

Participant Workbook

Instructions

This is the participant workbook you can use throughout this course. You will find valuable terminology and acronym definitions explained here. There is space for you to take notes and even additional links for you to dive deeper into the information you will learn in class today.

Table of Contents

Module 1: Introduction to Amazon Web Services (AWS)	2
Module 2: Global Infrastructure and Reliability	6
Module 3: Networking	8
Module 4: Object Storage	14

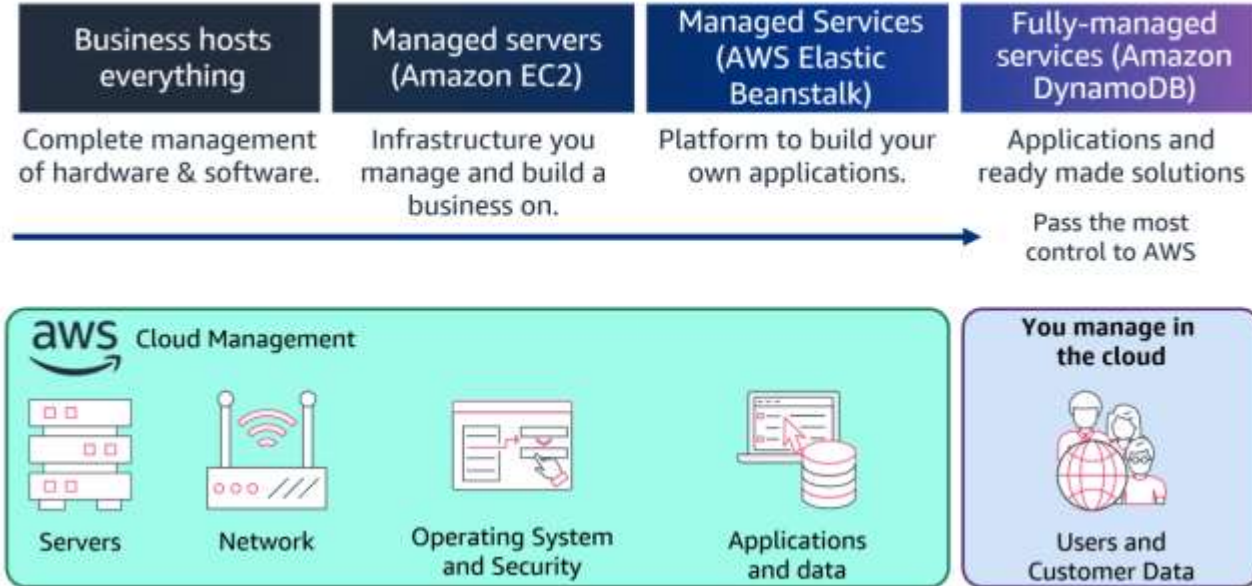
Module 1: Introduction to Amazon Web Services (AWS)

Helpful Terms

Term	Definition
Amazon Web Services (AWS)	Is a cloud services platform. Simply, it provides cloud services to both individuals and businesses.
Personal Computer (PC)	A small-scale computer made to be used by an individual. - Laptop or desktops
Internet Service Provider (ISP)	A company that provides access to the Internet.
Cloud Service Provider (CSP)	A company that provides cloud-based services such as platform, infrastructure, application, or storage. - AWS, Google, Azure
Information Technology (IT) or Information Systems (IS)	Often used to refer to the department in a company that is responsible for installing and maintaining computer hardware and software.
Device	A piece of hardware used to connect you to the applications, files, or services you need. - Cell phone, laptop, tablet, PC, or server.
Client	A device that gathers information and directions from another device. - Most commonly a laptop or PC. Can be a cell phone or tablet.
Server	A very powerful computer that provides access to applications, files, and services. - Print server, file server, network server, or application server.
On-premises / On-prem	IT hardware and software applications hosted where the business operates or in a physical data center.
Data Center	A facility dedicated to supporting a very large number of powerful servers used by organizations for remote storage and to prevent failures (fault tolerance).
Deploy	A term used to describe the process of installing and configuring a new virtual server or application. This can be used in the context of on-prem or cloud environments. - Synonymous with launch
Cloud-native	This describes an application or feature that was designed specifically to run in the cloud.

Topic A: Understanding networks

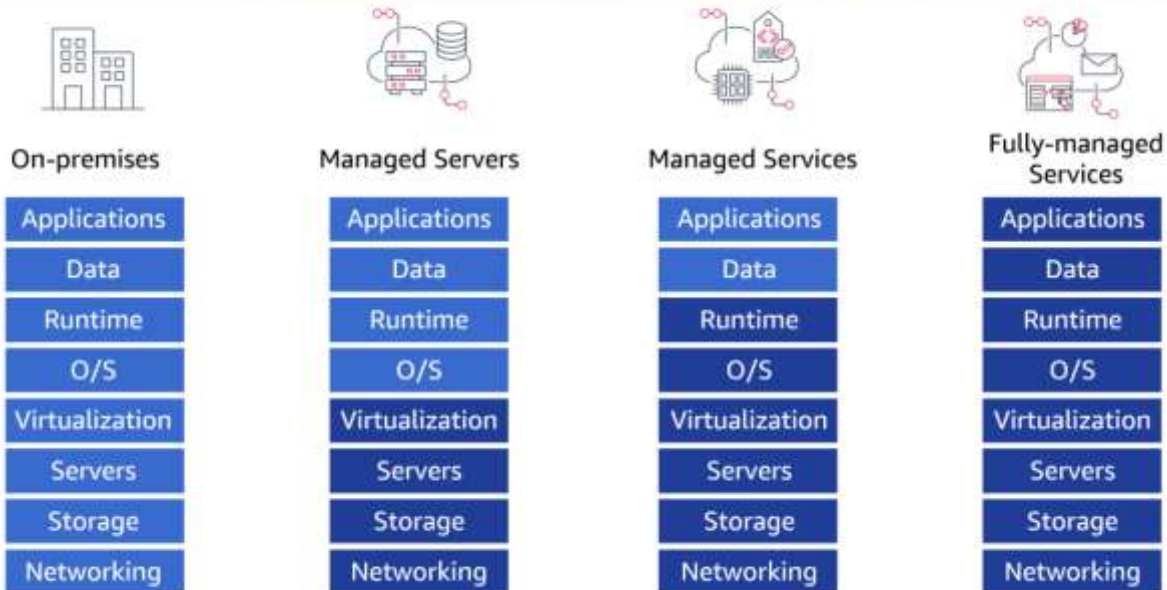
Shared infrastructure model



Notes:

Cloud computing models

Cloud computing models



For more information on cloud computing models, see:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/types-of-cloud-computing.html>

Notes:

Topic B: Cloud Computing Benefits

Six Benefits of cloud computing

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

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

Notes:

Module 2: Global Infrastructure and Reliability

Helpful Terms

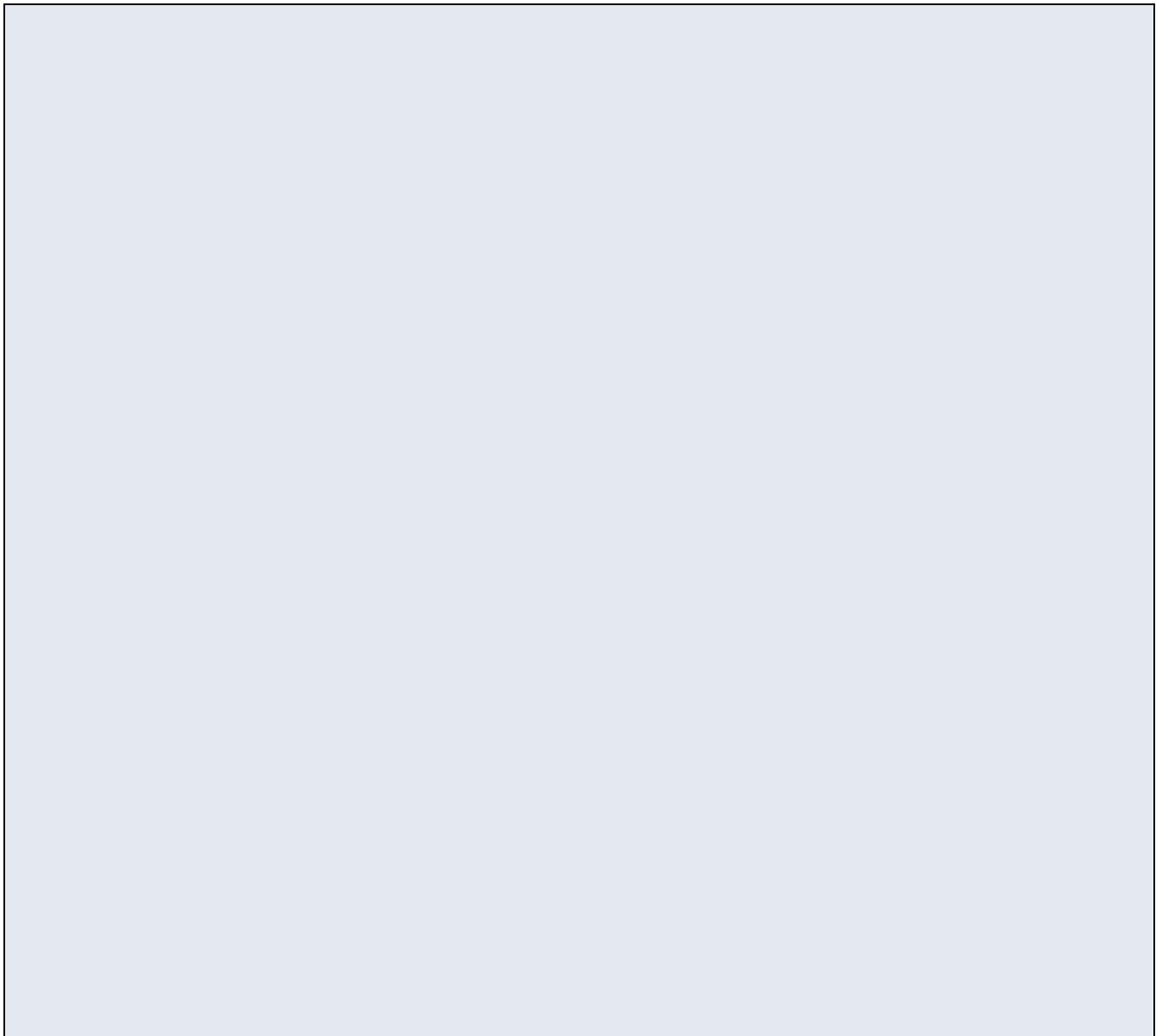
Term	Definition
Availability Zone (AZ)	A distinct location within a Region that's insulated from failures in other Availability Zones.
Region	A named set of AWS resources that's in the same geographical area.
Regional service	Regional services only require the assignment of a Region.
Zonal service	Zonal services require the assignment of a Region and an AZ.
Elasticity	The ability of a cloud service to dynamically grow and shrink based on demands of a workload. - <i>Amazon Auto Scaling</i>
Scalability	The ability of a cloud service to grow manually as the demands of a workload change over time. - <i>Horizontal or vertical scaling mechanisms</i>
Resiliency	Indicates the ability of a system to both recover and continue operating in the event of a disruption. - <i>Clustered servers, redundant workloads, failover mechanisms.</i>
Durability	The ability of a cloud service to ensure long term data stability. - <i>Data durability of Amazon S3 99.999999999%</i>
Availability	The ability of a cloud service to be available when it is needed. - <i>Deploying into multiple AZs and/or Region.</i>

Notes:

Topic A: Global Infrastructure

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer you the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. For the latest information on the AWS Cloud Availability Zones and AWS Regions, refer to [AWS Global Infrastructure](#).

Notes:

A large, empty rectangular box with a light blue background and a thin black border, intended for taking notes.

Module 3: Networking

Helpful Terms

Term	Definition
Operating System (OS)	A program that communicates between the hardware and software supported by that system.
Domain Name System (DNS)	A naming system used to identify servers reachable over the internet or private IP networks.
Classless inter-domain routing (CIDR)	A method for allocating IPv4 addresses using variable length IP addresses.
Classful routing	A method for allocating IPv4 addresses using IP addresses classes.
Hypertext Transfer Protocol (HTTP)	This is a protocol used to transmit data over the internet.
Hypertext Transfer Protocol Secured (HTTPS)	This is a protocol used to transmit data over the internet using TLS security.
Internet Protocol (IP)	This is a protocol that defines addressing on a computer network. - <i>IPv4, IPv6</i>
Access Control List (ACL)	A virtual firewall that controls inbound and outbound traffic at the subnet level.
Data packets	A unit of data made into a small package for travel along a network path.
Protocol	A set of rules that determine how data is transmitted between devices in the same network. - <i>HTTP, SMTP, SSL.</i>
Port / Port number	A Port is a logical construct that identifies a specific process or type of network service or protocol. A well-known Port number is the aligned with a specific transport. - <i>Port 80 HTTP; Port 443 HTTPS; port 53 DNS.</i>
IP address	A unique number that identifies a device on the internet or local network. Addresses are made up of 4 numbers with values of 0 – 255. - <i>127.0.0.1; 169.254.0.1; 176.16.0.1; 192.168.0.1;</i>
Routing	The process of selecting a path across one or more networks and transmitting data from the source network to the destination network.
Subnet / Subnetting / Subnet mask	A logical subdivision on an IP network. Subnetting is the process of creating the subdivision. This is enforced using a subnet mask.
Switch	A device that forwards data packets between devices in a single network. It is not aware of network addressing.
Router	A device that forwards data packets between networks.
Gateway	A device or node that connects two different networks by transmitting communications from one network to another.

Topic A: Amazon Virtual Private Cloud

What is Amazon VPC?

With Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated 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.

For more information see <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>.

IP addressing for your VPCs and subnets

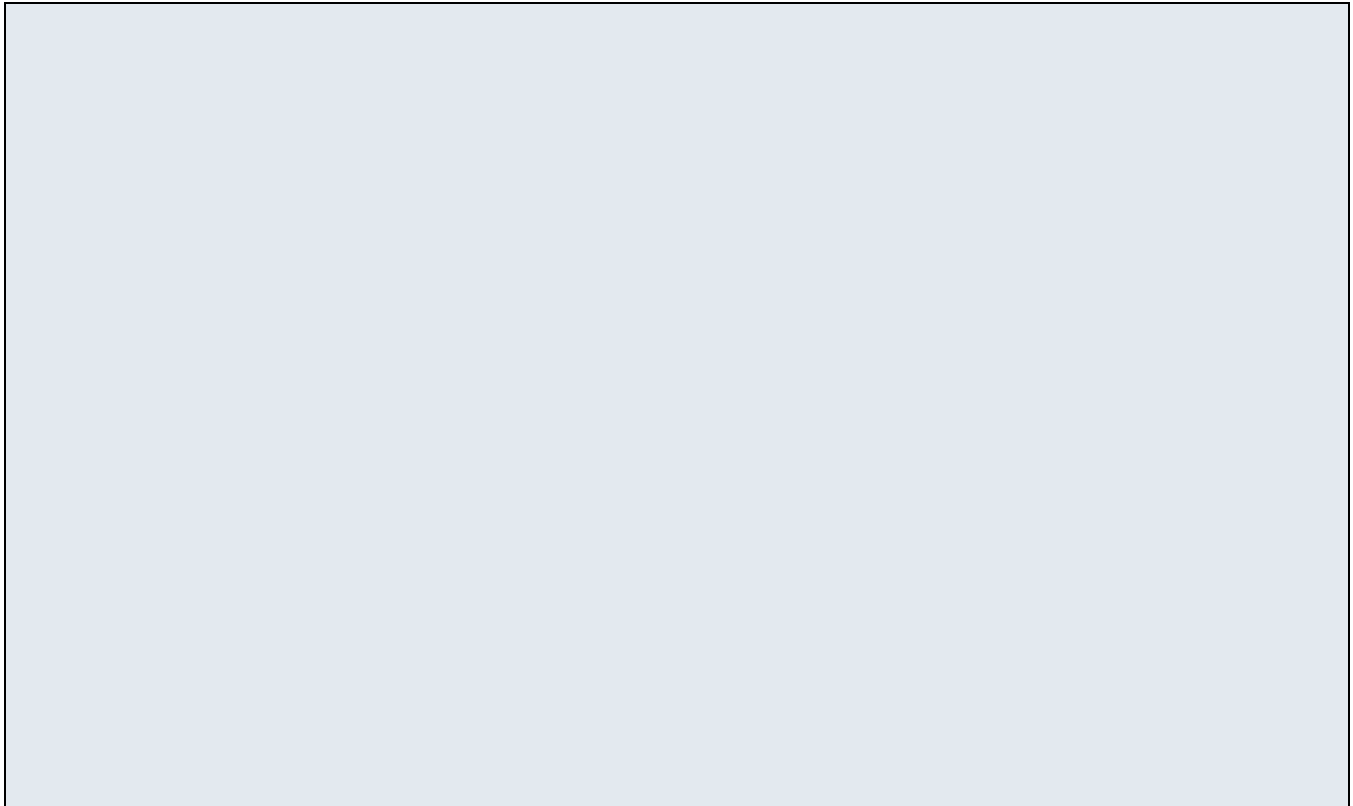
For more information see <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>.

Subnets for your VPC.

A *subnet* is a range of IP addresses in your VPC. You can create AWS resources, such as EC2 instances, in specific subnets.

For more information see <https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html>.

Notes:

A large, empty rectangular box with a thin black border, intended for taking notes.

Topic B: Network access control lists and security groups

Subnets for your VPC

A *subnet* is a range of IP addresses in your VPC. You can create AWS resources, such as EC2 instances, in specific subnets.

Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone.

Connect to the internet using an internet gateway

An internet gateway enables resources in your public subnets (such as EC2 instances) to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address. For example, an internet gateway enables you to connect to an EC2 instance in AWS using your local computer.

Public and private subnets

If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.

Tasks

- [Create a subnet](#)
- [Create and attach an internet gateway](#)
- [Create a custom route table](#)
- [Create a security group for internet access](#)

Notes:

Connect your VPC to remote networks

You can connect your VPC to remote networks and users using the following VPN connectivity options.

Connectivity option	Description
AWS Site-to-Site VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the Site-to-Site VPN connection, a virtual private gateway or transit gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your <i>customer gateway device</i> on the remote side of the Site-to-Site VPN connection. For more information, see the AWS Site-to-Site VPN User Guide .
AWS Client VPN	AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources or your on-premises network. With AWS Client VPN, you configure an endpoint to which your users can connect to establish a secure TLS VPN session. This enables clients to access resources in AWS or on-premises from any location using an OpenVPN-based VPN client. For more information, see the AWS Client VPN Administrator Guide .
AWS VPN CloudHub	If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS Site-to-Site VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing secure communication between sites using VPN CloudHub in the <i>AWS Site-to-Site VPN User Guide</i> .
Third party software VPN appliance	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third-party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open-source communities. Find third party software VPN appliances on the AWS Marketplace .

Notes:

Network Access Control Lists (ACLs)

A *network access control list (ACL)* allows or denies specific inbound or outbound traffic at the subnet level. You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are similar to the rules for your security groups in order to add an additional layer of security to your VPC.

- 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.
- A network ACL has inbound rules and outbound rules. Each rule can either allow or deny traffic. Each rule has a number from 1 to 32766. We evaluate the rules in order, starting with the lowest numbered rule, when deciding whether allow or deny traffic. If the traffic matches a rule, the rule is applied and we do not evaluate any additional rules. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules later on, if needed.
- We evaluate the network ACL rules when traffic enters and leaves the subnet, not as it is routed within a subnet.

For more information on network ACLs see <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>.

Notes:

Security groups

A *security group* controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance. You can associate a security group only with resources in the VPC for which it is created.

When you create a VPC, it comes with a default security group. You can create additional security groups for each VPC.

- Security groups are stateful. For example, if you send a request from an instance, the response traffic for that request is allowed to reach the instance regardless of the inbound security group rules. Responses to allowed inbound traffic are allowed to leave the instance, regardless of the outbound rules.
- Security groups do not filter traffic destined to and from the following:
 - Amazon Domain Name Services (DNS)
 - Amazon Dynamic Host Configuration Protocol (DHCP)
 - Amazon EC2 instance metadata
 - Amazon ECS task metadata endpoints
 - License activation for Windows instances
 - Amazon Time Sync Service
 - Reserved IP addresses used by the default VPC router

For more information on security groups see <https://docs.aws.amazon.com/vpc/latest/userguide/security-groups.html>.

Notes:

Module 4: Object Storage

Topic A: Object storage

Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

For more information on Amazon S3 features, see <https://aws.amazon.com/s3/features/>.

Amazon S3 storage classes

Amazon S3 offers a range of storage classes that you can choose from based on the data access, resiliency, and cost requirements of your workloads. S3 storage classes are purpose-built to provide the lowest cost storage for different access patterns. S3 storage classes are ideal for virtually any use case, including those with demanding performance needs, data residency requirements, unknown or changing access patterns, or archival storage.

For more information on Amazon S3 storage classes, see <https://aws.amazon.com/s3/storage-classes/>.

AWS Snow Family

Snow Family devices have computing resources to collect and process data at the edge. Devices can support Amazon EC2 instances, AWS IoT Greengrass functions, and Kubernetes deployments on Amazon EKS Anywhere. Applications can work with Snow Family devices so you can easily use Snow devices with your existing on-premises servers and file-based applications.

AWS Snow devices feature a Trusted Platform Module (TPM) that provides a hardware root of trust. Each device is inspected after each use to ensure the integrity of the device and helps preserve the confidentiality of your data. All data moved to AWS Snow Family devices is automatically encrypted with 256-bit encryption keys that are managed by the AWS Key Management Service (KMS). Encryption keys are never stored on the device so your data stays secure during transit.

Three physical devices are available.

- AWS Snowcone
- AWS Snowball
- AWS Snowmobile

Snow family feature comparison

	AWS SNOWCONE	AWS SNOWBALL EDGE STORAGE OPTIMIZED 80 TB	AWS SNOWBALL EDGE STORAGE OPTIMIZED 210 TB	AWS SNOWBALL EDGE COMPUTE OPTIMIZED
Usable HDD Storage	8 TB	80 TB HDD	N/A	N/A
Usable SSD Storage	14 TB	1 TB	210 TB NVMe	28 TB
Usable vCPUs	2 vCPUs	40 vCPUs	104vCPUs	104 vCPUs
Usable Memory	4 GB	80 GB	416 GB	416 GB
Device Size	9in x 6in x 3in 227 mm x 148.6 mm x 82.65 mm	548 mm x 320 mm x 501 mm	548 mm x 320 mm x 501 mm	548 mm x 320 mm x 501 mm
Device Weight	4.5 lbs. (2.1 kg)	49.7 lbs. (22.3 kg)	49.7 lbs. (22.3 kg)	49.7 lbs. (22.3 kg)
Storage Clustering	No	No	No	Yes, 3-16 nodes
256-bit Encryption	Yes	Yes	Yes	Yes
HIPAA Compliant	No	Yes, eligible	Yes, eligible	Yes, eligible

Notes: