

AWS Training

Topics

CONCEPTS AND COMPONENTS

SA Associate

A CLOUD GURU

The image displays a grid of orange rectangular boxes, each containing a different AWS service name. The services listed are:

- Desktop & App Streaming
- Application Integration
- Analytics
- Management Tools
- Migration
- Compute
- Networking & Content Delivery
- Storage
- Databases
- AWS Global Infrastructure

Activate Windows
Go to PC settings to activate Windows

Udemy

EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.

Amazon EC2 provides the following features:

- Virtual computing environments, known as **instances**
- Preconfigured templates for your instances, known as **Amazon Machine Images (AMIs)**, that package the bits you need for your server (including the operating system and additional software)
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as **instance types**
- Secure login information for your instances using **key pairs (AWS stores the public key, and you store the private key in a secure place)**
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as **instance store volumes**
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as **Amazon EBS volumes**
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as **regions and Availability Zones**
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your **instances using security groups**
- Static IPv4 addresses for dynamic cloud computing, known as **Elastic IP addresses**
- Metadata, known as **tags**, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as **virtual private clouds (VPCs)**
 - For more information about the features of Amazon EC2, see the Amazon EC2 product page.
 - For more information about running your website on AWS, see Web Hosting.

Setting Up with Amazon EC2

- Create an IAM User
 - Services in AWS, such as Amazon EC2, require that you provide credentials when you access them, so that the service can determine whether you have permission to access its resources. The console requires your password. You can create access keys for your AWS account to access the command line interface or API.
- Create a Key Pair
 - AWS uses public-key cryptography to secure the login information for your instance. A Linux instance has no password; you use a key pair to log in to your instance securely. You specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.
- Create a Virtual Private Cloud (VPC)
 - Amazon VPC enables you to launch AWS resources into a virtual network that you've defined.
- Create a Security Group
 - Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. You must add rules to a security group that enable you to connect to your instance from your IP address using SSH. You can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere.
 - **Note** that if you plan to launch instances in multiple regions, you'll need to create a security group in each region.

Best Practices for Amazon EC2

- Security and Network
 - Manage access to AWS resources and APIs using identity federation, IAM users, and IAM roles. Establish credential management policies and procedures for creating, distributing, rotating, and revoking AWS access credentials.
 - Implement the least permissive rules for your security group.
 - Regularly patch, update, and secure the operating system and applications on your instance.
 - Launch your instances into a VPC instead of EC2-Classic.
- Storage
 - Understand the implications of the root device type for data persistence, backup, and recovery.
 - Use separate Amazon EBS volumes for the operating system versus your data.
 - Use the instance store available for your instance to store temporary data. Remember that the data stored in instance store is deleted when you stop or terminate your instance.
- Resource Management
 - Use instance metadata and custom resource tags to track and identify your AWS resources.
 - View your current limits for Amazon EC2. Plan to request any limit increases in advance of the time that you'll need them.
- Backup and Recovery
 - Regularly back up your EBS volumes using Amazon EBS snapshots (p. 783), and create an Amazon Machine Image from your instance to save the configuration as a template for launching future instances.
 - Deploy critical components of your application across multiple Availability Zones, and replicate your data appropriately.
 - Design your applications to handle dynamic IP addressing when your instance restarts.
 - Monitor and respond to events
 - Ensure that you are prepared to handle failover. For a basic solution, you can manually attach a network interface or Elastic IP address to a replacement instance
 - Regularly test the process of recovering your instances and Amazon EBS volumes if they fail.

Increase the Availability of Application EC2

- Prerequisites (p. 74)
 - Created a virtual private cloud (VPC) with one public subnet in two or more Availability Zones.
 - Launched an instance in the VPC.
 - Connected to the instance and customized it. For example, installing software and applications, copying data, and attaching additional EBS volumes.
 - Tested your application on your instance to ensure that your instance is configured correctly.
 - Created a custom Amazon Machine Image (AMI) from your instance.
 - (Optional) Terminated the instance if you no longer need it.
 - Created an IAM role that grants your application the access to AWS it needs.
- Scale and Load Balance Your Application
 - Create a load balancer, Create a launch configuration for your instances, Create an Auto Scaling group with two or more instances, and associate the load balancer with the Auto Scaling group.
- Test Your Load Balancer
 - Verify that your instances are ready. From the Auto Scaling Groups page, select your Auto Scaling group, and then choose the Instances tab. Initially, your instances are in the Pending state. When their states are InService
 - Verify that your instances are registered with the load balancer. From the Target Groups page, select your target group, and then choose the Targets tab. If the state of your instances is initial, it's possible that they are still registering. When the state of your instances is healthy
 - From the Load Balancers page, select your load balancer.
 - On the Description tab, locate the DNS name
 - In a web browser, paste the DNS name for the load balancer into the address bar and press Enter. You'll see your website displayed.

Amazon Machine Images (AMI)

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it's launched
- AMI Types
 - You can select an AMI to use based on the following characteristics:
 - Region (see Regions and Availability Zones)
 - Operating system • Architecture (32-bit or 64-bit)
 - Launch Permissions
 - public The owner grants launch permissions to all AWS accounts.
 - explicit The owner grants launch permissions to specific AWS accounts.
 - implicit The owner has implicit launch permissions for an AMI.
- Storage for the Root Device

EC2

EC2 101

What Is EC2?



A CLOUD GURU



Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

Activate Windows
Go to PC settings to activate Windows.

Options

EC2 101

EC2 Options



A CLOUD GURU

- **On Demand** - allows you to pay a fixed rate by the hour (or by the second) with no commitment.
- **Reserved** - provides you with a capacity reservation, and offer a significant discount on the hourly charge for an instance.1 Year or 3 Year Terms
- **Spot** - enables you to bid whatever price you want for instance capacity, providing for even greater savings if your applications have flexible start and end times.
- **Dedicated Hosts** - 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.

Activate Windows
Go to PC settings to activate Windows.

On Demand

EC2 101

On Demand



A CLOUD GURU

- Perfect for users that want 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



Reserved

EC2 101

Reserved Instances



A CLOUD GURU

- Applications with steady state or predictable usage
- Applications that require reserved capacity
- Users can make up-front payments to reduce their total computing costs even further
 - Standard RIs (Up to 75% off on-demand)
 - Convertible RIs (Up to 54% off on-demand) feature the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value.
 - Scheduled RIs are available to launch within the time window you reserve. This option allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month.



RESERVED

Activate Windows
Go to PC settings to activate Windows.

Spot

EC2 101

Spot Instances



A CLOUD GURU

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



Dedicated

EC2 101

Dedicated Hosts



- Useful for regulatory requirements that may not support multi-tenant virtualization.
- Great for licensing which does not support multi-tenancy or cloud deployments.
- Can be purchased On-Demand (hourly.)
- Can be purchased as a Reservation for up to 70% off the On-Demand price.



Instance Types

EC2 101

EC2 Instance Types



Family	Speciality	Use case
F1	Field Programmable Gate Array	Genomics research, financial analytics, real-time video processing, big data etc
I3	High Speed Storage	NoSQL DBs, Data Warehousing etc
G3	Graphics Intensive	Video Encoding/ 3D Application Streaming
H1	High Disk Throughput	MapReduce-based workloads, distributed file systems such as HDFS and MapR-FS
T2	Lowest Cost, General Purpose	Web Servers/Small DBs
D2	Dense Storage	File servers/Data Warehousing/Hadoop
R4	Memory Optimized	Memory Intensive Apps/DBs
M5	General Purpose	Application Servers
C5	Compute Optimized	CPU Intensive Apps/DBs
P3	Graphics/General Purpose GPU	Machine Learning, Bit Coin Mining etc
X1	Memory Optimized	SAP HANA/Apache Spark etc

Activate Windows
Go to PC settings to activate Windows.



Instances Types

EC2 101

EC2 Instance Types

- How I remember them now;
- **F** for FPGA
- **I** for IOPS
- **G** - Graphics
- **H** - High Disk Throughput
- **T** cheap general purpose (think T2 Micro)
- **D** for Density
- **R** for RAM
- **M** - main choice for general purpose apps
- **C** for Compute
- **P** - Graphics (think Pics)
- **X** - Extreme Memory



A CLOUD GURU



Activate Windows
Go to PC settings to activate Windows.

Udemy

EBS

EC2 101

What is EBS?



A CLOUD GURU

Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. Amazon EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.



EBS Volume Types



- General Purpose SSD (GP2)
 - General purpose, balances both price and performance.
 - Ratio of 3 IOPS per GB with up to 10,000 IOPS and the ability to burst up to 3000 IOPS for extended periods of time for volumes at 3334 GiB and above.
- Provisioned IOPS SSD (IO1)
 - Designed for I/O intensive applications such as large relational or NoSQL databases.
 - Use if you need more than 10,000 IOPS.
 - Can provision up to 20,000 IOPS per volume.



Volume Types

EC2 101

EBS Volume Types



A CLOUD GURU

- Throughput Optimized HDD (ST1)
 - Big data
 - Data warehouses
 - Log processing
 - Cannot be a boot volume
- Cold HDD (SC1)
 - Lowest Cost Storage for infrequently accessed workloads
 - File Server
 - Cannot be a boot volume.
- Magnetic (Standard)
 - Lowest cost per gigabyte of all EBS volume types that is bootable. Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.

Summary

EC2 101

EC2 Exam Tips



A CLOUD GURU

SSD

General Purpose SSD - balances price and performance for a wide variety of workloads.

Provisioned IOPS SSD - Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads

Magnetic

Throughput Optimized HDD - Low cost HDD volume designed for frequently accessed, throughput-intensive workloads

Cold HDD - Lowest cost HDD volume designed for less frequently accessed workloads

Magnetic - Previous Generation. Can be a boot volume.

Activate Windows
Go to PC settings to activate Windows.

Summary

EC2 - Lab

Lab Summary



A CLOUD GURU

- Termination Protection is turned off by default, you must turn it on.
- On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated.
- EBS Root Volumes of your DEFAULT AMI's cannot be encrypted. You can also use a third party tool (such as bit locker etc) to encrypt the root volume, or this can be done when creating AMI's (lab to follow) in the AWS console or using the API.
- Additional volumes can be encrypted.

Activate Windows
Go to PC settings to activate Windows.

udemy

Security Groups

Security Groups & EC2

Security Group Lab



A CLOUD GURU

- All Inbound Traffic is Blocked By Default
- All Outbound Traffic is Allowed
- Changes to Security Groups take effect immediately
- You can have any number of EC2 instances within a security group.
- You can have multiple security groups attached to EC2 Instances
- Security Groups are **STATEFUL**.
 - If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again.
- You cannot block specific IP addresses using Security Groups, instead use Network Access Control Lists.
- You can specify allow rules, but not deny rules.

Activate Windows
Go to PC settings to activate Windows.

udemy

Volume & Snapshots

Volume vs Snapshot Lab

Volumes & Snapshots



A CLOUD GURU

- Volumes exist on EBS:
 - Virtual Hard Disk
- Snapshots exist on S3.
- Snapshots are point in time copies of Volumes.
- Snapshots are incremental – this means that only the blocks that have changed since your last snapshot are moved to S3.
- If this is your first snapshot, it may take some time to create.

Activate Windows
Go to PC settings to activate Windows.



Snapshots

Volume vs Snapshot Lab

Snapshots of Root Device Volumes



- To create a snapshot for Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.
- However you can take a snap while the instance is running.
- You can create AMI's from EBS-backed Instances and Snapshots.
- You can change EBS volume sizes on the fly, including changing the size and storage type.
- Volumes will ALWAYS be in the same availability zone as the EC2 instance.
- To move an EC2 volume from one AZ/Region to another, take a snap or an image of it, then copy it to the new AZ/Region

Activate Windows
Go to PC settings to activate Windows.

RAID

RAID, Volumes & Snapshots

RAID, Volumes & Snapshots



A CLOUD GURU

- RAID = Redundant Array of Independent Disks
 - RAID 0 - Striped, No Redundancy, Good Performance
 - RAID 1 - Mirrored, Redundancy
 - RAID 5 - Good for reads, bad for writes, AWS does not recommend ever putting RAID 5's on EBS
 - RAID 10 - Striped & Mirrored, Good Redundancy, Good Performance.

Activate Windows
Go to PC settings to activate Windows.

udemy

AMI

AMI Types

You can select your AMI based on;



A CLOUD GURU

- Region (see Regions and Availability Zones)
- Operating system
- Architecture (32-bit or 64-bit)
- Launch Permissions
- Storage for the Root Device (Root Device Volume)
 - Instance Store (EPHEMERAL STORAGE)
 - EBS Backed Volumes

Activate Windows
Go to PC settings to activate Windows.

udemy

EBS vs Instance Store

AMI Types

EBS vs Instance Store



A CLOUD GURU

All AMIs are categorized as either backed by Amazon EBS or backed by instance store.

For EBS Volumes: The root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot.

For Instance Store Volumes: The root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

AMI Types

EBS vs Instance Store - Exam Tips



- Instance Store Volumes are sometimes called Ephemeral Storage.
- Instance store volumes cannot be stopped. If the underlying host fails, you will lose your data.
- EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped.
- You can reboot both, you will not lose your data.
- By default, both ROOT volumes will be deleted on termination, however with EBS volumes, you can tell AWS to keep the root device volume.

Activate Windows
Go to PC settings to activate Windows.

udemy

Load Balancers

ELASTIC LOAD BALANCERS

Types Of Load Balancers

- Application Load Balancer
- Network Load Balancer
- Classic Load Balancer



A CLOUD GURU



Activate Windows
Go to PC settings to activate Windows.

Application LB

ELASTIC LOAD BALANCERS

Application Load Balancers



A CLOUD GURU

Application Load Balancers are best suited for load balancing of HTTP and HTTPS traffic. They operate at Layer 7 and are application-aware. They are intelligent, and you can create advanced request routing, sending specified requests to specific web servers.



Network LB

ELASTIC LOAD BALANCERS

Network Load Balancer



A CLOUD GURU

Network Load Balancers are best suited for load balancing of TCP traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer are capable of handling millions of requests per second, while maintaining ultra-low latencies.

Use for extreme performance!



Classic LB

ELASTIC LOAD BALANCERS

Classic Load Balancers



A CLOUD GURU

Classic Load Balancers are the legacy Elastic Load Balancers. You can load balance HTTP/HTTPS applications and use Layer 7-specific features, such as X-Forwarded and sticky sessions. You can also use strict Layer 4 load balancing for applications that rely purely on the TCP protocol.



LB Errors

ELASTIC LOAD BALANCERS

Load Balancer Errors



A CLOUD GURU

Classic Load Balancers - if your application stops responding, the ELB (Classic Load Balancer) responds with a 504 error.

This means that the application is having issues. This could be either at the Web Server layer or at the Database Layer.

Identify where the application is failing, and scale it up or out where possible.



Activate Windows
Go to PC settings to activate Windows.



Summary

ELASTIC LOAD BALANCERS

ELB Exam Tips

A CLOUD GURU

- 3 Types of Load Balancers;
 - Application Load Balancers
 - Network Load Balancers
 - Classic Load Balancers
- 504 Error means the gateway has timed out. This means that the application not responding within the idle timeout period.
 - Trouble shoot the application. Is it the Web Server or Database Server?
- If you need the IPv4 address of your end user, look for the X-Forwarded-For header.

Activate Windows
Go to PC settings to activate Windows.

Summary

Elastic Load Balancers Lab

Elastic Load Balancers



A CLOUD GURU

- Instances monitored by ELB are reported as ; InService , or OutofService
- Health Checks check the instance health by talking to it
- Have their own DNS name. You are never given an IP address.
- Read the ELB FAQ for Classic Load Balancers
- Want to deep dive on application load balancers? Check out our deep dive course!

Activate Windows
Go to PC settings to activate Windows.

Cloudwatch

CloudWatch Lab

What can I do with Cloudwatch?



A CLOUD GURU

- Dashboards - Creates awesome dashboards to see what is happening with your AWS environment.
- Alarms - Allows you to set Alarms that notify you when particular thresholds are hit.
- Events - CloudWatch Events helps you to respond to state changes in your AWS resources.
- Logs - CloudWatch Logs helps you to aggregate, monitor, and store logs.

Activate Windows
Go to PC settings to activate Windows.

udemy

Meta Data

```
[root@ip-172-31-36-83 ec2-user]# curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/[root@ip-172-31-36-83 ec2-user]# █
```

Activate Windows
Go to PC settings to activate Windows.



Placement

EC2 Placement Groups

What is a Placement Group?



A CLOUD GURU

Two Types of Placement Groups;

- Clustered Placement Group
- Spread Placement Group

Activate Windows
Go to PC settings to activate Windows.



Clustered Placement

EC2 Placement Groups

Clustered Placement Group



A CLOUD GURU

A cluster placement group is a grouping of instances within a single Availability Zone. Placement groups are recommended for applications that need low network latency, high network throughput, or both.

Only certain instances can be launched into a Clustered Placement Group.



Spread Placement

EC2 Placement Groups

Spread Placement Group

A spread placement group is a group of instances that are each placed on distinct underlying hardware.

Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other.



EC2 Placement

EC2 Placement Groups

EC2 Placement Groups



A CLOUD GURU

- A clustered placement group can't span multiple Availability Zones.
- A spread placement group can.
- The name you specify for a placement group must be unique within your AWS account.
- Only certain types of instances can be launched in a placement group (Compute Optimized, GPU, Memory Optimized, Storage Optimized)
- AWS recommend homogenous instances within placement groups.
- You can't merge placement groups.
- You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group.

Activate Windows
Go to PC settings to activate Windows.

EFS

EFS Lab

What is EFS



A CLOUD GURU

Amazon Elastic File System (Amazon EFS) is a file storage service for Amazon Elastic Compute Cloud (Amazon EC2) instances. Amazon EFS is easy to use and provides a simple interface that allows you to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it.

Activate Windows
Go to PC settings to activate Windows.

udemy

EFS Features

EFS Lab

EFS Features



A CLOUD GURU

- Supports the Network File System version 4 (NFSv4) protocol
- You only pay for the storage you use (no pre-provisioning required)
- Can scale up to the petabytes
- Can support thousands of concurrent NFS connections
- Data is stored across multiple AZ's within a region
- Read After Write Consistency

Activate Windows
Go to PC settings to activate Windows.

udemy

Lambda

Lambda

What Is Lambda?



A CLOUD GURU

- Data Centres
- Hardware
- Assembly Code/Protocols
- High Level Languages
- Operating Systems
- Application Layer/AWS APIs
- AWS Lambda

Activate Windows
Go to PC settings to activate Windows.

 Udemy

Lambda

Lambda

What Is Lambda?



A CLOUD GURU

AWS Lambda is a compute service where you can upload your code and create a Lambda function. AWS Lambda takes care of provisioning and managing the servers that you use to run the code. You don't have to worry about operating systems, patching, scaling, etc. You can use Lambda in the following ways.

- As an event-driven compute service where AWS Lambda runs your code in response to events. These events could be changes to data in an Amazon S3 bucket or an Amazon DynamoDB table.
- As a compute service to run your code in response to HTTP requests using Amazon API Gateway or API calls made using AWS SDKs. This is what we use at A Cloud Guru.

Activate Windows
Go to PC settings to activate Windows.



Priced

Lambda

How Is Lambda Priced?



- Number of requests
 - First 1 million requests are free. \$0.20 per 1 million requests thereafter.
- Duration
 - Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms. The price depends on the amount of memory you allocate to your function. You are charged \$0.00001667 for every GB-second used.

Activate Windows
Go to PC settings to activate Windows.

Lambda Cool

Lambda

Why Is Lambda Cool?



- NO SERVERS!
- Continuous Scaling
- Super super super cheap!

Activate Windows
Go to PC settings to activate Windows.

Summary

Lambda

Lambda - Exam Tips



- Lambda scales out (not up) automatically
- Lambda functions are independent, 1 event = 1 function
- Lambda is serverless
- Know what services are serverless!
- Lambda functions can trigger other lambda functions, 1 event can = x functions if functions trigger other functions
- Architectures can get extremely complicated, AWS X-ray allows you to debug what is happening
- Lambda can do things globally, you can use it to back up S3 buckets to other S3 buckets etc
- Know your triggers

Activate Windows
Go to PC settings to activate Windows.

Exam Tips EBS



- EBS Consists of:
 - SSD, General Purpose - GP2 - (Up to 10,000 IOPS)
 - SSD, Provisioned IOPS - IO1 - (More than 10,000 IOPS)
 - HDD, Throughput Optimized - ST1 - frequently accessed workloads
 - HDD, Cold - SC1 - less frequently accessed data.
 - HDD, Magnetic - Standard - cheap, infrequently accessed storage
- You cannot mount 1 EBS volume to multiple EC2 instances; instead use EFS.

Volumes vs Snapshots



- Volumes exist on EBS:
 - Virtual Hard Disk
- Snapshots exist on S3.
- You can take a snapshot of a volume, this will store that volume on S3.
- Snapshots are point in time copies of Volumes.
- Snapshots are incremental. This means that only the blocks that have changed since your last snapshot are moved to S3.
- If this is your first snapshot, it may take some time to create.

Activate Windows
Go to PC settings to activate Windows.

EBS vs Instance Store - Exam Tips



- Instance Store Volumes are sometimes called Ephemeral Storage.
- Instance store volumes cannot be stopped. If the underlying host fails, you will lose your data.
- EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped.
- You can reboot both, you will not lose your data.
- By default, both ROOT volumes will be deleted on termination. However, with EBS volumes, you can tell AWS to keep the root device volume.

Activate Windows
Go to PC settings to activate Windows.

How can I take a Snapshot of a RAID Array?



- Stop the application from writing to disk.
- Flush all caches to the disk.

- How can we do this?
 - Freeze the file system
 - Unmount the RAID Array
 - Shutting down the associated EC2 instance.

DNS Route 53

DNS 101

What is DNS?



A CLOUD GURU

If you've used the internet, you've used DNS. DNS is used to convert human friendly domain names (such as <http://acloud.guru>) into an Internet Protocol (IP) address (such as <http://82.124.53.1>).

IP addresses are used by computers to identify each other on the network. IP addresses commonly come in 2 different forms, IPv4 and IPv6.

Activate Windows
Go to PC settings to activate Windows.

udemy

IP4 vs IP6

DNS 101

IPv4 vs IPv6



A CLOUD GURU

The IPv4 space is a 32 bit field and has over 4 billion different addresses (4,294,967,296 to be precise).

IPv6 was created to solve this depletion issue and has an address space of 128bits which in theory is

340,282,366,920,938,463,463,374,607,431,768,211,456 addresses

or 340 undecillion addresses.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

DNS 101

Exam Tips



A CLOUD GURU

- ELB's do not have pre-defined IPv4 addresses, you resolve to them using a DNS name.
- Understand the difference between an Alias Record and a CNAME.
- Given the choice, always choose an Alias Record over a CNAME.

Activate Windows
Go to PC settings to activate Windows.

udemy

Policies

Route53 Routing Policies

Route53 Routing Policies



A CLOUD GURU

- Simple
- Weighted
- Latency
- Failover
- Geolocation

Activate Windows
Go to PC settings to activate Windows.

udemy

Simple And Weighted

Route53 Routing Policies

Simple



A CLOUD GURU

This is the default routing policy when you create a new record set. This is most commonly used when you have a single resource that performs a given function for your domain, for example, one web server that serves content for the `http://acloud.guru` website.

Weighted

Weighted Routing Policies let you split your traffic based on different weights assigned.

For example you can set 10% of your traffic to go to US-EAST-1 and 90% to go to EU-WEST-1.

Go to PC settings to activate windows.

udemy

Latency

Route53 Routing Policies

Latency



A CLOUD GURU

Latency based routing allows you to route your traffic based on the lowest network latency for your end user (ie which region will give them the fastest response time).

To use latency-based routing you create a latency resource record set for the Amazon EC2 (or ELB) resource in each region that hosts your website. When Amazon Route 53 receives a query for your site, it selects the latency resource record set for the region that gives the user the lowest latency. Route 53 then responds with the value associated with that resource record set.

Activate Windows
Go to PC settings to activate Windows.

udemy

Failover

Route53 Routing Policies

Failover



A CLOUD GURU

Failover routing policies are used when you want to create an active/passive set up. For example you may want your primary site to be in EU-WEST-2 and your secondary DR Site in AP-SOUTHEAST-2.

Route53 will monitor the health of your primary site using a health check.

A health check monitors the health of your end points.

Activate Windows
Go to PC settings to activate Windows.

udemy

GeoLocation

Route53 Routing Policies

Geolocation



Geolocation routing lets you choose where your traffic will be sent based on the geographic location of your users (ie the location from which DNS queries originate). For example, you might want all queries from Europe to be routed to a fleet of EC2 instances that are specifically configured for your European customers. These servers may have the local language of your European customers and all prices are displayed in Euros.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

DNS Exam Tips

Exam Tips



A CLOUD GURU

- ELB's do not have pre-defined IPv4 addresses, you resolve to them using a DNS name.
- Understand the difference between an Alias Record and a CNAME.
- Given the choice, always choose an Alias Record over a CNAME.

Activate Windows
Go to PC settings to activate Windows.

udemy

Amazon VPC

- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
- Amazon VPC is the networking layer for Amazon EC2
- Contents
 - VPCs and Subnets
 - Supported Platforms
 - Default and Nondefault VPCs
 - Accessing the Internet
 - Accessing a Corporate or Home Network
 - Accessing Services Through AWS PrivateLink

Amazon VPC continued

- VPCs and Subnets
 - A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC
 - 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.
- Supported Platforms
- Default and Nondefault VPCs
 - If your account supports the EC2-VPC platform only, it comes with a default VPC that has a default subnet in each Availability Zone. A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use. If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.
 - Regardless of which platforms your account supports, you can create your own VPC, and configure it as you need. This is known as a nondefault VPC. Subnets that you create in your nondefault VPC and additional subnets that you create in your default VPC are called nondefault subnets.
- Accessing the Internet
- Accessing a Corporate or Home Network
- Accessing Services Through AWS PrivateLink

VPC

Accessing the Internet

- You control how the instances that you launch into a VPC access resources outside the VPC.
- Your default VPC includes an internet gateway, and each default subnet is a public subnet. Each instance that you launch into a default subnet has a private IPv4 address and a public IPv4 address. These instances can communicate with the internet through the internet gateway. An internet gateway enables your instances to connect to the internet through the Amazon EC2 network edge.
- By default, each instance that you launch into a nondefault subnet has a private IPv4 address, but no public IPv4 address, unless you specifically assign one at launch, or you modify the subnet's public IP address attribute. These instances can communicate with each other, but can't access the internet.
- You can enable internet access for an instance launched into a nondefault subnet by attaching an internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance.
- Alternatively, to allow an instance in your VPC to initiate outbound connections to the internet but prevent unsolicited inbound connections from the internet, you can use a network address translation (NAT) device for IPv4 traffic. 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.

VPC

- Accessing a Corporate or Home Network
 - You can optionally connect your VPC to your own corporate data center using an IPsec AWS managed VPN connection, making the AWS Cloud an extension of your data center.
 - 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
- Accessing Services Through AWS PrivateLink
 - AWS PrivateLink is a highly available, scalable technology that enables you to privately connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services. You do not require an internet gateway, NAT device, public IP address, AWS Direct Connect connection, or VPN connection to communicate with the service. Traffic between your VPC and the service does not leave the Amazon network.
 - To use AWS PrivateLink, create an interface VPC endpoint for a service in your VPC. This creates an elastic network interface in your subnet with a private IP address that serves as an entry point for traffic destined to the service
 - You can create your own AWS PrivateLink-powered service (endpoint service) and enable other AWS customers to access your service

IPv4 for Amazon VPC

- Step 1: Create the VPC
 - Creates a VPC with a /16 IPv4 CIDR block (a network with 65,536 private IP addresses). For more information about CIDR notation and the sizing of a VPC
 - Attaches an Internet gateway to the VPC. For more information about Internet gateways, see Internet Gateways.
 - Creates a size /24 IPv4 subnet (a range of 256 private IP addresses) in the VPC.
 - Creates a custom route table, and associates it with your subnet, so that traffic can flow between the subnet and the Internet gateway.
- Step 2: Create a Security Group
 - A security group acts as a virtual firewall to control the traffic for its associated instances. To use a security group, you add the inbound rules to control incoming traffic to the instance, and outbound rules to control the outgoing traffic from your instance. To associate a security group with an instance, you specify the security group when you launch the instance.
 - Your VPC comes with a default security group. Any instance not associated with another security group during launch is associated with the default security group.
 - Rules for the WebServerSG Security Group (p. 13)
 - Creating Your WebServerSG Security Group (p. 13)
- Step 3: Launch an Instance into Your VPC
- Step 4: Assign an Elastic IP Address to Your Instance
- Step 5: Clean Up
 - Before you can delete a VPC, you must terminate any instances that are running in the VPC. If you delete a VPC using the VPC console, it also deletes resources that are associated with the VPC, such as subnets, security groups, network ACLs, DHCP options sets, route tables, and Internet gateways.

Scenarios and Examples

- This section has examples for creating and configuring a VPC, including scenarios for how to use the VPC wizard in the Amazon VPC console.

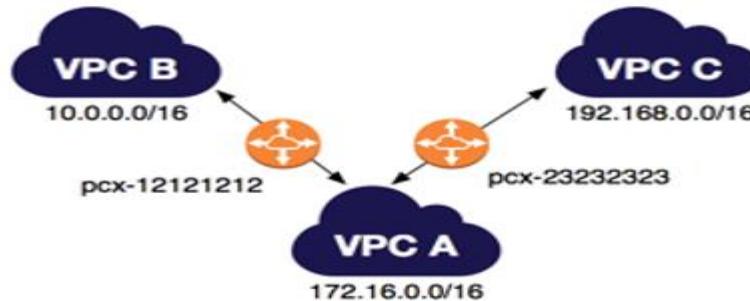
Scenario	Usage
Scenario 1: VPC with a Single Public Subnet	Use the VPC wizard to create a VPC for running a single-tier, public-facing web application such as a blog or simple web site.
Scenario 2: VPC with Public and Private Subnets (NAT)	Use the VPC wizard to create a VPC for running a public-facing web application, while still maintaining non-publicly accessible back-end servers in a second subnet.
Scenario 3: VPC with Public and Private Subnets and AWS Managed VPN Access	Use the VPC wizard to create a VPC for extending your data center into the cloud, and also directly access the Internet from your VPC.
Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access	Use the VPC wizard to create a VPC for extending your data center into the cloud, and leverage Amazon's infrastructure without exposing your network to the Internet.
Example: Create an IPv4 VPC and Subnets Using the AWS CLI	Use the AWS CLI to create a VPC with a public subnet and a private subnet
Example: Create an IPv6 VPC and Subnets Using the AWS CLI	Use the AWS CLI to create a VPC with an associated IPv6 CIDR block and a public subnet and a private subnet, each with an associated IPv6 CIDR block.

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.
- The VPCs can be in different regions (also known as an inter-region VPC peering connection).
- A VPC peering connection helps you to facilitate the transfer of data.
 - For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

Multiple VPC Peering Connections

- A VPC peering connection is a one to one relationship between two VPCs. You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported. You do not have any peering relationship with VPCs that your VPC is not directly peered with.
- The following diagram is an example of one VPC peered to two different VPCs. There are two VPC peering connections: VPC A is peered with both VPC B and VPC C. VPC B and VPC C are not peered, and you cannot use VPC A as a transit point for peering between VPC B and VPC C. If you want to enable routing of traffic between VPC B and VPC C, you must create a unique VPC peering connection between them.



VPC Peering Limitations

- You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks. Amazon always assigns your VPC a unique IPv6 CIDR block. If your IPv6 CIDR blocks are unique but your IPv4 blocks are not, you cannot create the peering connection.
- You have a limit on the number active and pending VPC peering connections that you can have per VPC. For more information, see [Amazon VPC Limits](#) in the [Amazon VPC User Guide](#).
- VPC peering does not support transitive peering relationships. In a VPC peering connection, your VPC does not have access to any other VPCs with which the peer VPC may be peered. This includes VPC peering connections that are established entirely within your own AWS account. For more information about unsupported peering relationships, see [Invalid VPC Peering Connection Configurations](#) (p. 59). For examples of supported peering relationships, see [VPC Peering Scenarios](#) (p. 17).
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.
- A placement group can span peered VPCs that are in the same region; however, you do not get full-bisection bandwidth between instances in peered VPCs. For more information about placement groups, see [Placement Groups](#) in the [Amazon EC2 User Guide for Linux Instances](#).
- Unicast reverse path forwarding in VPC peering connections is not supported. For more information, see [Routing for Response Traffic](#) (p. 45).
- If the VPCs are in the same region, you can enable the resources on either side of a VPC peering connection to communicate with each other over IPv6. IPv6 communication is not automatic. You must associate an IPv6 CIDR block with each VPC, enable the instances in the VPCs for IPv6 communication, and add routes to your route tables that route IPv6 traffic intended for the peer VPC to the VPC peering connection. For more information, see [Your VPC and Subnets](#) in the [Amazon VPC User Guide](#).
- Any tags that you create for your VPC peering connection are only applied in the account or region in which you create them.
- If the IPv4 CIDR block of a VPC in a VPC peering connection falls outside of the private IPv4 address ranges specified by RFC 1918, private DNS hostnames for that VPC cannot be resolved to private IP addresses. To resolve private DNS hostnames to private IP addresses, you can enable DNS resolution support for the VPC peering connection.

Inter-Region VPC Peering Limitations

An inter-region VPC peering connection has additional limitations:

- You cannot create a security group rule that references a peer VPC security group.
- You cannot enable support for an EC2-Classic instance that's linked to a VPC via ClassicLink to communicate with the peer VPC.
- You cannot enable DNS resolution support (a VPC cannot resolve public IPv4 DNS hostnames to private IPv4 addresses when queried from instances in the peer VPC).
- Communication over IPv6 is not supported.
- The Maximum Transmission Unit (MTU) across the VPC peering connection is 1500 bytes (jumbo frames are not supported).
- Inter-region VPC peering connections are supported in all public regions except Asia Pacific (Seoul).

VPC Peering

VPC PEERING

What is VPC Peering?



A CLOUD GURU

VPC Peering is simply a connection between two VPCs that enables you to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a **single region**.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

Activate Windows
Go to PC settings to activate Windows.

udemy

VPC Defn

VPC OVERVIEW

VPC - AWS Definition



A CLOUD GURU

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.



VPC

VPC OVERVIEW

VPC - AWS Definition



A CLOUD GURU

You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.



What can you do with VPC?

VPC OVERVIEW

What can you do with a VPC?



A CLOUD GURU

- Launch instances into a subnet of your choosing
- Assign custom IP address ranges in each subnet
- Configure route tables between subnets
- Create internet gateway and attach it to our VPC
- Much better security control over your AWS resources
- Instance security groups
- Subnet network access control lists (ACLs)



Default VPC vs Custom VPC

VPC OVERVIEW

Default VPC vs Custom VPC



A CLOUD GURU

- Default VPC is user friendly, allowing you to immediately deploy instances.
- All Subnets in default VPC have a route out to the internet.
- Each EC2 instance has both a public and private IP address.

Activate Windows
Go to PC settings to activate Windows.



VPC Peering

VPC OVERVIEW

VPC Peering



A CLOUD GURU

- Allows you to connect one VPC with another via a direct network route using private IP addresses.
- Instances behave as if they were on the same private network
- You can peer VPC's with other AWS accounts as well as with other VPCs in the same account.
- Peering is in a star configuration: ie 1 central VPC peers with 4 others. NO TRANSITIVE PEERING!!!



Activate Windows
Go to PC settings to activate Windows.

 Udemy

Summary

VPC OVERVIEW

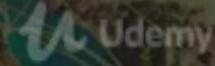
Exam Tips



A CLOUD GURU

- Think of a VPC as a logical datacenter in AWS.
- Consists of IGWs (Or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets, and Security Groups
- 1 Subnet = 1 Availability Zone
- Security Groups are Stateful; Network Access Control Lists are Stateless
- NO TRANSITIVE PEERING

Activate Windows
Go to PC settings to activate Windows.



Nat Instances

VPC Overview

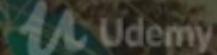
Exam Tips - NAT instances



A CLOUD GURU

- When creating a NAT instance, Disable Source/Destination Check on the Instance.
- NAT instances must be in a public subnet.
- There must be a route out of the private subnet to the NAT instance, in order for this to work.
- The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size.
- You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover.

Activate Windows
Go to PC settings to activate Windows.



NAT Gateways

VPC Overview

Exam Tips - NAT Gateways



A CLOUD GURU

- Preferred by the enterprise
- Scale automatically up to 10Gbps
- No need to patch
- Not associated with security groups
- Automatically assigned a public ip address
- Remember to update your route tables.
- No need to disable Source/Destination Checks
- More secure than a NAT instance

Activate Windows
Go to PC settings to activate Windows.



ACLs

VPC Overview



Exam Tips - Network ACLs

- Your VPC automatically comes with a default network ACL, and by default it allows all outbound and inbound traffic.
- You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.
- Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa.)
- Block IP Addresses using network ACLs not Security Groups

Activate Windows
Get a Cloud Guru Activate Windows



Flow Logs

A large orange icon representing VPC Flow Logs. It features three stylized orange cubes arranged in a perspective view, with a white cloud icon above them, all contained within a rounded rectangular frame.

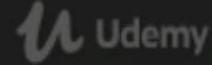
VPC FLOW LOGS

VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.

A CLOUD GURU

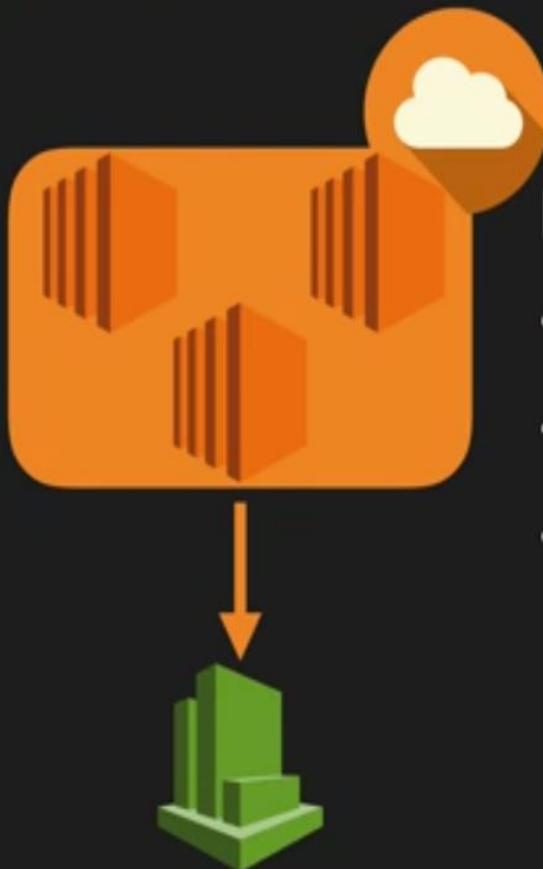
Activate Windows
Go to PC settings to activate Windows.

 Udemy

Flow Logs

VPC FLOW LOGS

VPC Flow Logs



A CLOUD GURU

- Flow logs can be created at 3 levels;
- VPC
 - Subnet
 - Network Interface Level

Activate Windows
Go to PC settings to activate Windows.

 Udemy

Summary

VPC FLOW LOGS

VPC Flow Logs Exam Tips



A CLOUD GURU

- You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.
- You cannot tag a flow log.
- After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log.

Activate Windows
Go to PC settings to activate Windows.

 Udemy

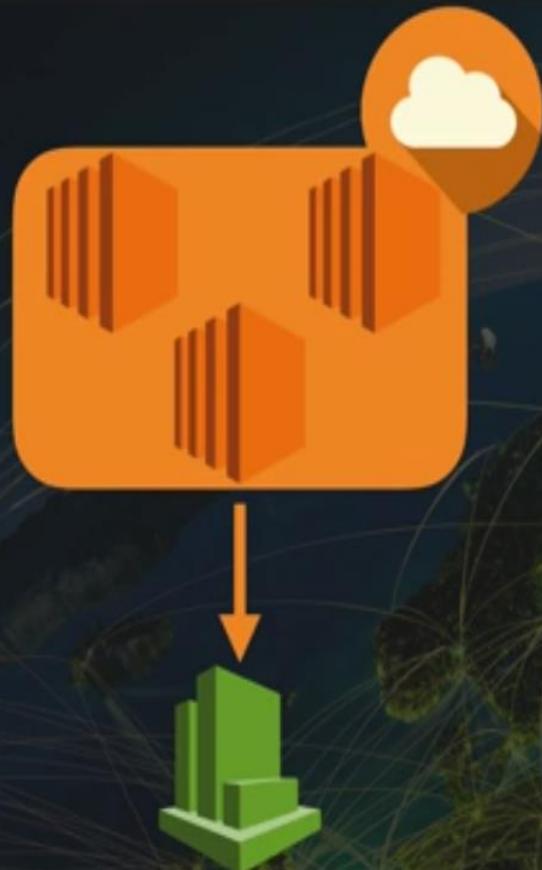
Summary

VPC FLOW LOGS

VPC Flow Logs Exam Tips



A CLOUD GURU



Not all IP Traffic is monitored;

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
- Traffic generated by a Windows instance for Amazon Windows license activation.
- Traffic to and from 169.254.169.254 for instance metadata.
- DHCP traffic.
- Traffic to the reserved IP address for the default VPC router.

Activate Windows
Go to settings > Update & security

Udemy

NAT vs Bastion

VPC Overview

Exam Tips - NAT vs Bastions



A CLOUD GURU

- A NAT is used to provide internet traffic to EC2 instances in private subnets
- A Bastion is used to securely administer EC2 instances (using SSH or RDP) in private subnets. In Australia we call them jump boxes.

Activate Windows
Go to PC settings to activate Windows.

udemy

Amazon S3

- Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers.
- Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web.
- It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites.
- The service aims to maximize benefits of scale and to pass those benefits on to developers.

Advantages S3

Amazon S3 is intentionally built with a minimal feature set that focuses on simplicity and robustness. Following are some of advantages of the Amazon S3 service:

- **Create Buckets** – Create and name a bucket that stores data. Buckets are the fundamental container in Amazon S3 for data storage.
- **Store data in Buckets** – Store an infinite amount of data in a bucket. Upload as many objects as you like into an Amazon S3 bucket. Each object can contain up to 5 TB of data. Each object is stored and retrieved using a unique developer-assigned key.
- **Download data** – Download your data or enable others to do so. Download your data any time you like or allow others to do the same.
- **Permissions** – Grant or deny access to others who want to upload or download data into your Amazon S3 bucket. Grant upload and download permissions to three types of users. Authentication mechanisms can help keep data secure from unauthorized access.
- **Standard interfaces** – Use standards-based REST and SOAP interfaces designed to work with any Internet-development toolkit.
- **Note** SOAP support over HTTP is deprecated, but it is still available over HTTPS. New Amazon S3 features will not be supported for SOAP. We recommend that you use either the REST API or the AWS SDKs.

S3 Concepts

- Buckets
 - A bucket is a container for objects stored in Amazon S3. 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>
 - Buckets serve several purposes: they organize the Amazon S3 namespace at the highest level, they identify the account responsible for storage and data transfer charges, they play a role in access control, and they serve as the unit of aggregation for usage reporting.
- Objects
 - Objects are the fundamental entities stored in Amazon S3. 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.
- Keys
 - A key is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key. Because the combination of a bucket, key, and version ID uniquely identify each object, Amazon S3 can be thought of as a basic data map between "bucket + key + version" and the object itself. Every object in Amazon S3 can be uniquely addressed through the combination of the web service endpoint, bucket name, key, and optionally, a version. For example, in the URL <http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl>, "doc" is the name of the bucket and "2006-03-01/AmazonS3.wsdl" is the key.
- Regions
 - You can choose the geographical region where Amazon S3 will store the buckets you create. You might choose a region to optimize latency, minimize costs, or address regulatory requirements. Objects stored in a region never leave the region unless you explicitly transfer them to another region.
- Amazon S3 Data Consistency Model
 - Amazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions with one caveat. 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.
 - **Note** Amazon S3 does not currently support object locking. If two PUT requests are simultaneously made to the same key, the request with the latest time stamp wins.

S3 Features

- Storage Classes
 - Amazon S3 offers a range of storage classes designed for different use cases. These include Amazon S3 STANDARD for general-purpose storage of frequently accessed data, Amazon S3 STANDARD_IA for long-lived, but less frequently accessed data, and GLACIER for long-term archive.
- Bucket Policies
 - Bucket policies provide centralized access control to buckets and objects based on a variety of conditions, including Amazon S3 operations, requesters, resources, and aspects of the request (e.g., IP address). The policies are expressed in our access policy language and enable centralized management of permissions. The permissions attached to a bucket apply to all of the objects in that bucket.
- AWS Identity and Access Management
 - You can use IAM with Amazon S3 to control the type of access a user or group of users has to specific parts of an Amazon S3 bucket your AWS account owns.
- Access Control Lists
- Versioning
- Operations
 - **Create a Bucket** – Create and name your own bucket in which to store your objects.
 - **Write an Object** – Store data by creating or overwriting an object. When you write an object, you specify a unique key in the namespace of your bucket. This is also a good time to specify any access control you want on the object.
 - **Read an Object** – Read data back. You can download the data via HTTP or BitTorrent.
 - **Deleting an Object** – Delete some of your data.
 - **Listing Keys** – List the keys contained in one of your buckets. You can filter the key list based on a prefix.

S3 API

- The REST Interface
 - The REST API is an HTTP interface to Amazon S3. Using REST, you use standard HTTP requests to create, fetch, and delete buckets and objects.
 - You can use any toolkit that supports HTTP to use the REST API. You can even use a browser to fetch objects, as long as they are anonymously readable.
 - The REST API uses the standard HTTP headers and status codes, so that standard browsers and toolkits work as expected. In some areas, we have added functionality to HTTP
- The SOAP Interface
 - **Note** SOAP support over HTTP is deprecated, but it is still available over HTTPS. New Amazon S3 features will not be supported for SOAP. We recommend that you use either the REST API or the AWS SDKs
 - The SOAP API provides a SOAP 1.1 interface using document literal encoding. The most common way to use SOAP is to download the WSDL (go to <http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl>), use a SOAP toolkit such as Apache Axis or Microsoft .NET to create bindings, and then write code that uses the bindings to call Amazon S3.

Paying for S3

- As part of the [AWS Free Usage Tier](#), you can get started with Amazon S3 for free. Upon sign-up, new AWS customers receive 5 GB of Amazon S3 storage in the Standard Storage class, 20,000 Get Requests, 2,000 Put Requests, and 15 GB of data transfer out each month for one year.
- Storage Pricing (varies by region)

Pricing		S3 Standard-Infrequent Access (S3 Standard-IA) Storage
S3 Standard Storage		All storage \$0.019 per GB
First 50 TB / Month	\$0.025 per GB	S3 One Zone-Infrequent Access (S3 One Zone-IA) Storage
Next 450 TB / Month	\$0.024 per GB	All storage \$0.0152 per GB
Over 500 TB / Month	\$0.023 per GB	Amazon Glacier Storage
		All storage \$0.005 per GB

Customizing S3 URLs with CNAMEs

- Depending on your needs, you might not want "s3.amazonaws.com" to appear on your website or service. For example, if you host your website images on Amazon S3, you might prefer `http://images.johnsmith.net/` instead of <http://johnsmith-images.s3.amazonaws.com/>
- The bucket name must be the same as the CNAME. So `http://images.johnsmith.net/filename` would be the same as `http://images.johnsmith.net.s3.amazonaws.com/filename` if a CNAME were created to map `images.johnsmith.net` to `images.johnsmith.net.s3.amazonaws.com`.
- The CNAME DNS record should alias your domain name to the appropriate virtual hosted-style host name. For example, if your bucket name and domain name are `images.johnsmith.net`, the CNAME record should alias to `images.johnsmith.net.s3.amazonaws.com`.
- Setting the alias target to `s3.amazonaws.com` also works, but it may result in extra HTTP redirects.

Basics

S3 101

S3 - The Basics



A CLOUD GURU

- S3 is Object-based – i.e. allows you to upload files.
- Files can be from 0 Bytes to 5 TB.
- There is unlimited storage.
- Files are stored in Buckets.
- S3 is a universal namespace. That is, names must be unique globally.
- <https://s3-eu-west-1.amazonaws.com/acloudguru>
- When you upload a file to S3, you will receive a HTTP 200 code if the upload was successful.



Data Consistency

S3 101

Data Consistency Model For S3



A CLOUD GURU

- Read after Write consistency for PUTS of new Objects
- Eventual Consistency for overwrite PUTS and Deletes (can take some time to propagate)



WU University

Key-Value Store

S3 101

S3 Is A Simple Key-value Store



- S3 is Object based. Objects consist of the following:
 - Key (This is simply the name of the object)
 - Value (This is simply the data and is made up of a sequence of bytes).
 - Version ID (Important for versioning)
 - Metadata (Data about data you are storing)
 - Subresources:
 - Access Control Lists
 - Torrent



Activate Windows
Go to PC settings to activate Windows.

The Basics

S3 101

S3 - The Basics



A CLOUD GURU

- Built for 99.99% availability for the S3 platform.
- Amazon Guarantee 99.9% availability
- Amazon guarantees 99.99999999% durability for S3 information. (Remember 11 x 9s).
- Tiered Storage Available
- Lifecycle Management
- Versioning
- Encryption
- Secure your data using Access Control Lists and Bucket Policies



Activate Windows
Go to PC settings to activate Windows.

Storage Tiers/Classes

S3 101

S3 - Storage Tiers/Classes



A CLOUD GURU

- **S3 Standard** : 99.99% availability, 99.99999999% durability, stored redundantly across multiple devices in multiple facilities, and is designed to sustain the loss of 2 facilities concurrently.
- **S3 - IA** : (Infrequently Accessed): For data that is accessed less frequently, but requires rapid access when needed. Lower fee than S3, but you are charged a retrieval fee.
- **S3 One Zone - IA**: want a lower-cost option for infrequently accessed data, but do not require the multiple Availability Zone data resilience.
- **Glacier**: Very cheap, but used for archival only. Expedited, Standard or Bulk. A Standard retrieval time takes 3 - 5 hours.

Activate Windows
Go to PC settings to activate Windows.

continued

S3 101

S3 - Storage Tiers/Classes



A CLOUD GURU

	S3 Standard	S3 Standard-IA	S3 One Zone-IA	Amazon Glacier
Designed for Durability	99.999999999%	99.999999999%	99.999999999%†	99.999999999%
Designed for Availability	99.99%	99.9%	99.5%	N/A
Availability SLA	99.9%	99%	99%	N/A
Availability Zones	≥3	≥3	1	≥3
Minimum Capacity Charge per Object	N/A	128KB*	128KB*	N/A
Minimum Storage Duration Charge	N/A	30 days	30 days	90 days
Retrieval Fee	N/A	per GB retrieved	per GB retrieved	per GB retrieved**
First Byte Latency	milliseconds	milliseconds	milliseconds	select minutes or hours***
Storage Type	Object	Object	Object	Object Activate Windows Go to PC settings to activate Windows.
Lifecycle Transitions	Yes	Yes	Yes	Yes

Charges

S3 101

S3 - Charges



A CLOUD GURU

- Charged for:
 - Storage
 - Requests
 - Storage Management Pricing
 - Data Transfer Pricing
 - Transfer Acceleration



Activate Windows
Go to PC settings to activate Windows.

Transfer Acceleration

S3 101

What Is S3 Transfer Acceleration?



A CLOUD GURU

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your end users 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.



Activate Windows
Go to PC settings to activate Windows.

Bucket

CREATE AN S3 BUCKET - LAB

Create an S3 Bucket - Exam Tips



- Buckets are a universal name space
- Upload an object to S3 receive a HTTP 200 Code
- S3, S3 - IA, S3 Reduced Redundancy Storage
- Encryption
 - Client Side Encryption
 - Server Side Encryption
 - Server side encryption with Amazon S3 Managed Keys (SSE-S3)
 - Server side encryption with KMS (SSE-KMS)
 - Server side encryption with Customer Provided Keys (SSE-C)
- Control access to buckets using either a bucket ACL or using Bucket Policies
- BY DEFAULT BUCKETS ARE PRIVATE AND ALL OBJECTS STORED INSIDE THEM ARE PRIVATE

Activate Windows
Go to PC settings to activate Windows.

udemy

Versioning

CREATE AN S3 BUCKET - LAB

S3 - Versioning Exam Tips



A CLOUD GURU

- Stores all versions of an object (including all writes and even if you delete an object)
- Great backup tool.
- Once enabled, Versioning cannot be disabled, only suspended.
- Integrates with Lifecycle rules
- Versioning's MFA Delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security.

Activate Windows
Go to PC settings to activate Windows.



Replication

S3 - CROSS REGION REPLICATION LAB

S3 - Cross Region Replication Exam Tips



A CLOUD GURU

- Versioning must be enabled on both the source and destination buckets.
- Regions must be unique.
- Files in an existing bucket are not replicated automatically. All subsequent updated files will be replicated automatically.
- You cannot replicate to multiple buckets or use daisy chaining (at this time.)
- Delete markers are replicated.
- Deleting individual versions or delete markers will not be replicated.
- Understand what Cross Region Replication is at a high level.

Activate Windows
Go to PC settings to activate Windows.



LCM

LIFECYCLE MANAGEMENT, IA S3 & GLACIER LAB

S3 - Lifecycle Management Lab



A CLOUD GURU

- Can be used in conjunction with versioning.
- Can be applied to current versions and previous versions.
- Following actions can now be done:
 - Transition to the Standard - Infrequent Access Storage Class (30 days after the creation date.)
 - Archive to the Glacier Storage Class (30 days after IA, if relevant)
 - Permanently Delete



CDN

Introduction to CloudFront

What is a CDN



A CLOUD GURU



A content delivery network (CDN) is a system of distributed servers (network) that deliver webpages and other web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server.

Activate Windows
Go to PC settings to activate Windows.



CloudFront - Key

Introduction to CloudFront

CloudFront - Key Terminology



A CLOUD GURU

- Edge Location - This is the location where content will be cached. This is separate to an AWS Region/AZ
- Origin - This is the origin of all the files that the CDN will distribute. This can be either an S3 Bucket, an EC2 Instance, an Elastic Load Balancer or Route53.
- Distribution - This is the name given the CDN which consists of a collection of Edge Locations.

Activate Windows
Go to PC settings to activate Windows.



CloudFront

Introduction to CloudFront

What is CloudFront



A CLOUD GURU



Amazon CloudFront can be used to deliver your entire website, including dynamic, static, streaming, and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location, so content is delivered with the best possible performance.

Activate Windows
Go to PC settings to activate Windows.

Udemy

Securing Buckets

S3 - Security & Encryption
Section 4, Lecture 23
S3 - Security & Encryption

Securing your buckets

Go to Dashboard

A CLOUD GURU

- By default, all newly created buckets are PRIVATE
- You can setup access control to your buckets using;
 - Bucket Policies
 - Access Control Lists
- S3 buckets can be configured to create access logs which log all requests made to the S3 bucket. This can be done to another bucket.

899 people bookmarked this moment.

Activate Windows
Go to PC settings to activate Windows.

udemy

▶ 1x ⏪ 1:27 / 5:39

Browse Q&A Add Bookmark Continue ▶

Encryption

S3 - Security & Encryption

Encryption



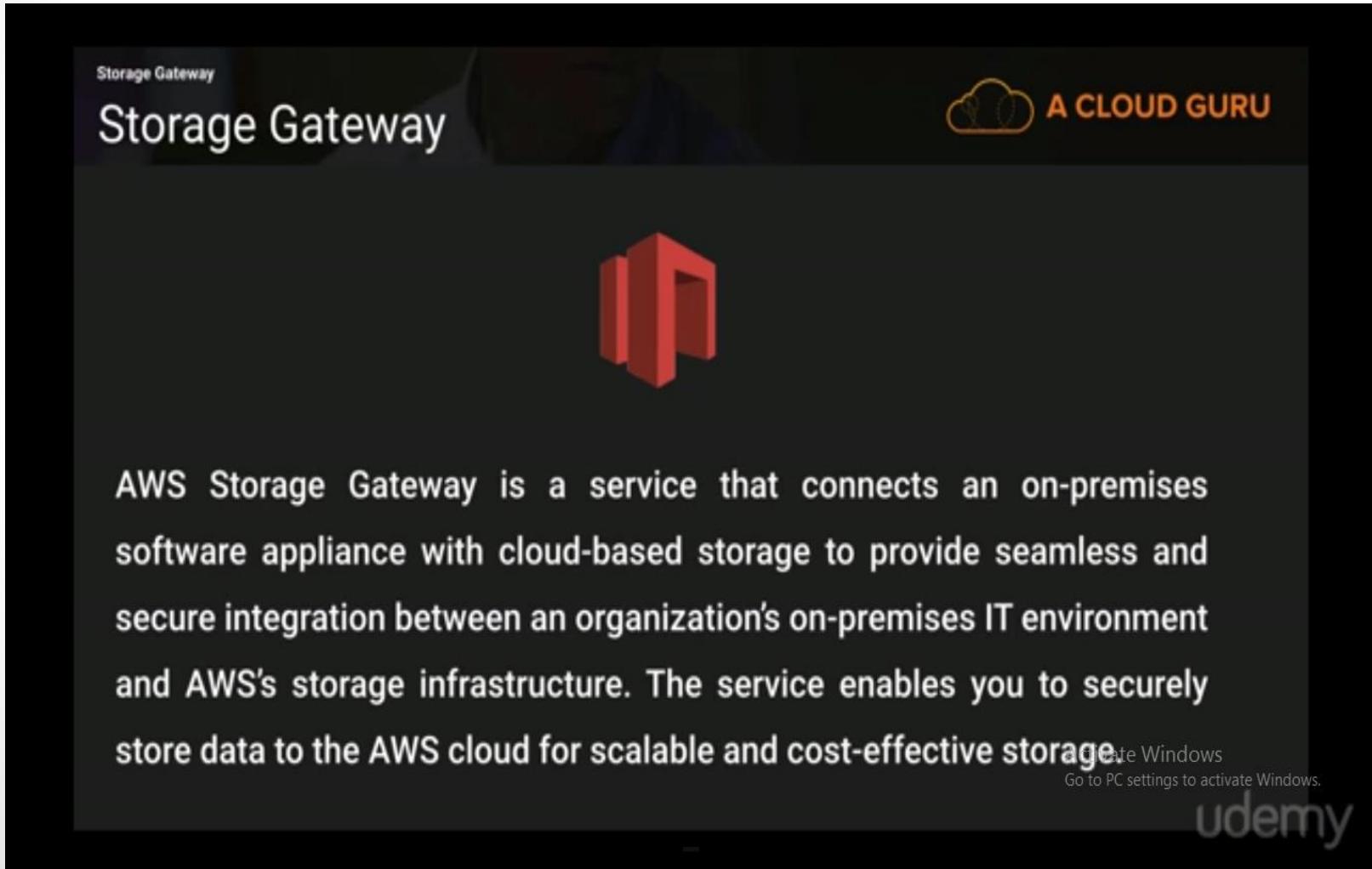
A CLOUD GURU

- In Transit;
 - SSL/TLS
- At Rest
 - Server Side Encryption
 - S3 Managed Keys - **SSE-S3**
 - AWS Key Management Service, Managed Keys - **SSE-KMS**
 - Server Side Encryption With Customer Provided Keys - **SSE-C**
 - Client Side Encryption

Activate Windows
Go to PC settings to activate Windows.

udemy

Storage Gateway

A screenshot of a web page for "Storage Gateway". The top navigation bar has "Storage Gateway" on the left and "A CLOUD GURU" with a cloud icon on the right. Below the header is a large red 3D letter "F" logo. The main content area contains a paragraph about AWS Storage Gateway, followed by a "Activate Windows" watermark.

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. The service enables you to securely store data to the AWS cloud for scalable and cost-effective storage.

Activate Windows
Go to PC settings to activate Windows.

udemy

Storage Gateway

Storage Gateway

Storage Gateway



A CLOUD GURU



AWS Storage Gateway's software appliance is available for download as a virtual machine (VM) image that you install on a host in your datacenter. Storage Gateway supports either VMware ESXi or Microsoft Hyper-V. Once you've installed your gateway and associated it with your AWS account through the activation process, you can use the AWS Management Console to create the storage gateway option that is right for you.

Activate Windows
Go to PC settings to activate Windows.

udemy

Types of Storage Gateways

Storage Gateway

Four Types of Storage Gateways



A CLOUD GURU

- File Gateway (NFS)
- Volumes Gateway (iSCSI)
 - Stored Volumes
 - Cached Volumes
- Tape Gateway (VTL)

Activate Windows
Go to PC settings to activate Windows.

udemy

File Gateway

Storage Gateway

File Gateway



Files are stored as objects in your S3 buckets, accessed through a Network File System (NFS) mount point. Ownership, permissions, and timestamps are durably stored in S3 in the user-metadata of the object associated with the file. Once objects are transferred to S3, they can be managed as native S3 objects, and bucket policies such as versioning, lifecycle management, and cross-region replication apply directly to objects stored in your bucket.

Activate Windows
Go to PC Settings to activate Windows.

udemy

Volume Gateway

Storage Gateway

Volume Gateway



A CLOUD GURU



The volume interface presents your applications with disk volumes using the iSCSI block protocol.

Data written to these volumes can be asynchronously backed up as point-in-time snapshots of your volumes, and stored in the cloud as Amazon EBS snapshots.

Snapshots are incremental backups that capture only changed blocks. All snapshot storage is also compressed to minimize your storage charges.

Activate Windows
Go to PC settings to activate Windows.

udemy

Stored Volumes

Storage Gateway

Volume Gateway - Stored Volumes



A CLOUD GURU



Stored volumes let you store your primary data locally, while asynchronously backing up that data to AWS. Stored volumes provide your on-premises applications with low-latency access to their entire datasets, while providing durable, off-site backups. You can create storage volumes and mount them as iSCSI devices from your on-premises application servers. Data written to your stored volumes is stored on your on-premises storage hardware. This data is asynchronously backed up to Amazon Simple Storage Service (Amazon S3) in the form of Amazon Elastic Block Store (Amazon EBS) snapshots. 1 GB - 16 TB in size for Stored Volumes.

Activate Windows
Go to PC settings to activate Windows.

udemy

Cached Volumes

The screenshot shows a dark-themed web page for 'Storage Gateway'. In the top left corner, it says 'Storage Gateway'. In the top right corner, there is a yellow cloud icon followed by the text 'A CLOUD GURU' in orange. Below the header, there is a large red 3D-style letter 'P' logo. The main content area contains the following text:

Cached volumes let you use Amazon Simple Storage Service (Amazon S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage. 1 GB - 32 TB in size for Cached Volumes.

At the bottom right of the page, there is a watermark for 'udemy'.

Tape Gateway

Storage Gateway

Volume Gateway - Tape Gateway



A CLOUD GURU



Tape Gateway offers a durable, cost-effective solution to archive your data in the AWS Cloud. The VTL interface it provides lets you leverage your existing tape-based backup application infrastructure to store data on virtual tape cartridges that you create on your tape gateway. Each tape gateway is preconfigured with a media changer and tape drives, which are available to your existing client backup applications as iSCSI devices. You add tape cartridges as you need to archive your data. Supported by NetBackup, Backup Exec, Veeam etc.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

Storage Gateway

Exam Tips

A CLOUD GURU

- File Gateway - For flat files, stored directly on S3.
- Volume Gateway:
 - Stored Volumes - Entire Dataset is stored on site and is asynchronously backed up to S3.
 - Cached Volumes - Entire Dataset is stored on S3 and the most frequently accessed data is cached on site.
- Gateway Virtual Tape Library (VTL)
 - Used for backup and uses popular backup applications like NetBackup, Backup Exec, Veeam etc.

Activate Windows
Go to PC settings to activate Windows.

udemy

Types Of Snowball

Snowball

Types Of Snowballs



A CLOUD GURU

- Snowball
- Snowball Edge
- Snowmobile

Activate Windows
Go to PC settings to activate Windows.



Snowball

Snowball

Snowball



A CLOUD GURU

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet.

80TB snowball in all regions. Snowball uses multiple layers of security designed to protect your data including tamper-resistant enclosures, 256-bit encryption, and an industry-standard Trusted Platform Module (TPM) designed to ensure both security and full chain-of-custody of your data. Once the data transfer job has been processed and verified, AWS performs a software erasure of the Snowball appliance.

Activate Windows
Go to PC settings to activate Windows.



Snowball Edge

Snowball

Snowball Edge



A CLOUD GURU

AWS Snowball Edge is a 100TB data transfer device with on-board storage and compute capabilities. You can use Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local datasets, or to support local workloads in remote or offline locations.

Snowball Edge connects to your existing applications and infrastructure using standard storage interfaces, streamlining the data transfer process and minimizing setup and integration. Snowball Edge can cluster together to form a local storage tier and process your data on-premises, helping ensure your applications continue to run even when they are not able to access the cloud.

Activate Windows
Go to PC settings to activate Windows.



Snowmobile

Snowball

Snowmobile



A CLOUD GURU

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. Transferring data with Snowmobile is secure, fast and cost effective.



Activate Windows
Go to PC settings to activate Windows.



Transfer Acceleration

DynamoDB 101

What is S3 Transfer Acceleration?



A CLOUD GURU

S3 Transfer Acceleration utilises the CloudFront Edge Network to accelerate your uploads to S3. Instead of uploading directly to your S3 bucket, you can use a distinct URL to upload directly to an edge location which will then transfer that file to S3. You will get a distinct URL to upload to;

acloudguru.s3-accelerate.amazonaws.com

Activate Windows
Go to PC settings to activate Windows.





Amazon RDS

- Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.
- Overview
 - Amazon RDS manages backups, software patching, automatic failure detection, and recovery.
 - To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges.
 - You can have automated backups performed when you need them, or manually create your own backup snapshot. You can use these backups to restore a database. The Amazon RDS restore process works reliably and efficiently.
 - You can get high availability with a primary instance and a synchronous secondary instance that you can fail over to when problems occur. You can also use MySQL, MariaDB, or PostgreSQL Read Replicas to increase read scaling.
 - You can use the database products you are already familiar with: MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server, and the new, MySQL-compatible Amazon Aurora DB engine (for information, see Amazon Aurora on Amazon RDS (p. 434)).
 - In addition to the security in your database package, you can help control who can access your RDS databases by using AWS Identity and Access Management (IAM) to define users and permissions. You can also help protect your databases by putting them in a virtual private cloud.

DB Instances

- The basic building block of Amazon RDS is the DB instance. A DB instance is an isolated database environment in the cloud.
- A DB instance can contain multiple user-created databases, and you can access it by using the same tools and applications that you use with a stand-alone database instance. You can create and modify a DB instance by using the AWS Command Line Interface, the Amazon RDS API, or the AWS Management Console.
- 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.
- The computation and memory capacity of a DB instance is determined by its DB instance class. You can select the DB instance that best meets your needs. If your needs change over time, you can change DB instances.
- DB instance storage comes in three types: Magnetic, General Purpose (SSD), and Provisioned IOPS (PIOPS). They differ in performance characteristics and price, allowing you to tailor your storage performance and cost to the needs of your database. Each DB instance has minimum and maximum storage requirements depending on the storage type and the database engine it supports.
- You can run a DB instance on a virtual private cloud using the Amazon Virtual Private Cloud (VPC) service.

Security

- A security group controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify.
- 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.

ElasticCache

Databases 101

What is ElastiCache?



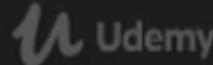
A CLOUD GURU

ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases.

ElastiCache supports two open-source in-memory caching engines:

- Memcached
- Redis

Activate Windows
Go to PC settings to activate Windows.



Elasticcach

Elasticcach

What is Elasticcach



A CLOUD GURU

Amazon ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads (such as social networking, gaming, media sharing and Q&A portals) or compute-intensive workloads (such as a recommendation engine).

Caching improves application performance by storing critical pieces of data in memory for low-latency access. Cached information may include the results of I/O-intensive database queries or the results of computationally-intensive calculations.

Activate Windows
Go to PC settings to activate Windows.

udemy

Types of ElastiCache



- Memcached
 - A widely adopted memory object caching system. ElastiCache is protocol compliant with Memcached, so popular tools that you use today with existing Memcached environments will work seamlessly with the service.
- Redis
 - A popular open-source in-memory key-value store that supports data structures such as sorted sets and lists. ElastiCache supports Master / Slave replication and Multi-AZ which can be used to achieve cross AZ redundancy.

DB Types

Databases 101

AWS Database Types - Summary

- RDS - OLTP
 - SQL
 - MySQL
 - PostgreSQL
 - Oracle
 - Aurora
 - MariaDB
- DynamoDB - No SQL
- RedShift - OLAP
- ElastiCache - In Memory Caching:



Activate Windows
Go to PC settings to activate Windows.

 Udemy

The Udemy logo features a stylized 'U' icon followed by the word 'Udemy' in a lowercase, sans-serif font.

Automated Backups

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

Automated Backups



A CLOUD GURU

- There are two different types of Backups for AWS: Automated Backups and Database Snapshots.
- Automated Backups allow you to recover your database to any point in time within a “retention period”. The retention period can be between one and 35 days. Automated Backups will take a full daily snapshot and will also store transaction logs throughout the day. When you do a recovery, AWS will first choose the most recent daily back up, and then apply transaction logs relevant to that day. This allows you to do a point in time recovery down to a second, within the retention period.

Activate Windows
Go to PC settings to activate Windows.



Continued

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

Automated Backups

Automated Backups are enabled by default. The backup data is stored in S3 and you get free storage space equal to the size of your database. So if you have an RDS instance of 10Gb, you will get 10Gb worth of storage.

Backups are taken within a defined window. During the backup window, storage I/O may be suspended while your data is being backed up and you may experience elevated latency.



A CLOUD GURU



Encryption

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

Encryption



A CLOUD GURU

Encryption at rest is supported for MySQL, Oracle, SQL Server, PostgreSQL, MariaDB & Aurora. Encryption is done using the AWS Key Management Service (KMS) service. Once your RDS instance is encrypted, the data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots.

At the present time, encrypting an existing DB Instance is not supported. To use Amazon RDS encryption for an existing database, you must first create a snapshot, make a copy of that snapshot and encrypt the copy.



Multi-AZ RDS

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

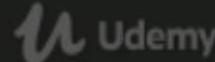
What is Multi-AZ RDS?



Multi-AZ allows you to have an exact copy of your production database in another Availability Zone. AWS handles the replication for you, so when your production database is written to, this write will automatically be synchronized to the stand by database.

In the event of planned database maintenance, DB Instance failure, or an Availability Zone failure, Amazon RDS will automatically failover to the standby so that database operations can resume quickly without administrative intervention.

Activate Windows
Go to PC settings to activate Windows.



Multi-AZ DBs

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

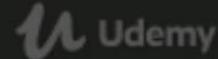
Multi-AZ Databases



A CLOUD GURU

- SQL Server
- Oracle
- MySQL Server
- PostgreSQL
- MariaDB

Activate Windows
Go to PC settings to activate Windows.



Read Replica

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

What is a Read Replica?



Read replicas allow you to have a read-only copy of your production database. This is achieved by using Asynchronous replication from the primary RDS instance to the read replica. You use read replicas primarily for very read-heavy database workloads.

Activate Windows
Go to PC settings to activate Windows.



Read Replica DBs

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

Read Replica Databases



A CLOUD GURU

- MySQL Server
- PostgreSQL
- MariaDB
- Aurora



Activate Windows
Go to PC settings to activate Windows.



Read Replica Databases

RDS - BACK UPS, MULTI-AZ & READ REPLICAS

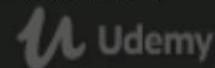
Read Replica Databases



A CLOUD GURU

- Used for scaling, **not** for DR!
- Must have automatic backups turned on in order to deploy a read replica.
- You can have up to 5 read replica copies of any database.
- You can have read replicas of read replicas (but watch out for latency.)
- Each read replica will have its own DNS end point.
- You **can** have read replicas that have Multi-AZ.
- You **can** create read replicas of Multi-AZ source databases.
- Read replicas can be promoted to be their own databases. This breaks the replication.
- You can have a read replica in a second region.

Activate Windows
Go to PC settings to activate Windows.



DynamoDB

DynamoDB

What is DynamoDB?



Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed database and supports both document and key-value data models. Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, IoT, and many other applications.

Activate Windows
Go to PC settings to activate Windows.

udemy

DynamoDb

DynamoDB

DynamoDB



A CLOUD GURU

- Stored on SSD storage
- Spread Across 3 geographically distinct data centres
- Eventual Consistent Reads (Default)
- Strongly Consistent Reads

Activate Windows
Go to PC settings to activate Windows.

udemy

continued

DynamoDB

DynamoDB



A CLOUD GURU

- Eventual Consistent Reads
 - Consistency across all copies of data is usually reached within a second. Repeating a read after a short time should return the updated data. (Best Read Performance)
- Strongly Consistent Reads
 - A strongly consistent read returns a result that reflects all writes that received a successful response prior to the read.

Activate Windows
Go to PC settings to activate Windows.

udemy

Pricing

DynamoDB

DynamoDB Pricing



- Provisioned Throughput Capacity
 - Write Throughput \$0.0065 per hour for every 10 units
 - Read Throughput \$0.0065 per hour for every 50 units
- Storage costs of \$0.25Gb per month.

Activate Windows
Go to PC settings to activate Windows.

udemy

Redshift

Redshift

What is Redshift



Amazon Redshift is a fast and powerful, fully managed, petabyte-scale data warehouse service in the cloud. Customers can start small for just \$0.25 per hour with no commitments or upfront costs and scale to a petabyte or more for \$1,000 per terabyte per year, less than a tenth of most other data warehousing solutions.

Activate Windows
Go to PC settings to activate Windows.

udemy

Configuration

Redshift

Redshift Configuration



- Single Node (160Gb)
- Multi-Node
 - Leader Node (manages client connections and receives queries).
 - Compute Node (store data and perform queries and computations). Up to 128 Compute Nodes

Activate Windows
Go to PC settings to activate Windows.

udemy

Feature

Redshift

Redshift - 10 times faster



Columnar Data Storage: Instead of storing data as a series of rows, Amazon Redshift organizes the data by column. Unlike row-based systems, which are ideal for transaction processing, column-based systems are ideal for data warehousing and analytics, where queries often involve aggregates performed over large data sets. Since only the columns involved in the queries are processed and columnar data is stored sequentially on the storage media, column-based systems require far fewer I/Os, greatly improving query performance.

Activate Windows
Go to www.microsoft.com/windows/activation

udemy

Feature

Redshift

Redshift - 10 times faster



A CLOUD GURU

Advanced Compression: Columnar data stores can be compressed much more than row-based data stores because similar data is stored sequentially on disk. Amazon Redshift employs multiple compression techniques and can often achieve significant compression relative to traditional relational data stores. In addition, Amazon Redshift doesn't require indexes or materialized views and so uses less space than traditional relational database systems.

When loading data into an empty table, Amazon Redshift automatically samples your data and selects the most appropriate compression scheme.

Activate Windows
www.microsoft.com/activate-windows

udemy

Pricing

Redshift

Redshift Pricing



- Compute Node Hours (total number of hours you run across all your compute nodes for the billing period. You are billed for 1 unit per node per hour, so a 3-node data warehouse cluster running persistently for an entire month would incur 2,160 instance hours. You will not be charged for leader node hours; only compute nodes will incur charges.)
- Backup
- Data transfer (only within a VPC, not outside it)

Activate Windows
Go to PC settings to activate Windows.

udemy

Availability

Redshift

Redshift Availability



A CLOUD GURU

- Currently only available in 1 AZ
- Can restore snapshots to new AZ's in the event of an outage.

Activate Windows
Go to PC settings to activate Windows.

udemy

Aurora

Aurora

What is Aurora



A CLOUD GURU

Amazon Aurora is a MySQL-compatible, relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases.

Amazon Aurora provides up to five times better performance than MySQL at a price point one tenth that of a commercial database while delivering similar performance and availability.

Activate Windows
Go to PC settings to activate Windows.



Scaling

Aurora

Aurora Scaling



A CLOUD GURU

- 2 copies of your data is contained in each availability zone, with minimum of 3 availability zones. 6 copies of your data.
- Aurora is designed to transparently handle the loss of up to two copies of data without affecting database write availability and up to three copies without affecting read availability.
- Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.

Activate Windows
Go to PC settings to activate Windows.



Aurora Replica

Aurora

Aurora Replicas



A CLOUD GURU

- 2 Types of Replicas are available.
- Aurora Replicas (currently 15)
- MySQL Read Replicas (currently 5)

Activate Windows
Go to PC settings to activate Windows.

AWS Well-Architected

- The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale with your application needs over time.
- Operational Excellence
 - The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.
- Security
 - The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
- Reliability
 - The ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.
- Performance Efficiency
 - The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.
- Cost Optimization
 - The ability to avoid or eliminate unneeded cost or suboptimal resources.

General Design Principles

The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud:

- **Stop guessing your capacity needs:** Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you might end up sitting on expensive idle resources or dealing with the performance implications of limited capacity. With cloud computing, these problems can go away. You can use as much or as little capacity as you need, and scale up and down automatically.
- **Test systems at production scale:** In the cloud, you can create a production-scale test environment on demand, complete your testing, and then decommission the resources. Because you only pay for the test environment when it's running, you can simulate your live environment for a fraction of the cost of testing on premises.
- **Automate to make architectural experimentation easier:** Automation allows you to create and replicate your systems at low cost and avoid the expense of manual effort. You can track changes to your automation, audit the impact, and revert to previous parameters when necessary.
- **Allow for evolutionary architectures:** Allow for evolutionary architectures. In a traditional environment, architectural decisions are often implemented as static, one-time events, with a few major versions of a system during its lifetime. As a business and its context continue to change, these initial decisions might hinder the system's ability to deliver changing business requirements.
- **Drive architectures using data:** In the cloud you can collect data on how your architectural choices affect the behavior of your workload. This lets you make fact-based decisions on how to improve your workload. Your cloud infrastructure is code, so you can use that data to inform your architecture choices and improvements over time.
- **Improve through game days:** Test how your architecture and processes perform by regularly scheduling game days to simulate events in production.

Operational-Excellence

Operational excellence in the cloud is composed of three areas:

- Prepare
 - Operational priorities
 - The Key AWS service that supports defining your operational priorities is AWS Support. It provides a combination of tools and expertise to help you define your goals on AWS.
 - **AWS Cloud Compliance** enables you to understand the robust controls in place at AWS to maintain security and data protection in the cloud.
 - **AWS Trusted Advisor** provides real-time guidance to help you provision your resources following AWS best practices.
 - **Business Support** provides access to the full set of Trusted Advisor checks and guidance to provision your resources following AWS best practices.
 - **Enterprise Support** customers also receive support from Technical Account Managers (TAMs) who, as designated technical points of contact, provide guidance to help you plan and build solutions using best practices, and proactively keep your AWS environment operationally healthy.
 - Design for operations
 - The key AWS service that supports designing for operations is Amazon CloudWatch, which allows you to monitor AWS Cloud resources and the applications that you run on AWS.
 - **AWS CloudFormation** allows you to create version-controlled standardized templates for your infrastructure.
 - **AWS Developer Tools** is a set of services enabling rapid and safe delivery of software.
 - **AWS X-Ray** traces user requests as they travel through your entire application, enabling analysis and debugging of distributed applications.
 - Operational readiness
 - The key AWS service that supports operational readiness is AWS Lambda, which enables the definition of operational procedures as code that can be triggered by events within your environment.
 - **AWS Config** allows you to track changes to your deployed CloudFormation stacks. With AWS Config rules you can evaluate whether your AWS resources comply with best practices.
 - **Amazon EC2 Systems Manager** is a collection of capabilities that helps you automate management tasks on your Amazon Elastic Compute Cloud (Amazon EC2) instances.

Operational-Excellence

Continued

- Operate
 - Understanding operational Health
 - The key AWS service that helps you understand operational health is Amazon CloudWatch through its feature set including metrics and dashboards.
 - **Amazon CloudWatch Logs** allows you to monitor and store logs from EC2 instances, AWS CloudTrail, and other sources.
 - **Amazon ES** makes it easy to deploy, secure, operate, and scale Elasticsearch for log analytics, and application monitoring.
 - **Personal Health Dashboard** provides alerts and remediation guidance when AWS is experiencing events that may impact you.
 - **Service Health Dashboard** provides up-to-the-minute information on AWS service availability.
 - Responding to Events
 - The key AWS service that helps you automate response to events is AWS Lambda, which enables the definition of operational procedures as code that can be triggered by events within your environment.
 - **Amazon CloudWatch** is used for the collection of logs and metrics. It enables the triggered execution of responses.
 - **Amazon CloudWatch Events** delivers a near real-time stream of system events that can be matched to rules you define to trigger automated responses.
 - **Amazon SNS** is a flexible, fully managed publication subscription messaging and mobile notifications service for coordinating the delivery
 - **Auto Scaling** helps you maintain application availability and allows you to dynamically scale your Amazon EC2 capacity up or down automatically according to conditions you define.
 - **Amazon EC2 Systems Manager** is a collection of capabilities that helps you automate management tasks on your EC2 instances.

Operational-Excellence

Continued

- Evolve
 - Learning from experience
 - The key AWS service that helps you learn from experience is Amazon ES, which allows you to go analyze your log data to gain actionable insights quickly and securely.
 - **Amazon QuickSight** is a business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get insights from your data.
 - **Amazon Athena** is a serverless interactive query service that makes it easy to analyze data in Amazon S3.
 - **Amazon S3** can be used for collection and archival retention of logs.
 - **Amazon CloudWatch** is used for the collection of logs and metrics and the creation of dashboards.
 - Sharing learnings
 - The key AWS service that supports sharing learnings is AWS IAM, which enables you to manage the sharing of resources within and across accounts.
 - **Amazon SNS** enables event-based notification of publishing of resources to subscribers.
 - **AWS CodeCommit** provides a version-controlled repository for your operations as code that can be shared through IAM.
 - **AWS Lambda** enables the definition of operational procedures as code that can be shared across accounts.
 - **AWS CloudFormation** allows you to create version-controlled standardized templates for your infrastructure.
 - **Amazon Machine Images (AMIs)** are predefined operating system templates for your EC2 compute environments. Resources

Security Summary

Well-Architected Framework - Security

Exam Tips - Security Pillar - Questions



A CLOUD GURU

- Data protection
 - How are you encrypting and protecting your data at rest?
 - How are you encrypting and protecting your data in transit? (SSL)
- Privilege management
 - How are you protecting access to and use of the AWS root account credentials?
 - How are you defining roles and responsibilities of system users to control human access to the AWS Management Console and APIs?
 - How are you limiting automated access (such as from applications, scripts, or third-party tools or services) to AWS resources?

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary Security

Well-Architected Framework - Security

Exam Tips - Security Pillar - Questions



- Infrastructure protection
 - How are you enforcing network and host-level boundary protection?
 - How are you enforcing AWS service level protection?
 - How are you protecting the integrity of the operating systems on your Amazon EC2 instances?
- Detective controls
- How are you capturing and analyzing AWS logs?

Activate Windows
Go to PC settings to activate Windows.

udemy

Reliability

Well-Architected Framework - Reliability

Exam Tips - Reliability Pillar



A CLOUD GURU

Reliability in the cloud consists of 3 areas;

- Foundations
- Change management
- Failure management

Activate Windows
Go to PC settings to activate Windows.

udemy

Efficiency

Well-Architected Framework - Performance Efficiency

Exam Tips - Performance Efficiency Pillar A CLOUD GURU

Performance Efficiency in the cloud consists of 4 areas;

- Compute
- Storage
- Database
- Space-time trade-off

Activate Windows
Go to PC settings to activate Windows.

udemy

Cost Optimization

Well-Architected Framework - Cost Optimization

Exam Tips - Cost Optimization Pillar



A CLOUD GURU

Cost Optimization in the cloud consists of 4 areas;

- Matched supply and demand
- Cost-effective resources
- Expenditure awareness
- Optimizing over time

Activate Windows
Go to PC settings to activate Windows.

udemy

Design For Failure

ARCHITECTING FOR THE CLOUD BEST PRACTICES WHITEPAPER

Design For Failure



A CLOUD GURU

Rule of thumb: Be a pessimist when designing architectures in the cloud; assume things will fail. In other words, always design, implement and deploy for automated recovery from failure.

In particular, assume that your hardware will fail. Assume that outages will occur. Assume that some disaster will strike your application.

Assume that you will be slammed with more than the expected number of requests per second some day. Assume that with time your application software will fail too. By being a pessimist, you end up thinking about recovery strategies during design time, which helps in designing an overall system better.

Activate Windows
Go to PC settings to activate Windows.

udemy

IAM Offers

Identity Access Management 101

What does IAM give you?



A CLOUD GURU

- Centralised control of your AWS account
- Shared Access to your AWS account
- Granular Permissions
- Identity Federation (including Active Directory, Facebook, LinkedIn etc)
- Multifactor Authentication
- Provide temporary access for users/devices and services where necessary
- Allows you to set up your own password rotation policy
- Integrates with many different AWS services
- Supports PCI DSS Compliance

Activate Windows
Go to PC settings to activate Windows.

udemy

Terms

Identity Access Management 101



A CLOUD GURU

Critical Terms:

- Users - End Users (think people)
- Groups - A collection of users under one set of permissions.
- Roles - You create roles and can then assign them to AWS resources
- Policies - A document that defines one (or more permissions)

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

Identity Access Management 101

What have we learnt so far?



A CLOUD GURU

- IAM is universal. It does not apply to regions at this time.
- The “root account” is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have NO permissions when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created.
- These are not the same as a password, and you cannot use the Access key ID & Secret Access Key to Login in to the console. You can use this to access AWS via the APIs and Command Line however.
- You only get to view these once. If you lose them, you have to regenerate them. So save them in a secure location.
- Always setup Multifactor Authentication on your root account.
- You can create and customise your own password rotation policies.

Activate Windows
Go to PC settings to activate Windows.



- Always setup Multifactor Authentication on your account.
- You can create and customise your own password policies.

SQS

SQS

What is SQS?



A CLOUD GURU

Amazon SQS is a web service that gives you access to a message queue that can be used to store messages while waiting for a computer to process them.

Amazon SQS is a distributed queue system that enables web service applications to quickly and reliably queue messages that one component in the application generates to be consumed by another component. A queue is a temporary repository for messages that are awaiting processing.

Activate Windows
Go to PC settings to activate Windows.



SQS

SQS

What Is SQS?



A CLOUD GURU

Using Amazon SQS, you can decouple the components of an application so they run independently, easing message management between components.

Any component of a distributed application can store messages in the queue. Messages can contain up to 256 KB of text in any format. Any component can later retrieve the messages programmatically using the Amazon SQS API.

The queue acts as a buffer between the component producing and saving data, and the component receiving the data for processing. This means the queue resolves issues that arise if the producer is producing work faster than the consumer can process it, or if the producer or consumer are only intermittently connected to the network.

Types

SQS

Queue Types



A CLOUD GURU

There are two types of Queue:

- Standard Queues (default)
- FIFO Queues (First-In-First-Out)



Activate Windows
Go to PC settings to activate Windows.

Standard Queues

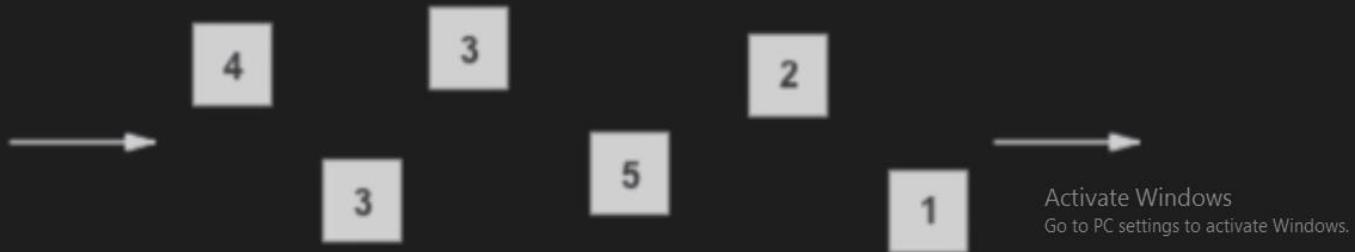
SQS

Standard Queues



A CLOUD GURU

Amazon SQS offers standard as the default queue type. A standard queue lets you have a nearly-unlimited number of transactions per second. Standard queues guarantee that a message is delivered at least once. However, occasionally (because of the highly-distributed architecture that allows high throughput), more than one copy of a message might be delivered out of order. Standard queues provide best-effort ordering which ensures that messages are generally delivered in the same order as they are sent.



Activate Windows
Go to PC settings to activate Windows.

FIFO Queues

SQS

FIFO Queues



A CLOUD GURU

The FIFO queue complements the standard queue. The most important features of this queue type are FIFO (first-in-first-out) delivery and exactly-once processing: The order in which messages are sent and received is strictly preserved and a message is delivered once and remains available until a consumer processes and deletes it; duplicates are not introduced into the queue. FIFO queues also support message groups that allow multiple ordered message groups within a single queue. FIFO queues are limited to 300 transactions per second (TPS), but have all the capabilities of standard queues.



Activate Windows
Go to PC settings to activate Windows.

Keys

SQS

SQS Key Facts

A CLOUD GURU

- SQS is pull-based, not pushed-based
- Messages are 256 KB in size
- Messages can be kept in the queue from 1 minute to 14 days
- Default retention period is 4 days
- SQS guarantees that your messages will be processed at least once.



Activate Windows
Go to PC settings to activate Windows.

Udemy

Visibility Timeout

SQS

SQS Visibility Timeout



A CLOUD GURU

- The Visibility Timeout is the amount of time that the message is invisible in the SQS queue after a reader picks up that message. Provided the job is processed before the visibility time out expires, the message will then be deleted from the queue. If the job is not processed within that time, the message will become visible again and another reader will process it. This could result in the same message being delivered twice.
- Default Visibility Timeout is 30 seconds
- Increase it if your task takes >30 seconds
- Maximum is 12 hours



Activate Windows
Go to PC settings to activate Windows.

Udemy

SQS Long Polling

SQS

SQS Long Polling



A CLOUD GURU

- Amazon SQS long polling is a way to retrieve messages from your Amazon SQS queues.
- While the regular short polling returns immediately (even if the message queue being polled is empty), long polling doesn't return a response until a message arrives in the message queue, or the long poll times out.
- As such, long polling can save you money.



Udemy

Summary

SQS

SQS Exam Tips



A CLOUD GURU

- Visibility Timeout
 - Default is 30 seconds - increase if your task takes >30 seconds to complete
 - Max 12 hours
- Short Polling - returned immediately even if no messages are in the queue
- Long Polling - polls the queue periodically and only returns a response when a message is in the queue or the timeout is reached

Activate Windows
Go to PC settings to activate Windows.

SWF

SIMPLE WORKFLOW SERVICE

SWF



Amazon Simple Workflow Service (Amazon SWF) is a web service that makes it easy to coordinate work across distributed application components. Amazon SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks.

Tasks represent invocations of various processing steps in an application which can be performed by executable code, web service calls, human actions, and scripts.



Activate Windows
Go to PC settings to activate Windows.

SWF Worker

SIMPLE WORKFLOW SERVICE

SWF Workers



A CLOUD GURU

Workers are programs that interact with Amazon SWF to get tasks, process received tasks, and return the results.



Activate Windows
Go to PC settings to activate Windows.



SWF Worker & Deciders

SIMPLE WORKFLOW SERVICE

SWF Workers & Deciders



A CLOUD GURU

The workers and the decider can run on cloud infrastructure, such as Amazon EC2, or on machines behind firewalls. Amazon SWF brokers the interactions between workers and the decider. It allows the decider to get consistent views into the progress of tasks and to initiate new tasks in an ongoing manner.

At the same time, Amazon SWF stores tasks, assigns them to workers when they are ready, and monitors their progress. It ensures that a task is assigned only once and is never duplicated. Since Amazon SWF maintains the application's state durably, workers and deciders don't have to keep track of execution state. They can run independently, and scale quickly.

Activate Windows
Go to PC settings to activate Windows.



SWF Domains

SIMPLE WORKFLOW SERVICE

SWF Domains



A CLOUD GURU

Your workflow and activity types and the workflow execution itself are all scoped to a domain. Domains isolate a set of types, executions, and task lists from others within the same account.

You can register a domain by using the AWS Management Console or by using the RegisterDomain action in the Amazon SWF API.



Activate Windows
Go to PC settings to activate Windows.



SWF vs SQS

SIMPLE WORKFLOW SERVICE

SWF vs SQS



A CLOUD GURU

- Amazon SWF presents a task-oriented API, whereas Amazon SQS offers a message-oriented API.
- Amazon SWF ensures that a task is assigned only once and is never duplicated. With Amazon SQS, you need to handle duplicated messages and may also need to ensure that a message is processed only once.
- Amazon SWF keeps track of all the tasks and events in an application. With Amazon SQS, you need to implement your own application-level tracking, especially if your application uses multiple queues.



Activate Windows
Go to PC settings to activate Windows.



SNS

SNS

What is SNS?



A CLOUD GURU

Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud. It provides developers with a highly scalable, flexible, and cost-effective capability to publish messages from an application and immediately deliver them to subscribers or other applications.

Activate Windows
Go to PC settings to activate Windows.

udemy

SNS

SNS

What is SNS?



A CLOUD GURU

Besides pushing cloud notifications directly to mobile devices, Amazon SNS can also deliver notifications by SMS text message or email, to Amazon Simple Queue Service (SQS) queues, or to any HTTP endpoint. SNS notifications can also trigger Lambda functions. When a message is published to an SNS topic that has a Lambda function subscribed to it, the Lambda function is invoked with the payload of the published message. The Lambda function receives the message payload as an input parameter and can manipulate the information in the message, publish the message to other SNS topics, or send the message to other AWS services.

Activate Windows
Go to PC settings to activate Windows.

udemy

SNS

SNS

What is SNS?



A CLOUD GURU

SNS allows you to group multiple recipients using topics. A topic is an “access point” for allowing recipients to dynamically subscribe for identical copies of the same notification. One topic can support deliveries to multiple endpoint types -- for example, you can group together iOS, Android and SMS recipients. When you publish once to a topic, SNS delivers appropriately formatted copies of your message to each subscriber.

Activate Windows
Go to PC settings to activate Windows.

udemy

Benefits

SNS

SNS Benefits



A CLOUD GURU

- Instantaneous, push-based delivery (no polling)
- Simple APIs and easy integration with applications
- Flexible message delivery over multiple transport protocols
- Inexpensive, pay-as-you-go model with no up-front costs
- Web-based AWS Management Console offers the simplicity of a point-and-click interface

Activate Windows
Go to PC settings to activate Windows.

udemy

Pricing

SNS

SNS Pricing



A CLOUD GURU

- Users pay \$0.50 per 1 million Amazon SNS Requests
- \$0.06 per 100,000 Notification deliveries over HTTP
- \$0.75 per 100 Notification deliveries over SMS
- \$2.00 per 100,000 Notification deliveries over Email

Activate Windows
Go to PC settings to activate Windows.

udemy

Elastic Transcoder

Elastic Transcoder

What is Elastic Transcoder?



A CLOUD GURU

Media Transcoder in the cloud.

Convert media files from their original source format in to different formats that will play on smartphones, tablets, PC's etc.

Provides transcoding presets for popular output formats, which means that you don't need to guess about which settings work best on particular devices.

Pay based on the minutes that you transcode and the resolution at which you transcode.

Activate Windows
Go to PC settings to activate Windows.

udemy

API Gateway

API Gateway 101

What is API Gateway?



A CLOUD GURU

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as applications running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.

Activate Windows
Go to PC settings to activate Windows.

udemy

API Caching

API Gateway 101



What is API Caching?

You can enable API caching in Amazon API Gateway to cache your endpoint's response. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of the requests to your API. When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint.

Activate Windows
Go to PC settings to activate Windows.

udemy

Features

API Gateway

What can API Gateway Do?



A CLOUD GURU

- Low Cost & Efficient
- Scales Effortlessly
- You can Throttle Requests to prevent attacks
- Connect to Cloudwatch to log all requests

Activate Windows
Go to PC settings to activate Windows.

udemy

Same Origin Policy

API Gateway

Same Origin Policy



A CLOUD GURU

In computing, the same-origin policy is an important concept in the web application security model. Under the policy, a web browser permits scripts contained in a first web page to access data in a second web page, but only if both web pages have the same origin.

Activate Windows
Go to PC settings to activate Windows.

udemy

CORS

API Gateway

Cross-Origin Resource Sharing (CORS)



A CLOUD GURU

CORS is one way the server at the other end (not the client code in the browser) can relax the same-origin policy.

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the first resource was served.

Error - “Origin policy cannot be read at the remote resource?”. You need to enable CORS on API Gateway.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

API Gateway

Exam Tips



A CLOUD GURU

- Remember what API Gateway is at a high level
- API Gateway has caching capabilities to increase performance
- API Gateway is low cost and scales automatically
- You can throttle API Gateway to prevent attacks
- You can log results to CloudWatch
- If you are using Javascript/AJAX that uses multiple domains with API Gateway, ensure that you have enabled CORS on API Gateway

Activate Windows
Go to PC settings to activate Windows.

udemy

Streaming Data

Kinesis 101



A CLOUD GURU

What is streaming data

Streaming Data is data that is generated continuously by thousands of data sources, which typically send in the data records simultaneously, and in small sizes (order of Kilobytes).

- Purchases from online stores (think amazon.com)
- Stock Prices
- Game data (as the gamer plays)
- Social network data
- Geospatial data (think uber.com)

Activate Windows
Go to PC settings to activate Windows.

udemy

Kinesis

Kinesis 101

What is Kinesis



A CLOUD GURU

Amazon Kinesis is a platform on AWS to send your streaming data too. Kinesis makes it easy to load and analyze streaming data, and also providing the ability for you to build your own custom applications for your business needs.

- Kinesis Streams



- Kinesis Firehose



- Kinesis Analytics



Activate Windows
Go to PC settings to activate Windows.

udemy

Streams

Kinesis 101



Kinesis Streams

- Kinesis Streams consist of shards
- 5 transactions per second for reads, up to a maximum total data read rate of 2 MB per second and up to 1,000 records per second for writes, up to a maximum total data write rate of 1 MB per second (including partition keys).
- The data capacity of your stream is a function of the number of shards that you specify for the stream. The total capacity of the stream is the sum of the capacities of its shards.

Activate Windows
Go to PC settings to activate Windows.

udemy

Summary

Kinesis 101

Exam Tips



A CLOUD GURU

- Know the difference between Kinesis Streams and Kinesis Firehose. You will be given scenario questions and you must choose the most relevant service.
- Understand what Kinesis Analytics is.

Activate Windows
Go to PC settings to activate Windows.

udemy

SWF Actors



- Workflow Starters - An application that can initiate (start) a workflow. Could be your e-commerce website when placing an order or a mobile app searching for bus times.
- Deciders - Control the flow of activity tasks in a workflow execution. If something has finished in a workflow (or fails) a Decider decides what to do next.
- Activity Workers - Carry out the activity tasks

Activate Windows
Go to PC settings to activate Windows.

OpsWorks

ADDITIONAL EXAM TIPS

OpsWorks



A CLOUD GURU

- Orchestration Service that uses Chef
- Chef consists of recipes to maintain a consistent state
- Look for the term “chef” or “recipes” or “cook books” and think OpsWorks



Activate Windows
Go to PC settings to activate Windows.

AWS Organizations

AWS Organizations & Consolidated Billing

What is AWS Organizations?



A CLOUD GURU

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

Available in two feature sets;

- Consolidated Billing
- All Features

Activate Windows
Go to PC settings to activate Windows.

udemy

Tags

TAGGING & RESOURCE GROUPS

What Are Tags?

A CLOUD GURU

- Key Value Pairs attached to AWS resources
- Metadata (data about data)
- Tags can sometimes be inherited
 - Autoscaling, CloudFormation and Elastic Beanstalk can create other resources

Activate Windows
Go to PC settings to activate Windows.

udemy

Resource groups

TAGGING & RESOURCE GROUPS

What Are Resource Groups?

A CLOUD GURU



Resource groups make it easy to group your resources using the tags that are assigned to them. You can group resources that share one or more tags.

Resource groups contain information such as;

- Region
- Name
- Health Checks

Specific information

- For EC2 - Public & Private IP Addresses
- For ELB - Port Configurations
- For RDS - Database Engine etc

Activate Windows
Go to PC settings to activate Windows.

udemy

Direct Connect

DIRECT CONNECT

Direct Connect



A CLOUD GURU

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Activate Windows
Go to PC settings to activate Windows.

udemy

STS

SECURITY TOKEN SERVICE (STS)

Security Token Service (STS)



A CLOUD GURU

Grants users limited and temporary access to AWS resources. Users can come from three sources;

Federation (typically Active Directory)

- Uses Security Assertion Markup Language (SAML)
- Grants temporary access based off the users Active Directory credentials. Does not need to be a user in IAM
- Single sign on allows users to log in to AWS console without assigning IAM credentials
- Federation with Mobile Apps
 - Use Facebook/Amazon/Google or other OpenID providers to log in
- Cross Account Access
 - Lets users from one AWS account access resources in another

Activate Windows
Go to PC settings to activate Windows.

udemy

STS Key Terms

SECURITY TOKEN SERVICE (STS)

Understanding The Key Terms



A CLOUD GURU

- Federation
 - Combining or joining a list of users in one domain (such as IAM) with a list of users in another domain (such as Active Directory, Facebook etc)
- Identity Broker
 - A service that allows you to take an identity from point A and join it (federate it) to point B
- Identity Store
 - Services like Active Directory, Facebook, Google etc.
- Identities
 - A user of a service like Facebook etc.

Activate Windows
Go to PC settings to activate Windows.

udemy

Workspaces

Workspaces 101

What is Workspaces?



A CLOUD GURU

It's basically VDI. A WorkSpace is a cloud-based replacement for a traditional desktop. A WorkSpace is available as a bundle of compute resources, storage space, and software application access that allow a user to perform day-to-day tasks just like using a traditional desktop. A user can connect to a WorkSpace from any supported device (PC, Mac, Chromebook, iPad, Kindle Fire, or Android tablets) using a free Amazon WorkSpaces client application and credentials set up by an administrator, or their existing Active Directory credentials. If Amazon WorkSpaces is integrated with an existing Active Directory domain.

Activate Windows
Go to PC Settings to activate Windows.

udemy

Docker Components

DevOps Core Concepts

Docker Components



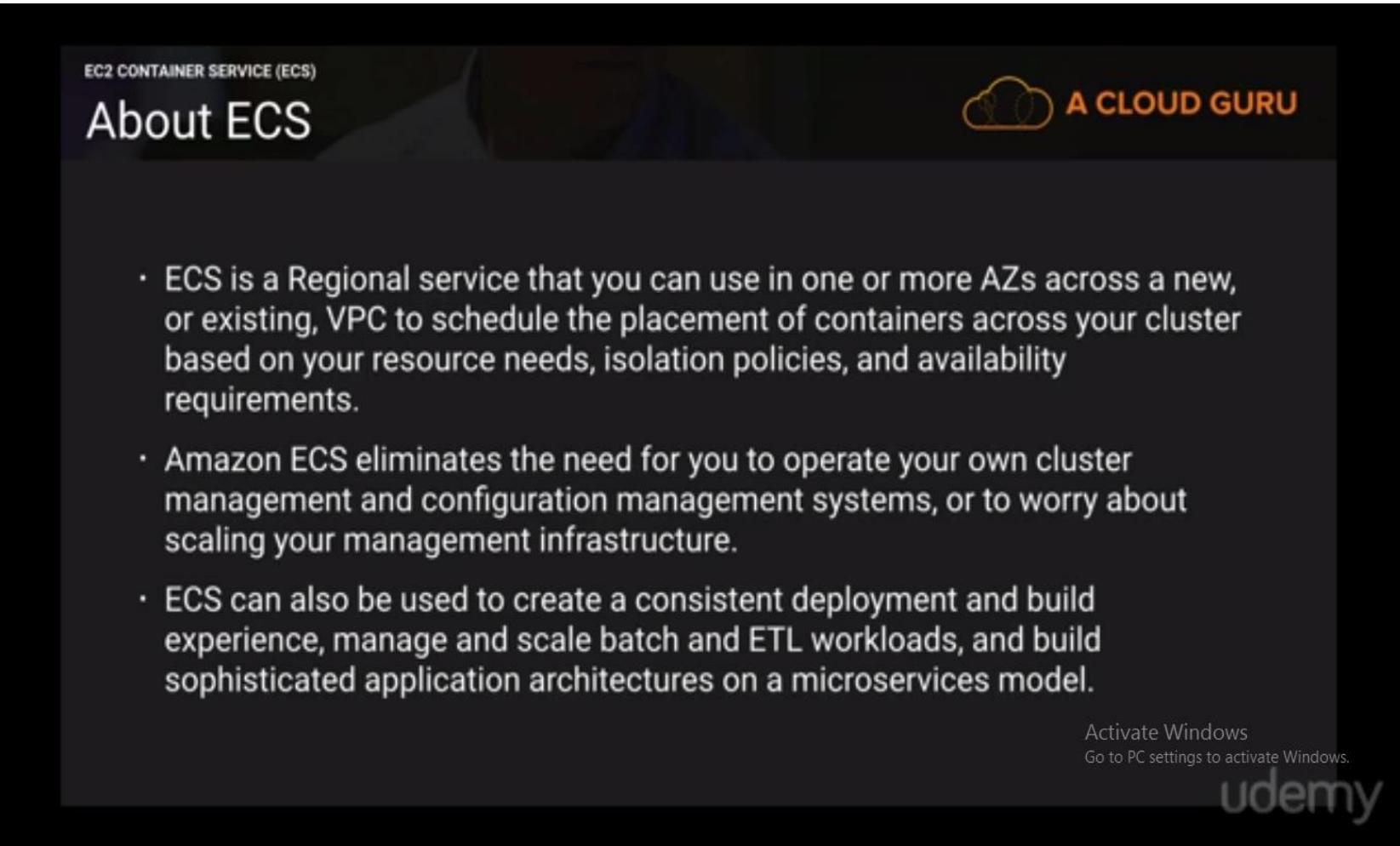
A CLOUD GURU

- Docker Image
- Docker Container
- Layers / Union File System
- DockerFile
- Docker Daemon/ Engine
- Docker Client
- Docker Registries / Docker Hub

Activate Windows
Go to PC settings to activate Windows.

udemy

ECS



The screenshot shows a dark-themed web page for the EC2 Container Service (ECS). At the top left, it says "EC2 CONTAINER SERVICE (ECS)". In the top right corner, there is a logo consisting of a stylized cloud icon with three dots and the text "A CLOUD GURU". The main content area has a dark background with white text. It features the heading "About ECS" and a bulleted list of benefits.

About ECS

- ECS is a Regional service that you can use in one or more AZs across a new, or existing, VPC to schedule the placement of containers across your cluster based on your resource needs, isolation policies, and availability requirements.
- Amazon ECS eliminates the need for you to operate your own cluster management and configuration management systems, or to worry about scaling your management infrastructure.
- ECS can also be used to create a consistent deployment and build experience, manage and scale batch and ETL workloads, and build sophisticated application architectures on a microservices model.

Activate Windows
Go to PC settings to activate Windows.

udemy

ECS Limits

EC2 CONTAINER SERVICE (ECS)

ECS Limits



A CLOUD GURU

- Soft Limits:
 - Clusters per Region (default = 1000)
 - Instances per Cluster (default = 1000)
 - Services per Cluster (default = 500)
- Hard Limits
 - One Load Balancer per Service
 - 1000 Tasks per Service (the "desired count")
 - Max. 10 Containers per Task Definition
 - Max. 10 Tasks per instance (host)

Activate Windows
Go to PC settings to activate Windows.

udemy

ECS Summary

EC2 CONTAINER SERVICE (ECS)

ECS Exam Tips

A CLOUD GURU

- ECS - Amazon's managed EC2 container service. Allows you to manage Docker containers on a cluster of EC2 instances
- Containers are a method of operating system virtualization that allow you to run an application and its dependencies in resource-isolated processes.
- Containers are created from a read-only template called an Image.
- An Image is a read-only template with instructions for creating a Docker container.
- Images are stored in a Registry, such as DockerHub or AWS ECR.
- Amazon EC2 Container Registry (Amazon ECR) is a managed AWS Docker registry service

Activate Windows
Go to PC settings to activate Windows.

udemy