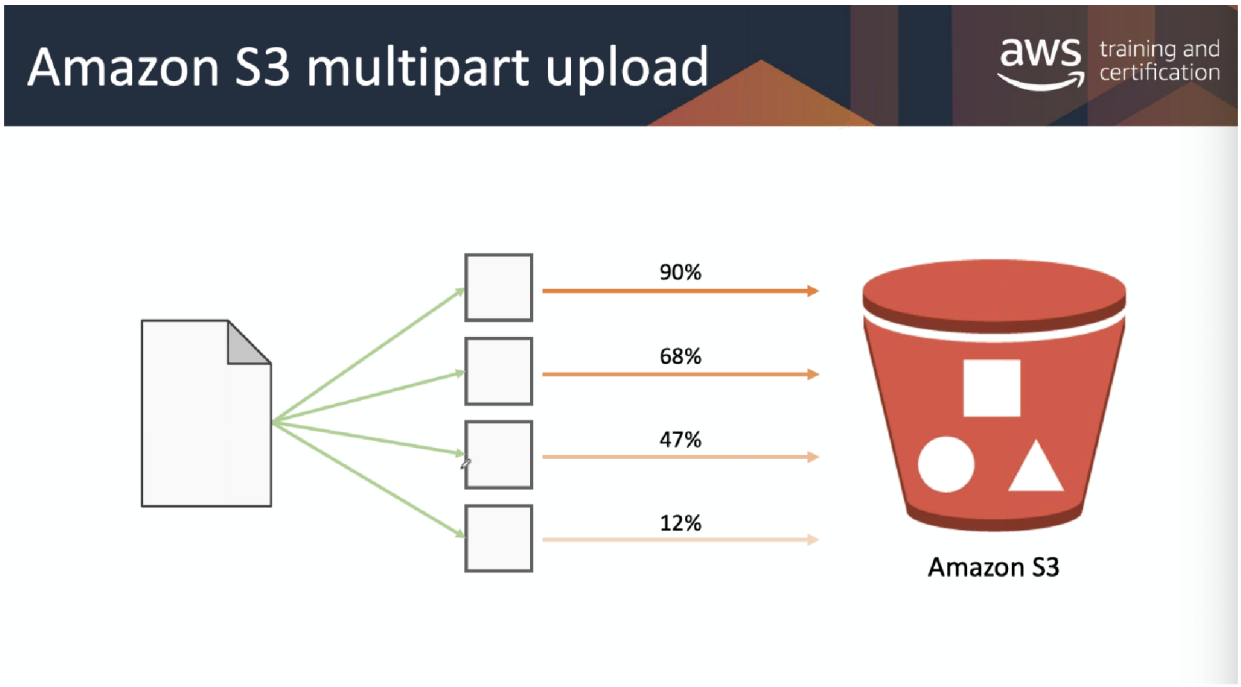
© 2019. Amazon Web Services. Inc. or its Affiliates. All rights reserved.

Amazon S3 use case 4

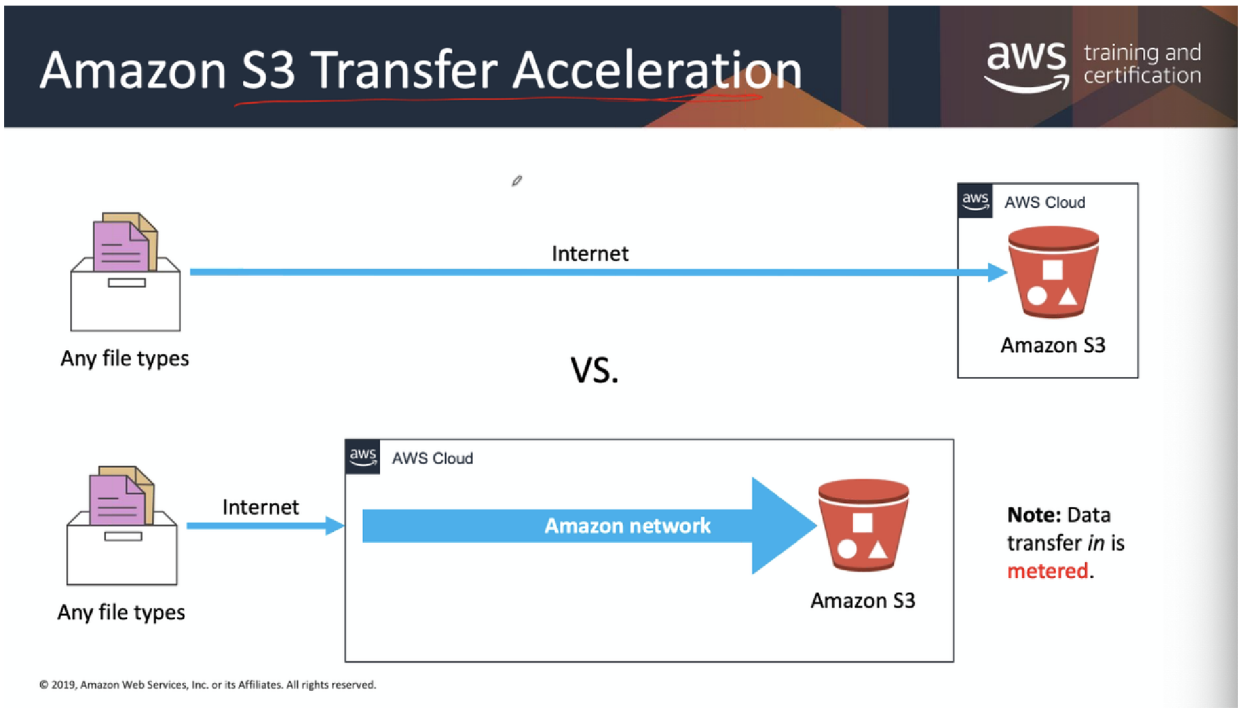
aws training and certification

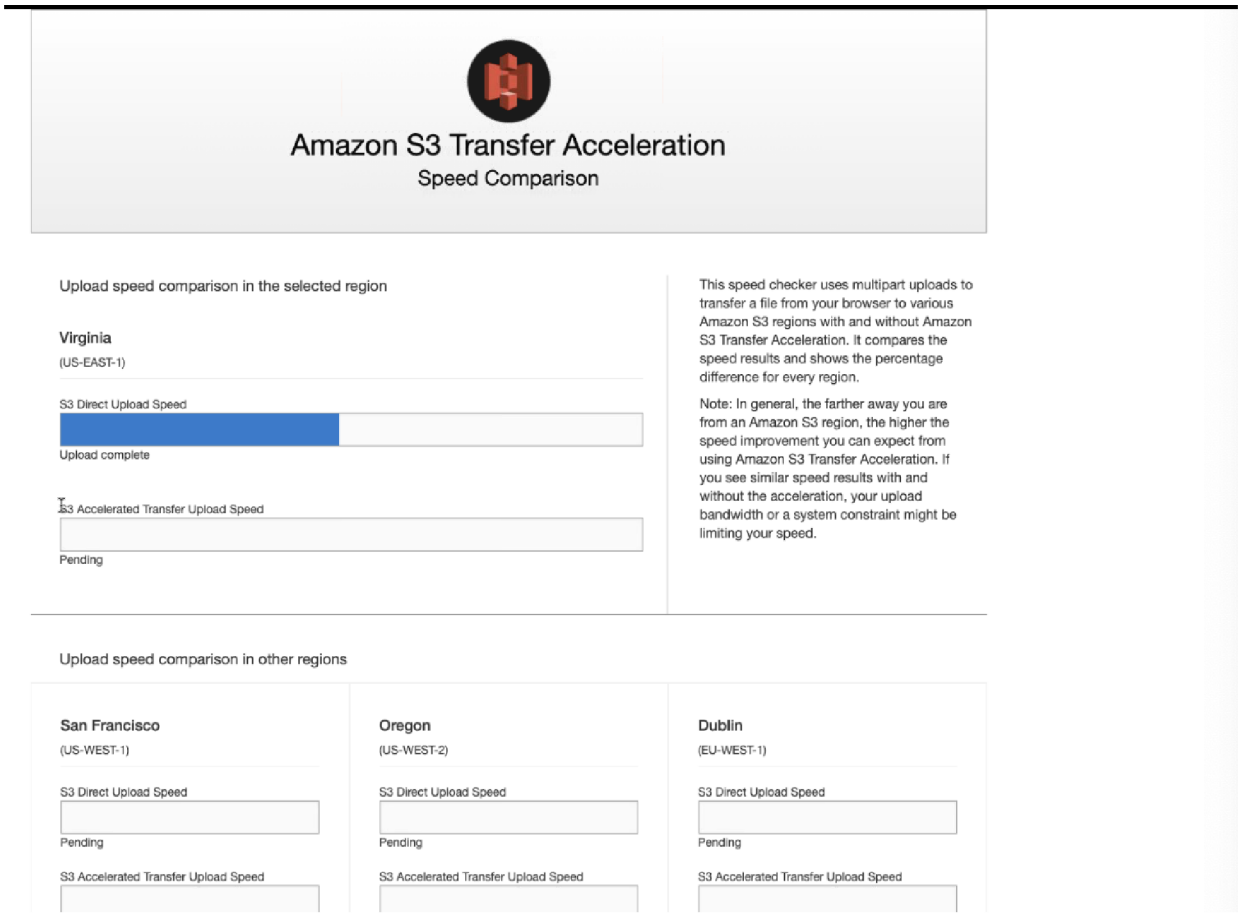
Backup tool



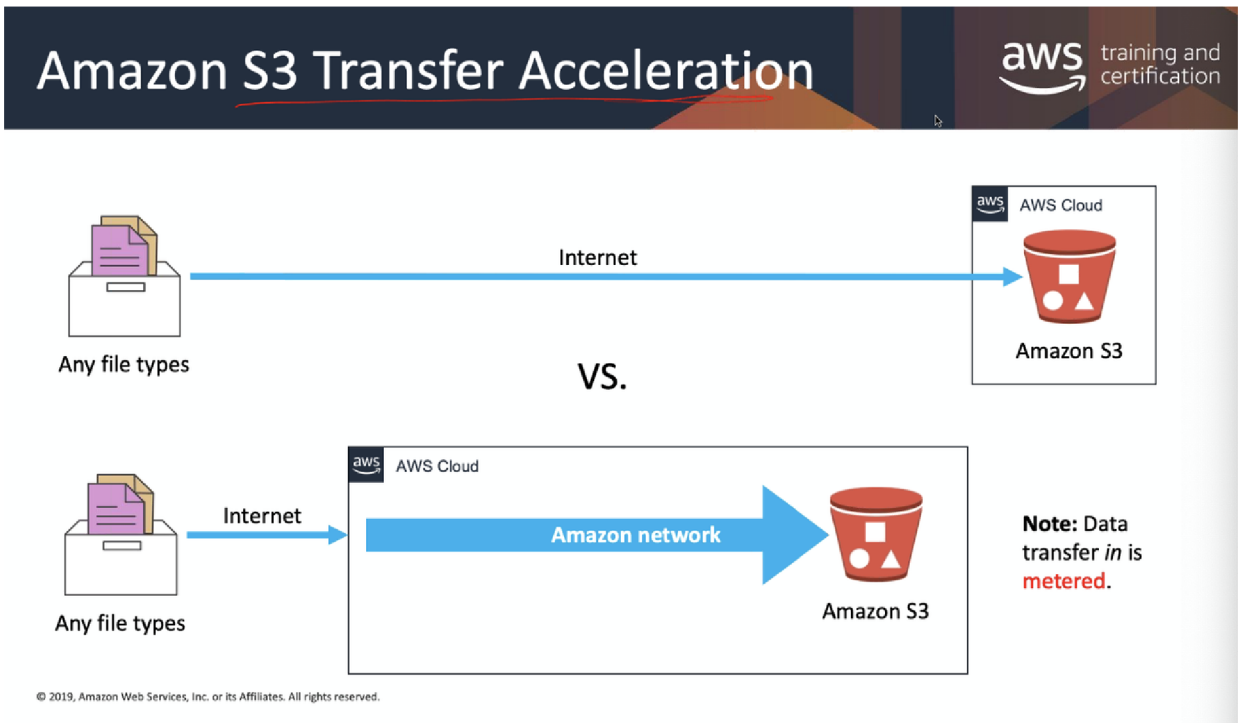


it will break down a large file into parts, then upload!! 5 terra byte per file is the limit!



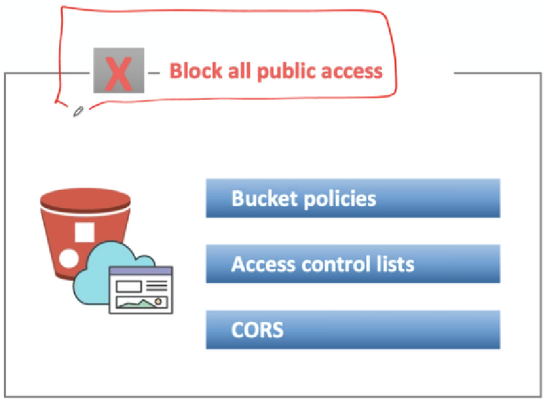


https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html



Securing your bucket completely

aws training and certification



Block public access to buckets and objects granted through any access control lists (ACLs)

Block public access to buckets and objects granted through *new* ACLs

Block public and cross-account access to buckets and objects through any public bucket policies

Block public access to buckets and objects granted through *new* public bucket policies

Moving large data into Amazon S3

aws

AWS Snowball

Petabyte-scale data transport

AWS Snowball

AWS Snowball Edge Optimized

AWS Snowmobile

Exabyte-scale data transport

AWS Snowmobile

Amazon S3 costs

aws training and certification

Pay only for what you use, including:

GBs per month

Transfer OUT to other Regions or the internet

PUT, COPY, POST, LIST, and GET requests

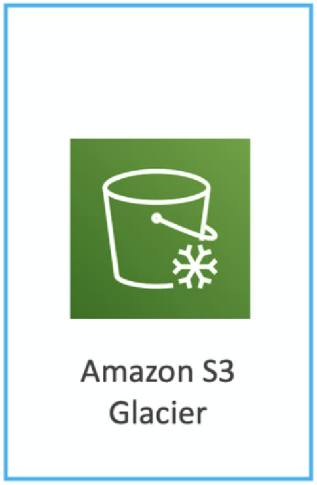
You do NOT have to pay for:

Transfer IN to Amazon S3

Transfer OUT to Amazon EC2 in the same Region, or to Amazon CloudFront

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon S3 Glacier



Long-term data storage

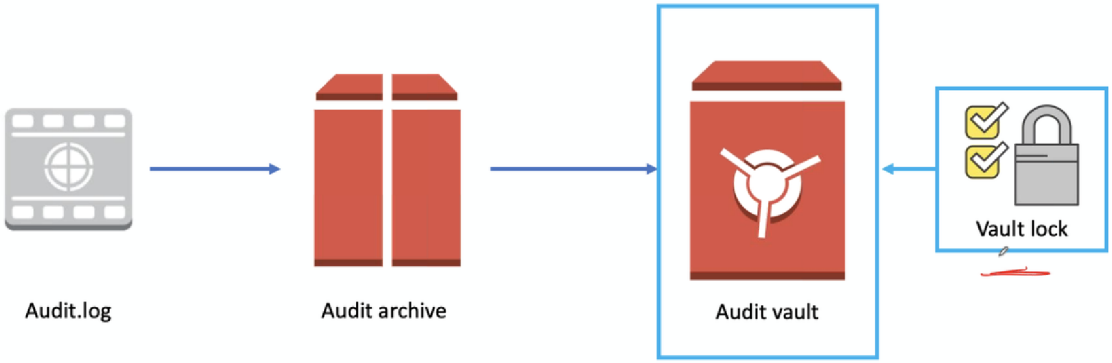
Archival or backup

Very low-cost storage

replacement to long term archive (tape??)

Amazon S3 Glacier archives and vaults

aws training and certification

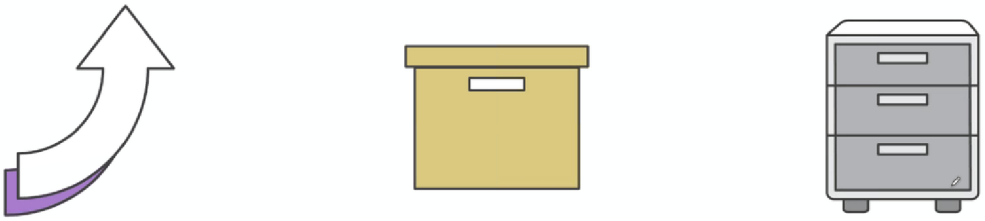


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Costs related to Amazon S3 Glacier

aws training and certification

Retrieving data from Amazon S3 Glacier

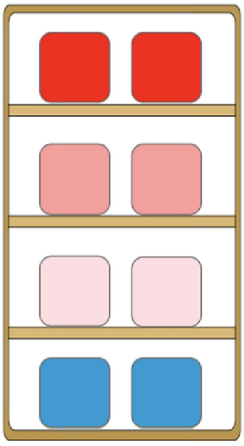


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Retrieval times: 1-5 min | 3-5 hr | 5 - 12 hrs

Amazon S3/Amazon S3 Glacier storage classes

aws training and certification



S3 Standard:
General purpose

S3 Standard IA:
Infrequent but rapid access

S3 One Zone IA:
Recreatable, infrequently accessed data

Amazon S3 Glacier/Deep Archive:
Archival data, cheapest available storage tier

Amazon S3 Intelligent Tiering

Automatically moves your objects between two access tiers of storage

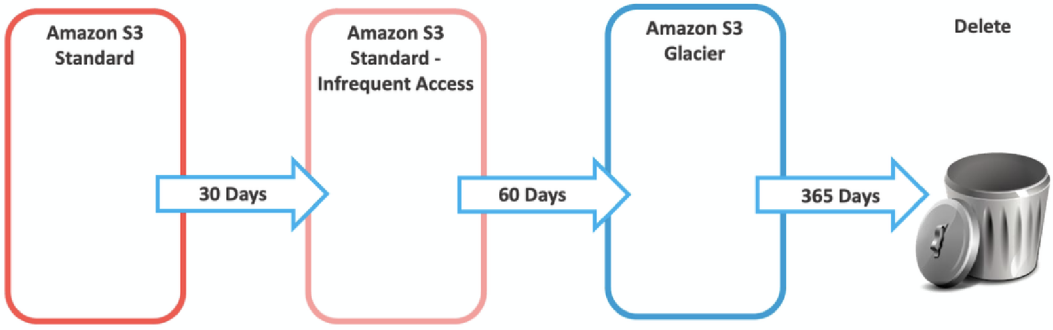
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

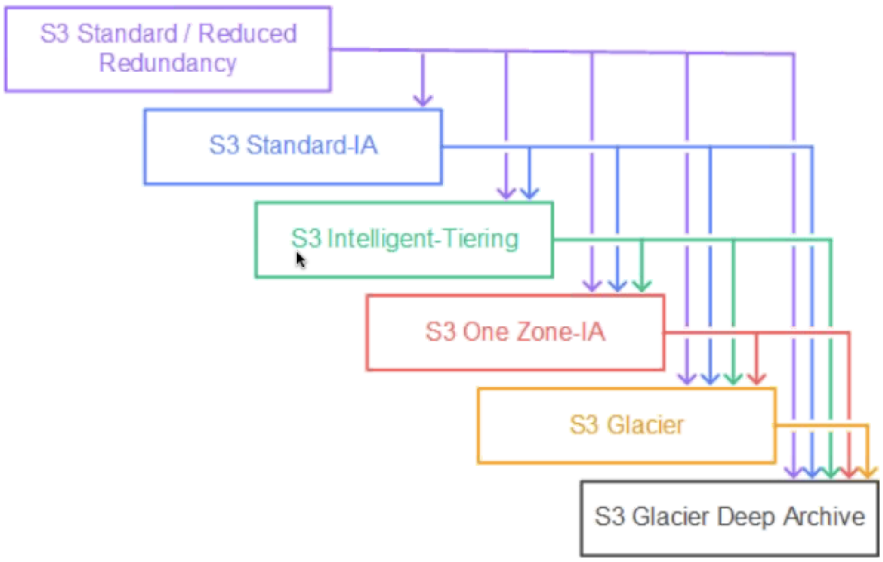
Lifecycle policies

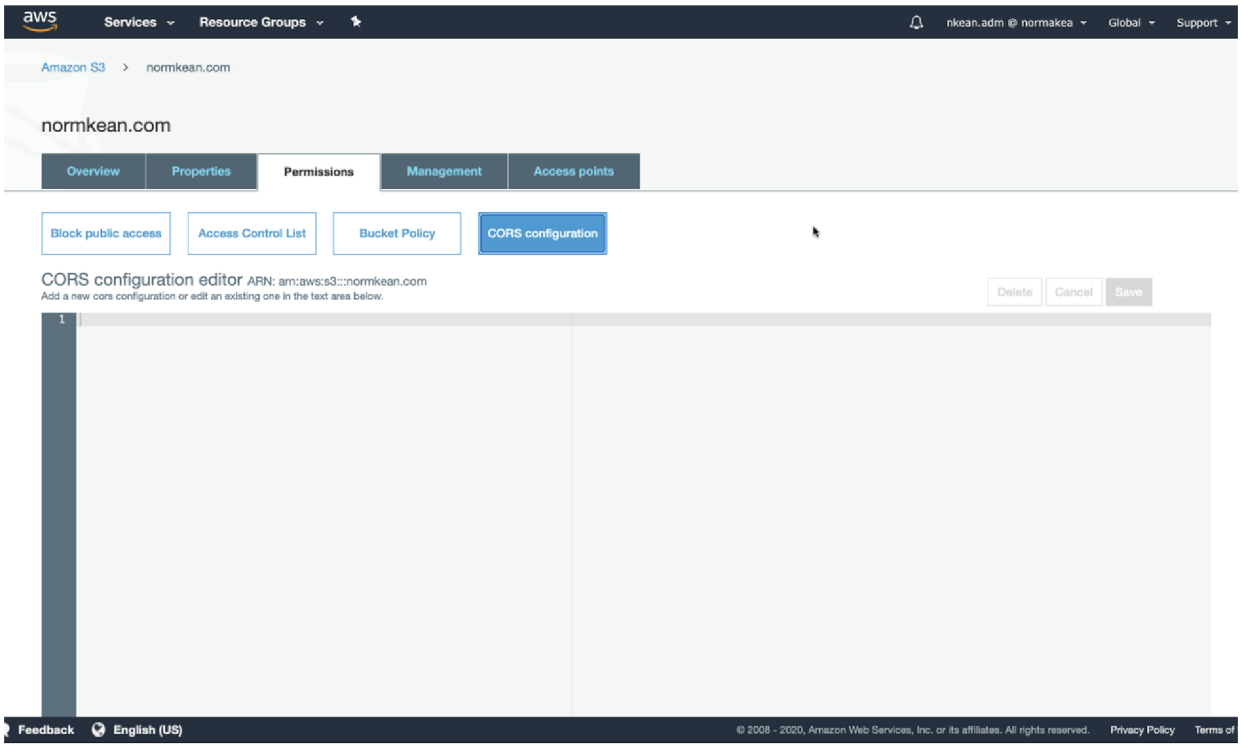
aws training and certification

Amazon S3 lifecycle policies allow you to delete or move objects based on age.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

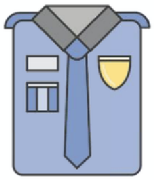




CORS: cross region resources sharing

Choosing a Region

Data residency and regulatory compliance



Are there relevant data privacy laws in the Region?

Can customer data be stored outside the country?

Can you meet you governance obligation?

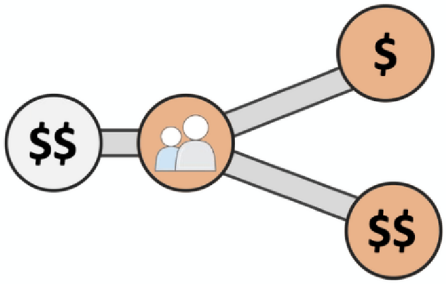
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Choosing a Region

Proximity of users to data

Small differences in latency can impact customer experience

Choose the Region closest to your users



Choosing a Region

aws training and certification

Cost-effectiveness

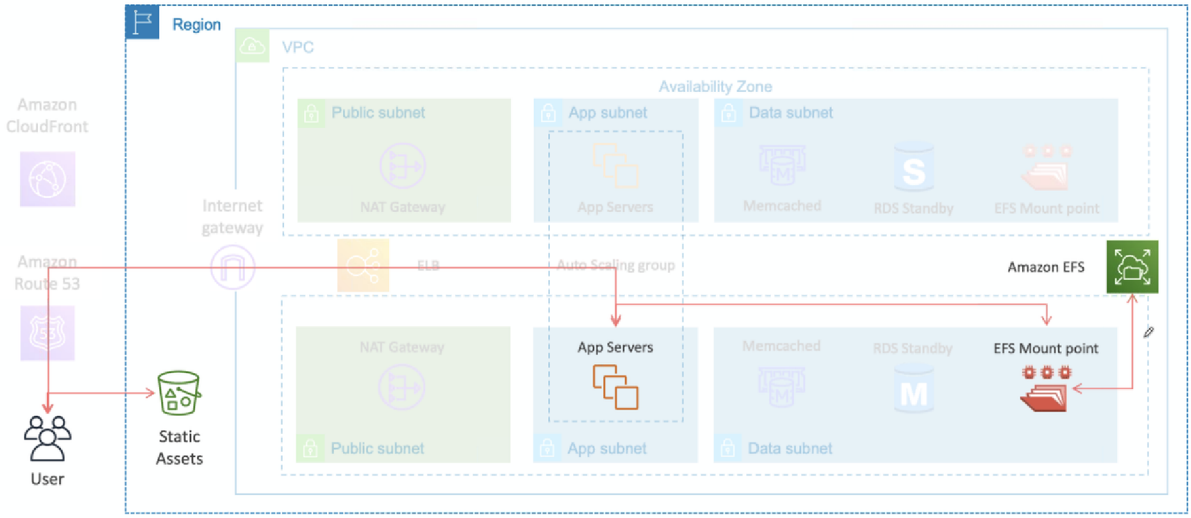
- Costs vary by AWS Region
- Some services like Amazon S3 have costs for transferring data out
- Consider the cost-effectiveness of replicating the entire environment in another Region

https://aws.qwiklabs.com/

Common Data Storage Measurements

UNIT	VALUE
bit	1 bit
byte	8 bits
kilobyte	1,024 bytes
megabyte	1,024 kilobytes
gigabyte	1,024 megabytes
terabyte	1,024 gigabytes
petabyte	1,024 terabytes
exabyte	1,024 petabytes
zettabyte	1,024 exabytes
yottabyte	1,024 zettabytes
brontobyte	1,024 yottabytes

Adding the compute layer



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 3

The architectural need

You need to run applications that are going to be used by a consistent but small number of users.

Module overview

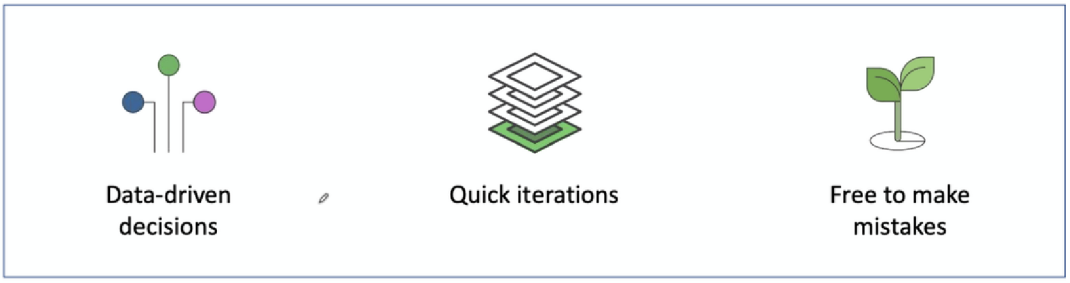
- Amazon Elastic Compute Cloud (Amazon EC2)
- Instance types and families
- Amazon Elastic Block Store (Amazon EBS) volumes
- Compliance options

Virtual machines vs. physical servers

aws training and certification

Amazon EC2 can solve some problems that are more difficult with an on-premises server.

When using disposable resources



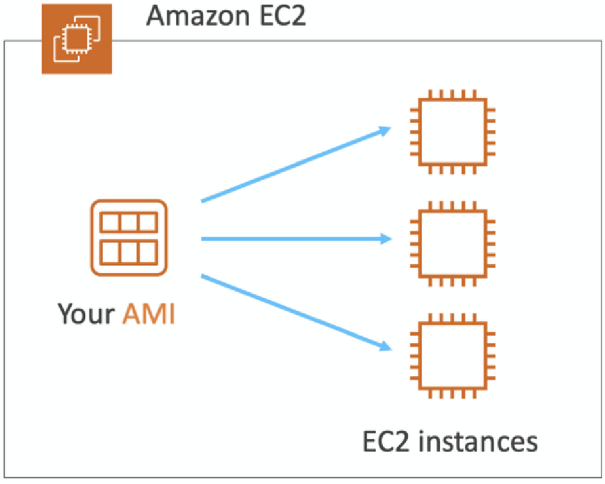
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon EC2 and AMIs

aws training and certification

AMIs include:

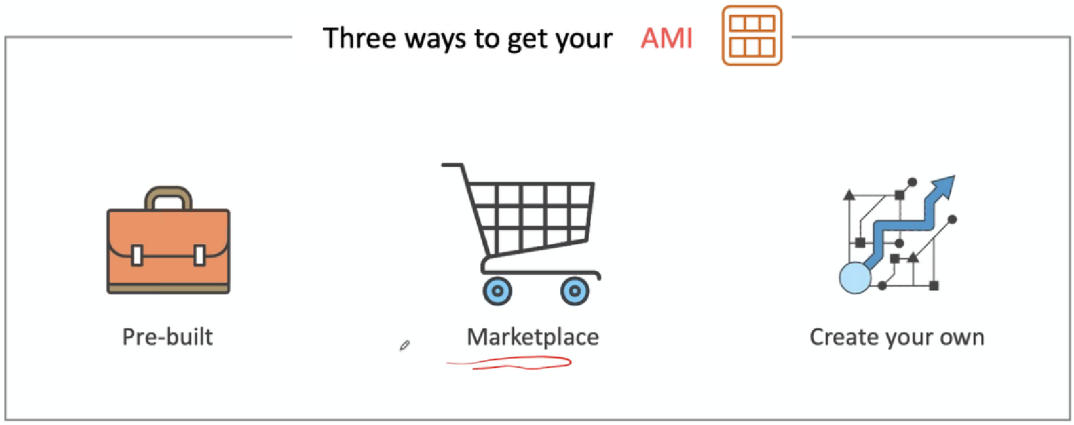
- A template for the root volume (copy of the boot drive)
- Launch permissions
- A block device mapping



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

boot drive: is it linux?

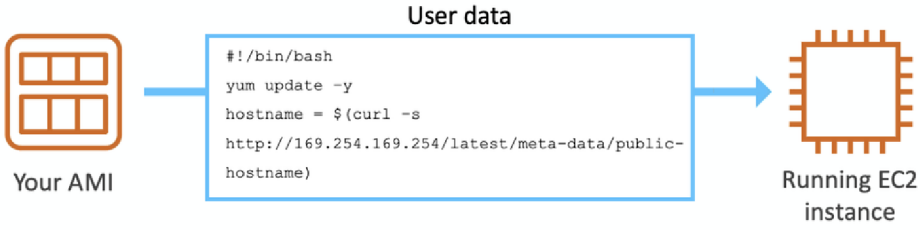
Where do you get an AMI?



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

An Amazon Machine Image is a special type of virtual appliance that is used to create a virtual machine within the Amazon Elastic Compute Cloud. It serves as the basic unit of deployment for services delivered using EC2.

Retrieving information about your EC2 instance with instance metadata



Metadata	Value
instance-id	i-1234567890abcdef0
mac	00-1B-63-84-45-E6
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.12

What needs can Amazon EBS address?

aws training and certification

Amazon Elastic Block Store (Amazon EBS) is an easy-to-use, high-performance block storage service designed for use with Amazon EC2.

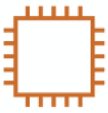
- Replicating within the Availability Zone, offering 99.999% availability
- Offers four different volume types at various price points and performance benchmarks
- Enables you to increase storage without any disruption to your critical workloads

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

What problems does Amazon EBS solve?

aws training and certification


Application needs block-level storage


Instance storage is ephemeral


Need data to persist through shutdowns


Need to be able to back up data volumes

Amazon EBS volume types

aws training and certification

Solid-state backed

Volume Type	General-Purpose SSD	Provisioned IOPS SSD
Description	General-purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads
Use Cases	• Recommended for most workloads 3 IOPS / GB	• Critical business applications that require sustained IOPS performance • Large database workloads

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

IOPS (input/output operations per second) is a popular performance metric used to distinguish one storage type from another. Similar to device makers, **AWS** associates **IOPS** values to the volume component backing the storage option. As **IOPS** values increase, performance needs and costs rise.

Amazon EBS volume types

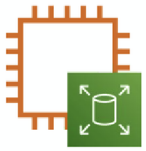
aws training and certification

Hard-disk backed

Volume Type	Throughput-Optimized HDD	Cold HDD
Description	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest-cost HDD volume designed for less frequently accessed workloads
Use Cases	• Streaming workloads • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Instances optimized for Amazon EBS



EBS Optimized Instance

- Optimized configuration stack
- Additional dedicated capacity for Amazon EBS I/O
- Minimizes contention between Amazon EBS and other traffic
- Options between 425 Mbps and 14,000 Mbps

Shared file systems

What if I have multiple instances that need to use the same storage?

Amazon EBS only attaches to one instance

Amazon S3 is an option but is not ideal

Amazon EFS and Amazon FSx are perfect for this task

Amazon EFS and Amazon FSx

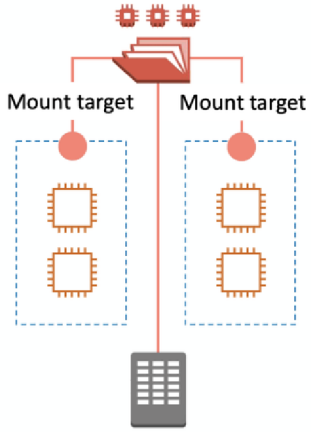
aws training and certification

Amazon EFS
(Linux workloads)
NFSv4 file system

Shared across:
- Availability Zones
- AWS Regions
- VPCs
- Account

Amazon FSx
(Windows workloads)
NTFS file system

Shared across:
- Availability Zones



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon Elastic File System (Amazon **EFS**) provides a simple, scalable, fully managed elastic NFS file system for use with **AWS** Cloud services and on-premises resources. ... Amazon **EFS** offers two storage classes: the Standard storage class, and the Infrequent Access storage class (**EFS** IA).

EC2 instances – What's in a name?

aws training and certification

m5.large

m is the family name

5 Is the generation number

large is the size of the instance

Examples

t3.large

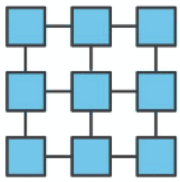
c5.xlarge

p3.2xlarge

EC2 instances – types

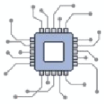
Choosing the correct type is very important for:

Efficient utilization of your instances



Reducing unneeded cost

EC2 instances – types



General purpose — 6 available selections

Compute optimized — 3 available selections

Memory optimized — 7 available selections

Accelerated computing — 4 available selections

Storage optimized — 3 available selections

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://aws.amazon.com/ec2/instance-types/

Intel® Xeon CPUs and EC2 instances

aws training and certification

All current EC2 instance types include:

- Intel AES-NI: Reduces performance hit due to encryption
- Intel AVX (AVX2, AVX-512): Improve floating-point performance. Only available on HVM deployments

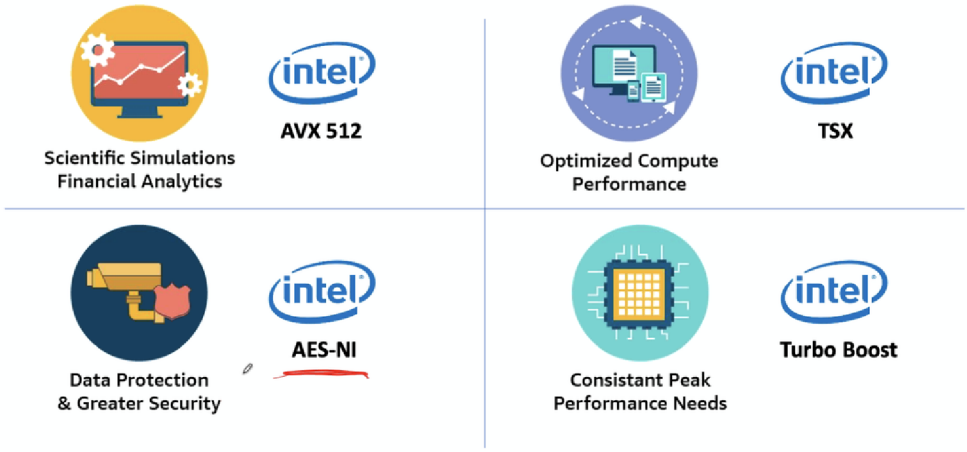
Some EC2 instance types include:

- Intel Turbo Boost: Runs cores faster than base clock speed when needed
- Intel TSX: Uses multiple threads or single thread depending on need
- P state and C state control: Fine-tune performance and sleep state of each core

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Intel® processors for your workloads

aws training and certification



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Intel® Xeon scalable processors

aws training and certification

Latest generation of Intel Xeon processors up to:

- 28 cores per CPU
- 6 memory channels
- 48 PCIe lanes of bandwidth/throughput
- 100 Gbps network bandwidth (C5n.16xlarge)

Intel AVX-512:

- Twice the floating-point performance of AVX2
- 512-bit instructions (vs 256 for AVX/AVX2)

EC2 pricing options

aws training and certification

On-demand instances

Reserved instances

Spot instances

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

On-Demand instances

- Pay for compute capacity per second (Amazon Linux and Ubuntu) or by the hour (all other OS)
- No long-term commitments
- No upfront payments
- Increase or decrease your compute capacity depending on the demands of your application

On-Demand instances

- Pay for compute capacity per second (Amazon Linux and Ubuntu) or by the hour (all other OS)
- No long-term commitments
- No upfront payments
- Increase or decrease your compute capacity depending on the demands of your application