AWS Certified Solutions Architect - Associate

Week 1 Content Review

September Accelerator Cohort

aws training and certification

Thank you for joining!

AWS Certified Solutions Architect – Associate (SAA) Week 1 Review

- This session will be recorded
- Please stay on mute
- Submit questions via chat function
- If you have other questions please contact mpatraininghelp@amazon.com

Kevin Zook
Enablement Manager

About the Exam

aws training and certification

AWS Certified Solutions Architect - Associate

About the Exam

- 130 minutes
- 65 Questions
  - *50 questions count to your score*
  - Scored 100 to 1000 (720+ pass)
- $150/voucher
- Multiple Response & Individual response questions
- In-Person & Remote proctoring available

AWS Certified Solutions Architect - Associate

Key Exam Topics

Domains Covered:	% of Exam
Domain 1: Design Resilient Architectures	30%
Domain 2: Design High-Performing Architectures	28%
Domain 3: Design Secure Applications and Architectures	24%
Domain 4: Design Cost-Optimized Architectures	18%
Total:	**100%**

AWS Certified Solutions Architect - Associate

Helpful Resources

Training

- AWS Partner Accreditation: Technical
- AWS Well Architected Labs

Kinda Cool

- https://aws.amazon.com/about-aws/global-infrastructure/

White Papers

- Overview of Amazon Web Services
- AWS Well-Architected Framework
- Management and Governance Lens
- AWS Global Infrastructure
- Shared Responsibility Model
- How AWS Pricing Works
- AWS Architecture Center
- Secure Content Delivery with Amazon CloudFront
- IPv6 on AWS
- Overview of Deployment options on AWS
- Organizing your AWS Environment using multiple accounts

Exam Preparation

- Twitch Power Hours
- Sample Questions
- Schedule an Exam

aws training and certification

AWS Global Infrastructure

aws training and certification

AWS Regions

A Region location around the world where AWS clusters data centers

What's in a Region?

Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ's)

Why are they important?

AWS Regions are totally isolated from each other, creating the greatest possible fault tolerance and stability.

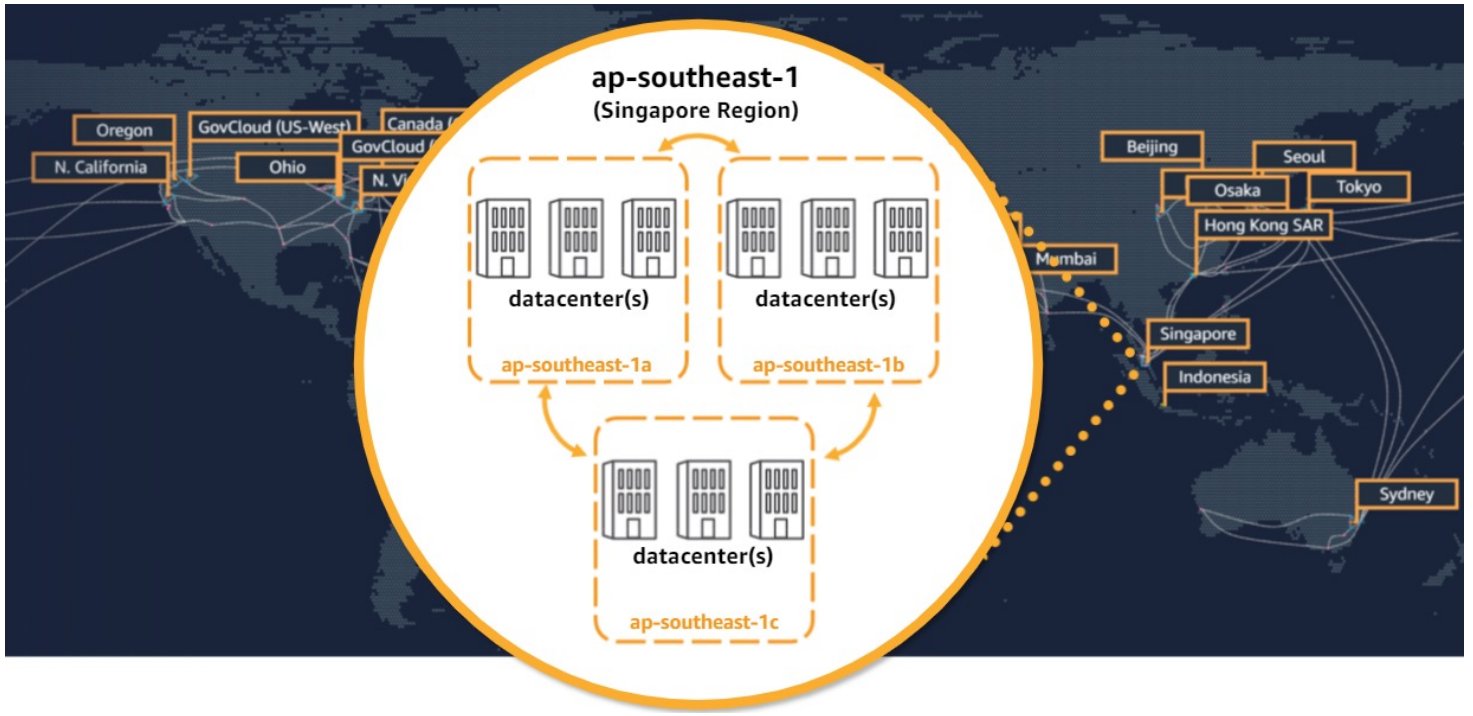
AWS Availability Zones (AZs)

One or more discrete data centers with redundant power, networking, and connectivity located within an AWS Region

Why are they important?

AZs give customers 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.

AZs are connected to each other with fast, private, and secure fiber-optic networking, enabling you to easily architect applications that automatically fail-over between AZs without interruption.



Points of Presence (PoP)

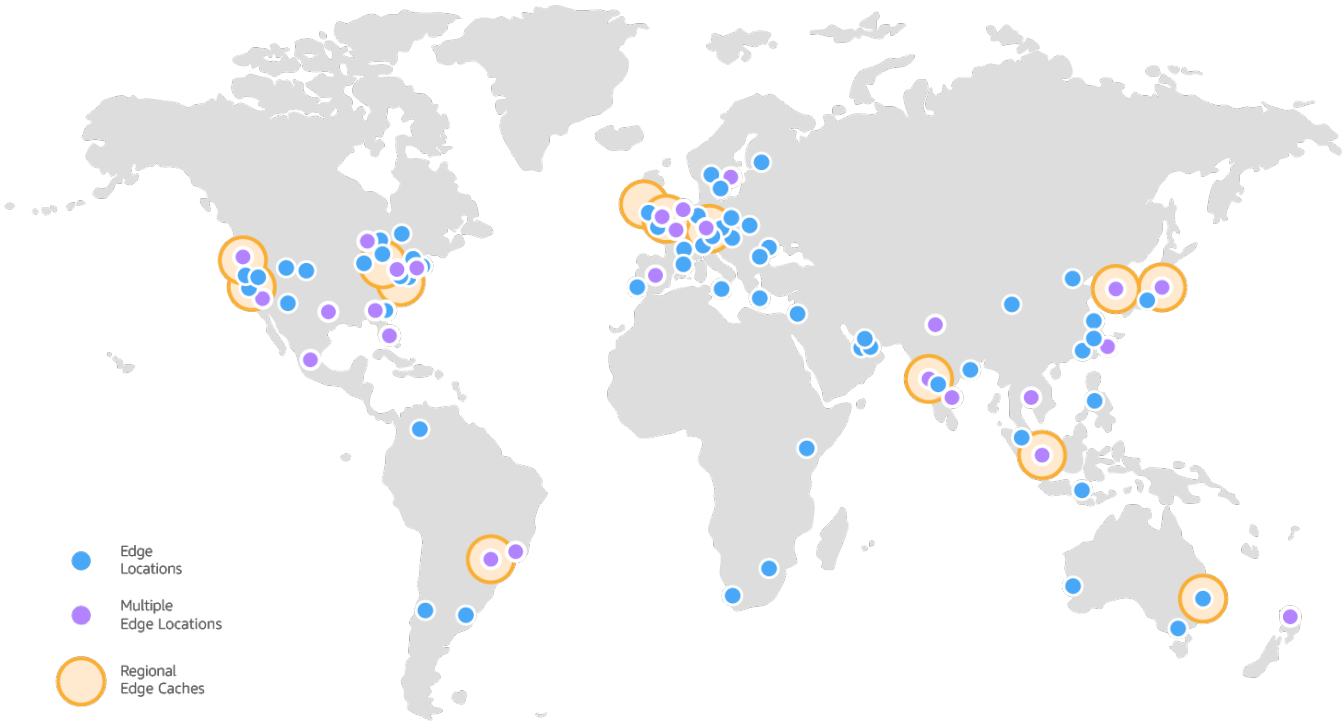
410+ Points of Presences and 13 regional edge caches

What are they?

Smaller endpoints used for hosting cached, frequently accessed, data.

Why are they important?

Points of Presence enable Amazon CloudFront to securely deliver data, videos, applications, and APIs to customers globally with low latency and high transfer speeds, all within the security of the AWS network and a developer-friendly environment.



aws training and certification

Identity and Access Management

aws training and certification

What is IAM?

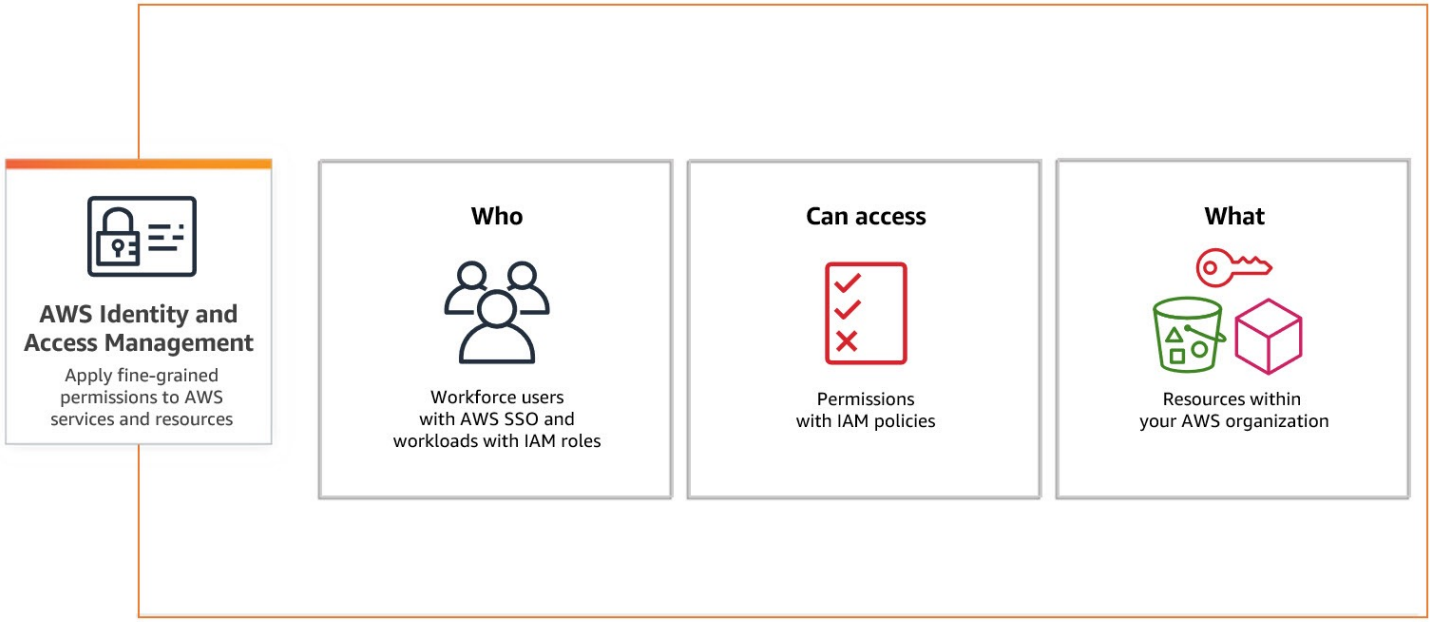
Policies and Technologies used to ensure the appropriate access to technology resources

Overview

AWS IAM provides fine-grained access control across all of AWS. With IAM, you can specify who can access which services and resources, under which conditions.

IAM Policies

IAM Policies allow you to manage permissions for your workforce and systems to ensure leas-privileged access.



What is Least – Privileged?

A core component in AWS Security Best Practices AND in understanding Access

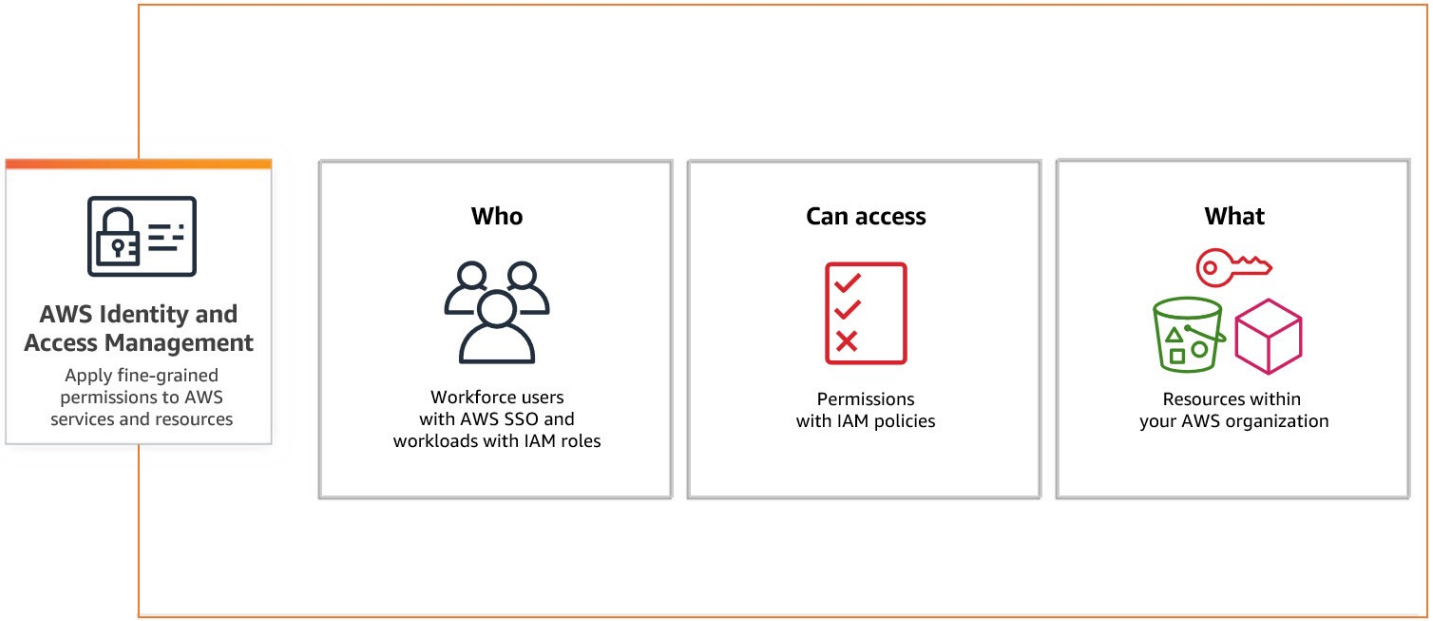
Overview

The principle of Least-Privileged is that a user/resource should be granted the least amount of permissions or privileges needed to complete their job role.

If a user does not need an access right, they should not have that access right

Exam Questions

The exam will sometimes ask you to evaluate permissions / policy documents in response to providing access to a user. These questions are assuming you understand least-privileged.



IAM Users and Groups

The building blocks of AWS Identity and Access Management

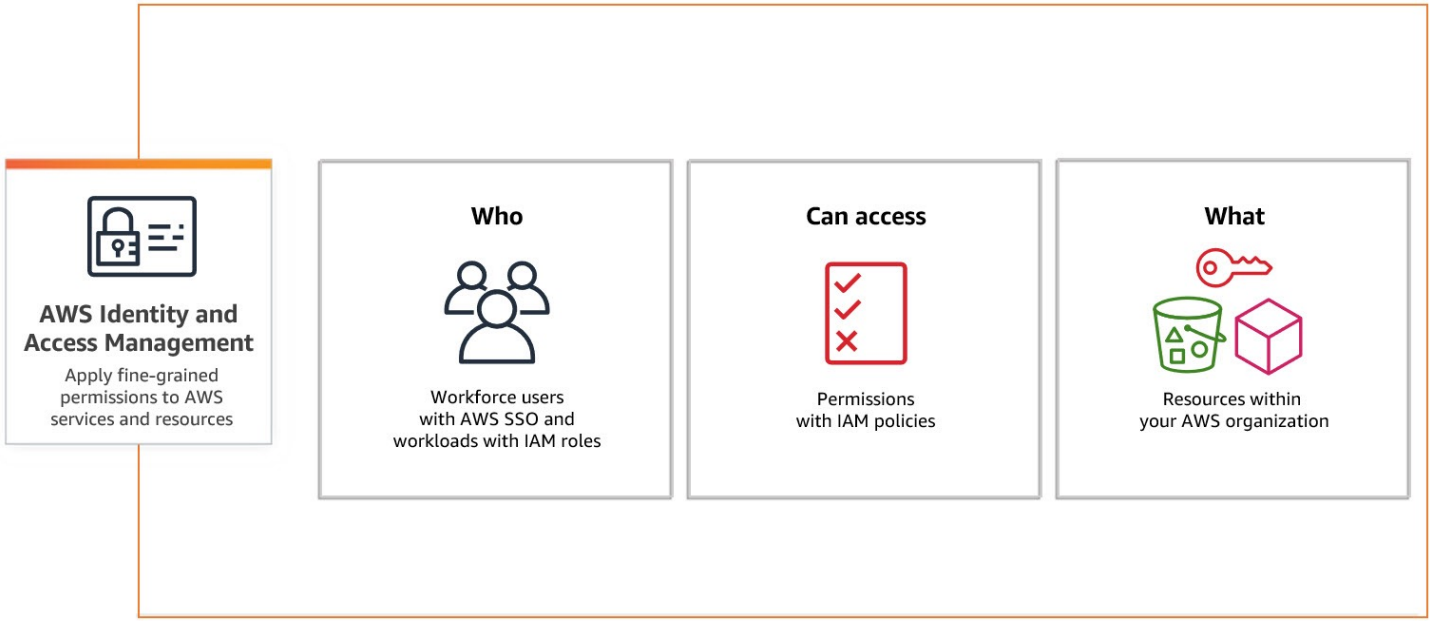
IAM Users

An IAM user is an entity that is created in AWS to represent the person, or application, that uses it to interact with AWS.

IAM Groups

An IAM Group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

Ex: You could have a user group called Admins and give that user group typical administrator permissions.



AWS Organizations (1 of 2)

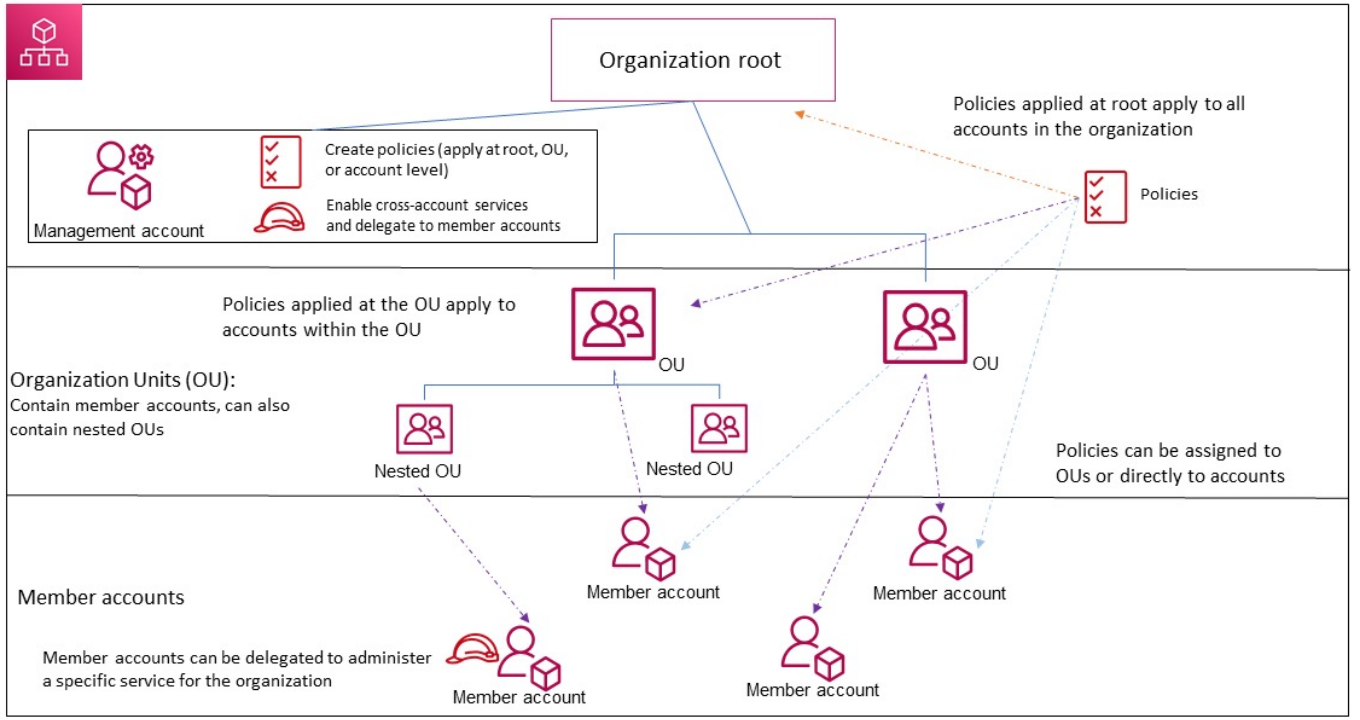
An account management service that enables account consolidation and organization

Purpose

A way to consolidate accounts, assign permissions to OU's, and automate the onboarding of new team members based on job function.

Components

- **Organizations –** an entity created to consolidate your AWS accounts.
- **Root –** Parent container for all the accounts for your organization
- **Organization Unit (OU) –** A container for accounts within a root. An OU can also contain other OU's



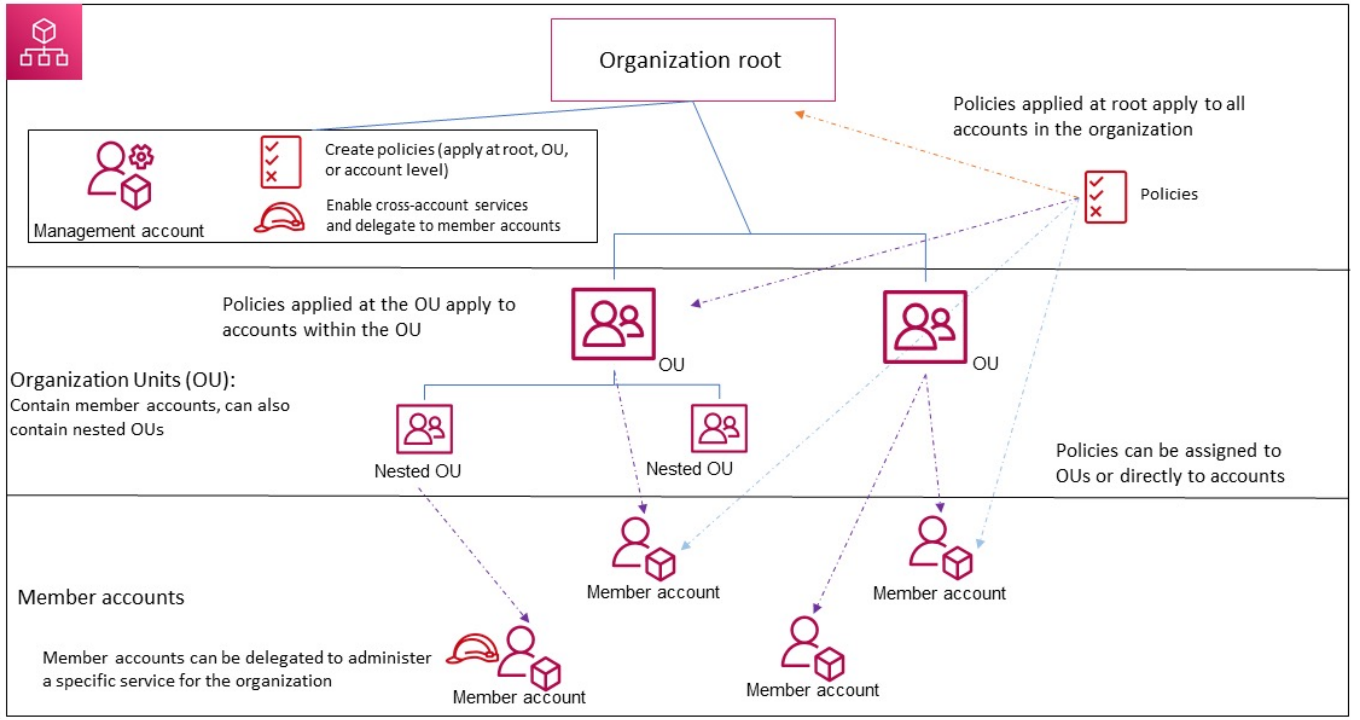
aws training and certification

AWS Organizations (cont. 2/2)

An account management service that enables account consolidation and organization

Components

- **Account –** An account in an organization is a standard AWS account that contains AWS resources and identities.
- **Service Control Policy (SCP) –** A policy that specifies the services and actions that users and roles can use in the accounts that the SCP affects.
- **Tagging –** A best practices for your OU's to keep track of your AWS accounts and resources. This assists with more granular monitoring and logging of your AWS environment.



IAM Policies

aws training and certification

Policy Interpretation Deep Dive!

IAM Policies are the bedrock of strong IAM security. Understanding how the policies work and being able to interpret them is critical for success as an Architect and on the exam

Identity Policies

Identity Policies are IAM policies that are applied to identities. This can include both users as well as roles that users can assume. These are **different** than resource policies.

Implicit vs. Explicit Allow/Deny

The default response to all requests is an **Implicit Deny**. This 'stance' can be overridden by allowing the user access with a permissions policy – this grants the user access because it has been **Explicitly Allowed.** The same process can be done with an **Explicit Deny** policy. This will deny access regardless of the permissions the user might have.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExplicitDenyIfNotTheOwner",
            "Effect": "Deny",
            "Action": [
                "datapipeline:ActivatePipeline",
                "datapipeline:AddTags",
                "datapipeline:DeactivatePipeline",
                "datapipeline:DeletePipeline",
                "datapipeline:DescribeObjects",
                "datapipeline:EvaluateExpression",
                "datapipeline:GetPipelineDefinition",
                "datapipeline:PollForTask",
                "datapipeline:PutPipelineDefinition",
                "datapipeline:QueryObjects",
                "datapipeline:RemoveTags",
                "datapipeline:ReportTaskProgress",
                "datapipeline:ReportTaskRunnerHeartbeat",
                "datapipeline:SetStatus",
                "datapipeline:SetTaskStatus",
                "datapipeline:ValidatePipelineDefinition"
            ],
            "Resource": ["*"],
            "Condition": {
                "StringNotEquals": {"datapipeline:PipelineCreator": "${aws:userid}"}
            }
        }
    ]
}
```

Policy Interpretation Deep Dive!

IAM Policies are the bedrock of strong IAM security. Understanding how the policies work and being able to interpret them is critical for success as an Architect and on the exam

Resource Policies

Unlike an identity-based policy, a resource-based policy specifies WHO (which principle) can access that resource. The principles identified within a resource-based policy include accounts, IAM users, federated users, IAM roles, assumed-role sessions, or AWS services.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/carlossalazar"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::carlossalazar/*",
                "arn:aws:s3:::carlossalazar"
            ]
        }
    ]
}
```

Policy Interpretation Deep Dive!

More practice! What does this permissions policy allow or not allow? What would this policy be applied to?

Policy Interpretation

What is allowed, or not allowed, in the policy shown at right? Are there any specific instances where this might not apply?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableDisableHongKong",
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"account:TargetRegion": "ap-east-1"}
            }
        },
        {
            "Sid": "ViewConsole",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewAccount",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

The Importance of IAM Roles

Roles are a way for users to temporarily gain permissions

What are they?

AWS Roles have the same makeup as an IAM user with the following differences:

- An IAM role does not have long term credentials associated with it. A principle (user, machine, or authenticated identity) assumes the role and inherits permissions assigned to the user.
- Temporary access is granted using tokens (STS). Token expiration reduces the risks associated with credentials leaking or being reused.
- An IAM role has a trust policy that defines which conditions must be met to allow other principles to assume it.

When should they be used?

In general, there are four scenarios where IAM roles might be used:

1. One AWS service accesses another AWS Service
2. One AWS account accesses another AWS account
3. A third-party web identity needs access (i.e Google, Facebook, or Cognito)
4. Authentication using SAML2.0 federation (enables SSO)

Amazon Resource Names (ARN)

A way to uniquely identify AWS resources

What are they?

We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

ARN Format (right)

The specific formats depend on the resource. To use an ARN, replace the italicized text with the resource-specific information.

Be aware that the ARNs for some resources omit the Region, the account ID, or both the Region and the account ID.

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
arn:partition:service:region:account-id:resource-type:resource-id
```

Security Token Service (STS)

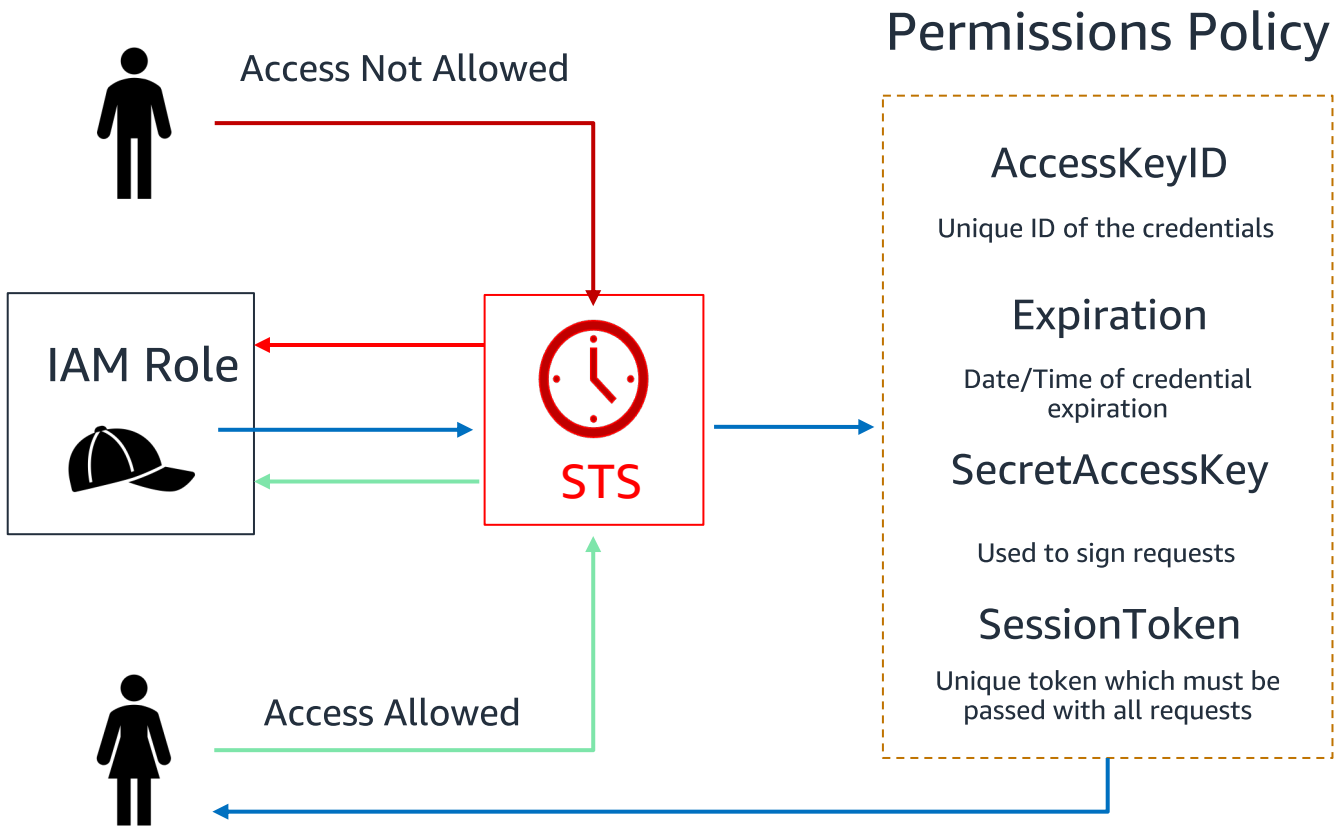
Request temporary, limited-privilege credentials for AWS IAM

Your Users OR Federated Users

STS allows you to provide temporary, limited-privilege credentials for your IAM users, or users that you federate as a part of access authentication. STS is a service that is available globally

Generating Credentials

Temporary credentials can be assumed by authorized identities through the generate temporary credentials (sts:AssumeRole*) command. The process of authorization follows the process at the right



Revoking Temporary Credentials

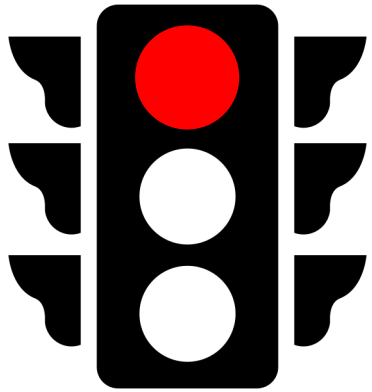
Remember that Roles can be assumed by MANY identities who will all get the same permissions. What happens if those credentials are compromised?

Trust Policies

Changing Trust policies only effect identities that have not already assumed the role. These policy changes have **NO impact** on existing credentials.

Permission Policies

Changing the **PERMISSIONS** policy will impact **ALL** credentials. Updating the policy with a **AWSRevokeOlderSessions** inline deny for any sessions older than now. This signs out all identities that have currently assumed the role and applies the new policies.



AWS S3 – Overview

aws training and certification

Amazon Simple Storage Service (S3)

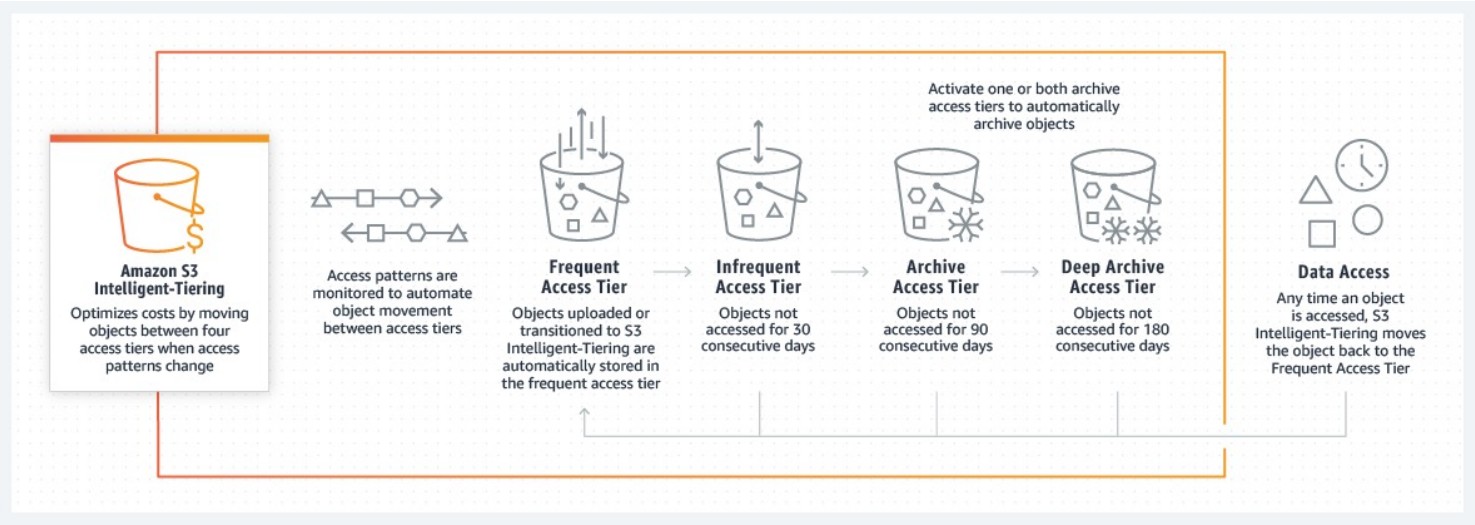
Provides infinitely scalable, highly durable object storage in the AWS Cloud

What does it do?

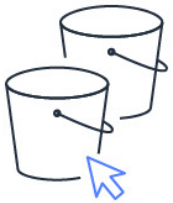
Stores objects in resources called Buckets, which can be up to 5TB in size, but there are no total limits to the# of objects stored.

Designed to provide 99.999999999% durability and 99.99% availability

Offered at multiple tiers of pricing based on the frequency the objects are needed, and the speed at which they are required to be retrieved.



Amazon Simple Storage Service (S3)



Provides infinitely scalable, highly durable object storage in the AWS Cloud

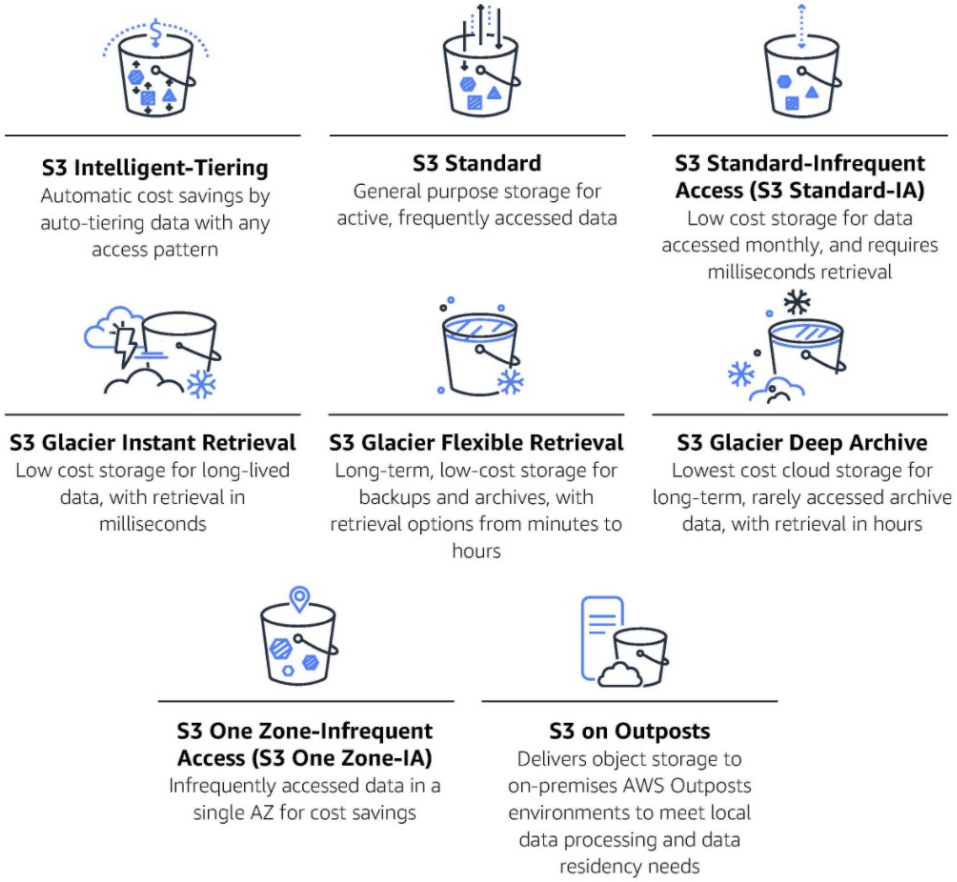
Storage Classes

Amazon S3 currently provides a range of storage class offerings to fit our customers needs.

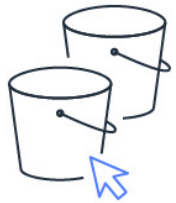
Each storage class is purpose-built for varying access patterns at corresponding costs.

Exam Tip

Amazon S3 features heavily in questions and use cases that are presented in the exam. Read these carefully for 'giveaways' that might be included in the question stem that highlight a storage class as an option.



Your Choice of Amazon S3 Storage classes



Become familiar with which class you should choose – and when

S3 Intelligent-Tiering

S3 Standard

S3 Standard-IA

S3 Glacier

S3 Glacier Deep Archive

S3 One Zone-IA

S3 Outposts

AWS Region ≥ 3 Availability Zones

- Data with changing access patterns
- Opt in for automatic archiving

- Active, frequently accessed data
- Milliseconds access

- Infrequently accessed data
- Milliseconds access
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

- Archive data
- In minutes and hours
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

- Long-term archive data
- Select hours
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

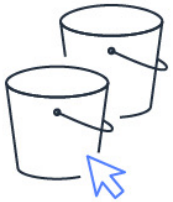
AWS Single AZ

- Re-creatable, less accessed data
- Milliseconds access
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

AWS Outposts

- On-premises data
- Milliseconds access
- Encrypted with SSE-S3

Amazon S3 Transfer Accelerator



Provides faster, long-distance S3 uploads & downloads

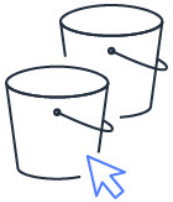
What does it do?

S3 Transfer Acceleration (S3TA) reduces the variability in Internet routing, congestion and speeds that can affect transfers, and logically shortens the distance to S3 for remote applications. S3TA improves transfer performance by routing traffic through Amazon CloudFront's globally distributed Edge Locations and over AWS backbone networks, and by using network protocol optimizations.

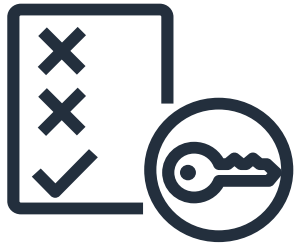
Exam Tip

S3TA helps reduce network variability by physically shortening the distance between your apps and AWS. Any question that speaks to long-distance uploads, or finding ways to increase data transfer with S3 - consider S3TA

S3 Security – The Core of what we do

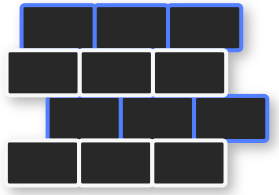


Data stored in S3 is secure by default

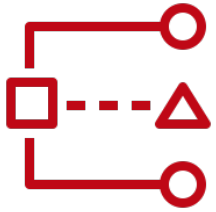


Access control with identity and access management (IAM) and bucket policy

Amazon S3 Access Points



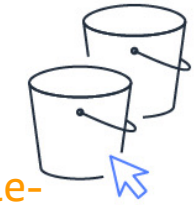
Amazon S3 Block Public Access



AWS Access Analyzer

Encrypt data by default in Amazon S3

S3 Bucket Policies



A bucket policy that allows a principal (AWS Account ID 111111111111) to read and write to the bucket “sample-bucket-reinvent”

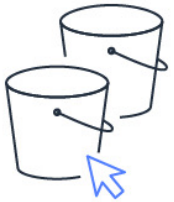
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/sample-
bucket-reinvent/*“,
            ”Principal”: {"AWS":"111111111111"}
        }
    ]
```

Same syntax as IAM policy but adds a principal statement

Principal: specifies who the statement covers

aws training and certification

S3 Bucket Policy Principles



Who/What can be a principle in an S3 bucket policy?

Valid principals for your bucket policies include

- AWS account and root user
- IAM users
- Federated users (using web identity or SAML federation)
- IAM roles
- Assumed-role sessions
- AWS services
- Anonymous users (public) – not recommended

Amazon CloudFront

aws training and certification

Amazon CloudFront

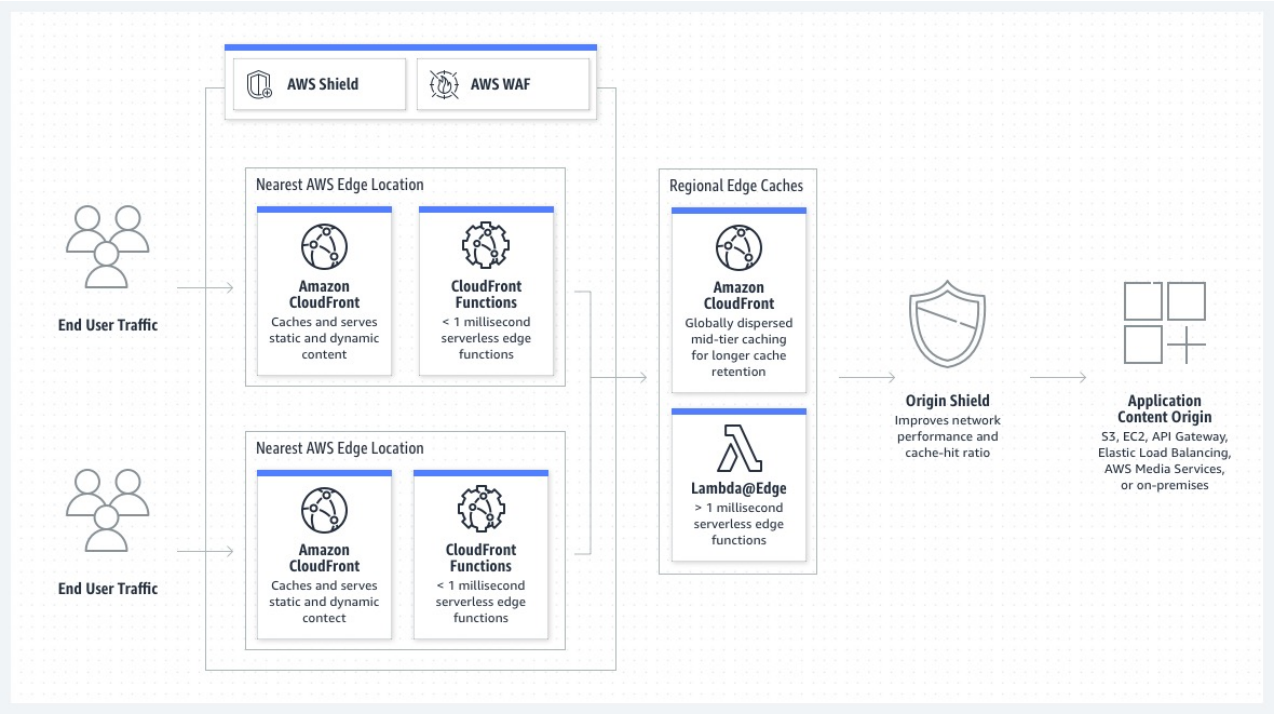
Securely deliver content with low latency and high transfer speeds

Content Delivery

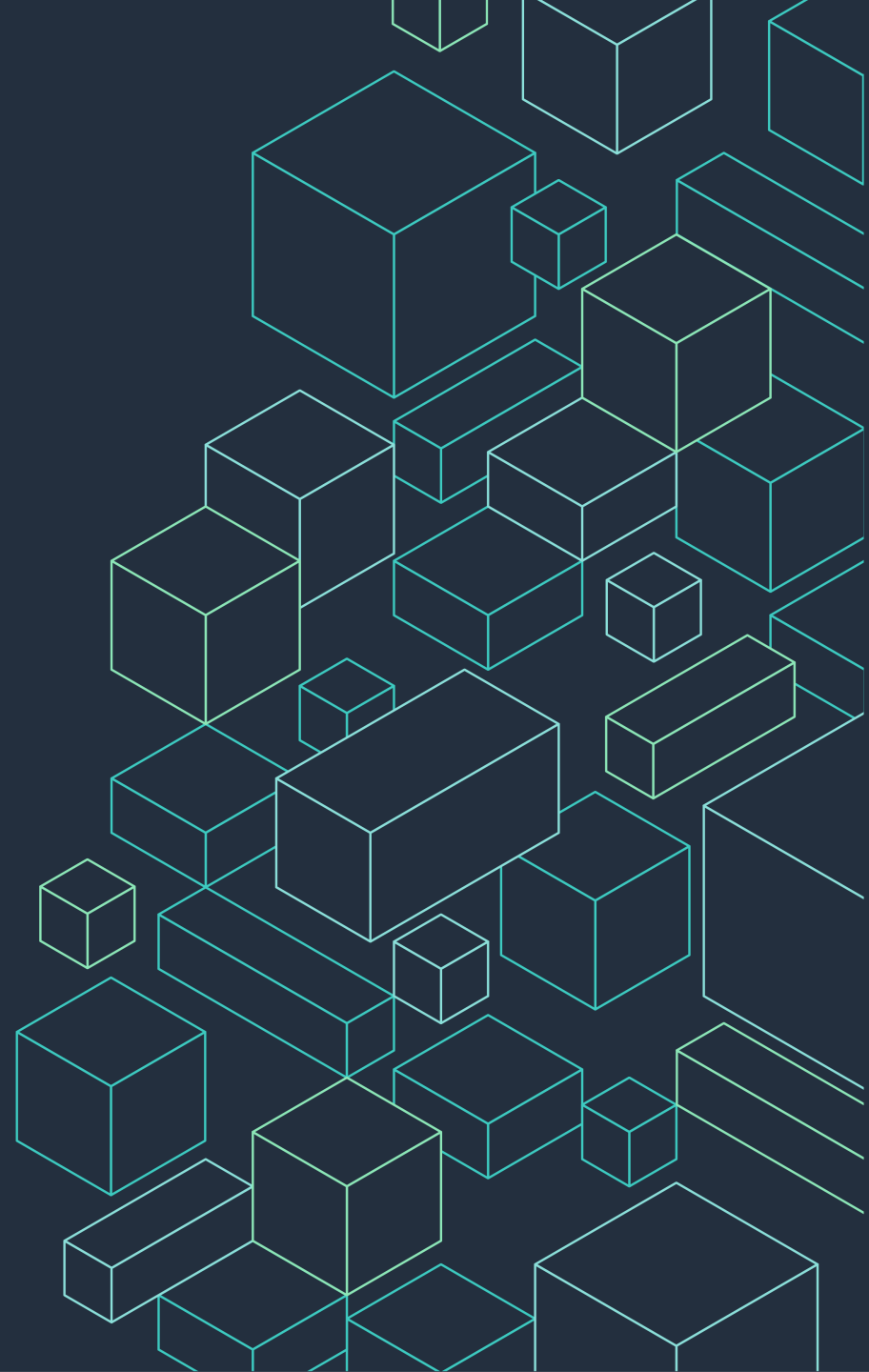
CloudFront is a Content Delivery Network (CDN). It reduces latency for end users by leveraging the 310+ Points of Presence in the AWS network to deliver content to a global audience.

Exam Tip

Any exam question that addresses the distribution of content to a global audience (especially static content) typically points to the use of Amazon CloudFront.



Thank you!



aws training and certification