Designing Applications and Architectures in AWS

(Aligned with AWS Solution Architect Associate Certification)

simplilearn

Storage Services

A Day in the Life of a Cloud Architect

You are a cloud architect in an organization and have been asked to identify cloud services for a data-intensive e-commerce company.

Your tasks include:

- Establishing a scalable, highly available, and secure database system to manage data effectively
- Implementing version control to preserve, retrieve, and restore every version of an object in the database and ensuring data encryption for high security
- Using standard SQL to execute queries on the data
- Providing the option to upgrade the volume type to adjust the database performance as needed

To achieve these, you will learn a few concepts in this lesson to help you find a solution for the given scenario.

Learning Objectives

By the end of this lesson, you will be able to:

- Create Amazon S3 buckets to store data and objects in the Cloud
- Enable versioning in Amazon S3 buckets to enable data protection
- Demonstrate static web hosting using Amazon S3 to optimize the cost and enable scalability
- Share Amazon S3 buckets between multiple accounts to centralize data storage within an organization

Learning Objectives

By the end of this lesson, you will be able to:

- Backup and sync data with Amazon S3 to provide data durability and redundancy
- Transfer files from Amazon S3 to on-premises storage to perform data analysis on-premises

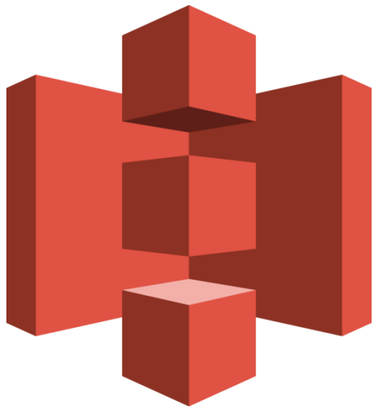
TECHNOLOGY

Introduction to Amazon S3

simplilearn

What Is Amazon S3?

Amazon Simple Storage Service (Amazon S3) is a web-based storage service offered by AWS for archiving and backing up data online.



Amazon S3

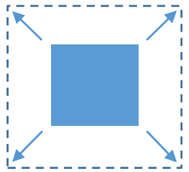
Users can store, retrieve, and protect any amount of data at any time from anywhere.

Amazon S3: Features

Amazon S3 offers a range of features for storage solutions, including:

Availability

Scalability



Durability

Performance

Cost-efficiency

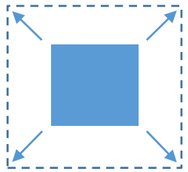
Security

Amazon S3: Features

Amazon S3 is designed to provide 99.99% availability. Users can select the desired AWS region to store their data, optimizing latency and minimizing costs.

Availability

Scalability



Durability

Performance

Cost-efficiency

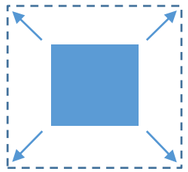
Security

Amazon S3: Features

Amazon S3 is designed to offer unparalleled scalability, enabling users to store and manage their data regardless of its size.

Availability

Scalability



Durability

Performance

Cost-efficiency

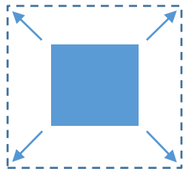
Security

Amazon S3: Features

Amazon S3 stores data redundantly across multiple facilities and multiple devices in each facility, making it durable.

Availability

Scalability



Durability

Performance

Cost-efficiency

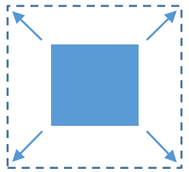
Security

Amazon S3: Features

Amazon S3 supports multipart uploads, maximizing network throughput and resilience.

Availability

Scalability



Durability

Performance

Cost-efficiency

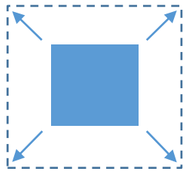
Security

Amazon S3: Features

Amazon S3 uses a pay-per-use model that allows users to store large data sets at a low cost.

Availability

Scalability



Durability

Performance

Cost-efficiency

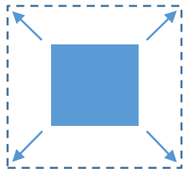
Security

Amazon S3: Features

Amazon S3 supports SSL (Secure Sockets Layer) data transfer and encryption once the data is uploaded.

Availability

Scalability



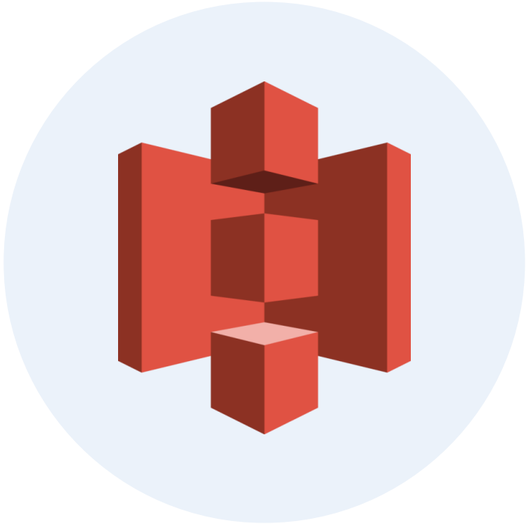
Durability

Performance

Cost-efficiency

Security

Amazon S3: Components



01

Buckets:
Buckets are containers for storing and organizing data of any format in Amazon S3.

02

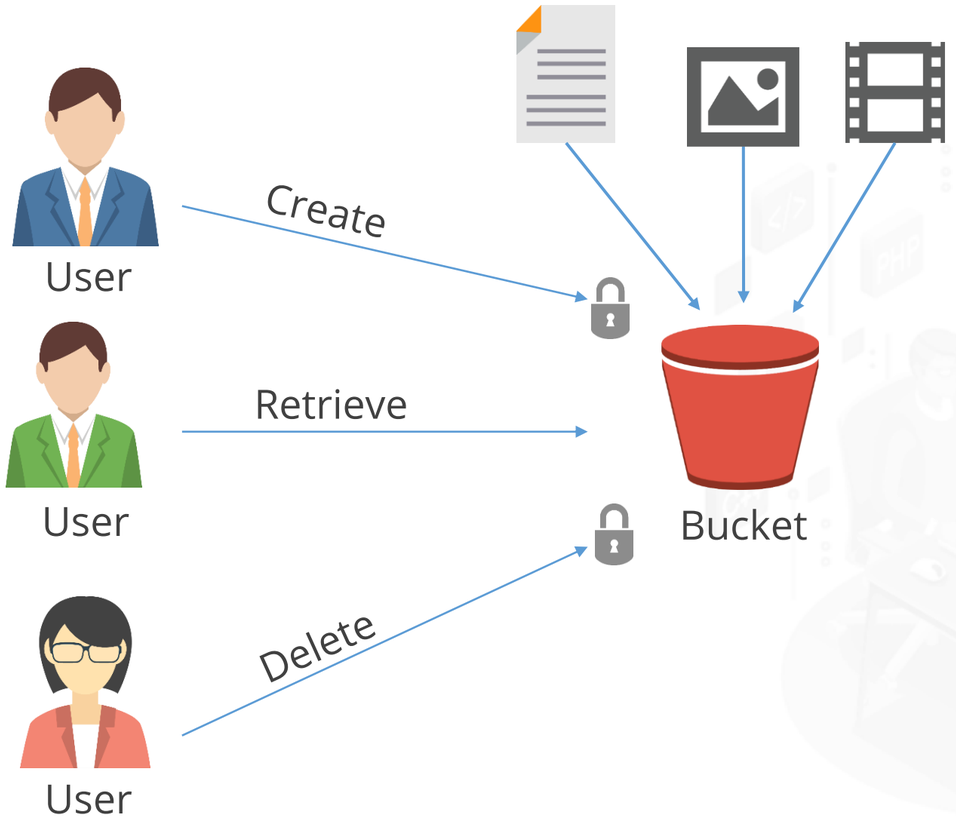
Keys:
Keys are a unique identifier for a piece of data stored in Amazon S3 buckets.

03

Regions:
Regions are geographical locations where Amazon stores the S3 buckets created by its users.

Amazon S3: Components

- Buckets can store text files, images, videos, and more.
- Any number of objects can be stored in a bucket, and the total bucket size is 5TB.
- The user can control access to each bucket option.



Amazon S3: Storage Classes

Amazon S3 has the following range of storage classes:

- Amazon S3 Standard
- Amazon S3 Intelligent-Tiering
- Amazon S3 Standard-Infrequent Access
- Amazon S3 One Zone-Infrequent Access
- Amazon S3 Glacier
- Amazon S3 Glacier Deep Archive

Amazon S3 Standard

Features of Amazon S3 Standard

- Stores objects that are frequently accessed
- Has low latency and high throughput performance
- Is backed by the Amazon S3 service-level agreement for availability
- Is ideal for dynamic websites, cloud and mobile applications, and file storage
- Has S3 Lifecycle management for an automatic transition of objects between S3 storage classes

Amazon S3 Intelligent-Tiering

Features of Amazon S3 Intelligent-Tiering

- Stores objects in two access tiers optimized for frequent and infrequent access
- Is designed for 99.99% availability
- Has the same low latency and high throughput performance as S3 Standard
- Includes a small monthly monitoring and auto-tiering fee
- Is ideal for long-lived data with unpredictable access patterns
- Moves objects automatically between two access tiers based on changing access patterns

Amazon S3 Standard-Infrequent Access (IA)

Features of Amazon S3 Standard-Infrequent Access

- Stores objects that are accessed less frequently
- Is designed for 99.99% availability
- Has the same low latency and high throughput performance as S3 Standard
- Has a low price per GB of storage
- Is ideal for long-term storage, backups, and as a data store for disaster recovery files

Amazon S3 One Zone-Infrequent Access (IA)

Features of Amazon S3 One Zone-Infrequent Access

- Stores objects that are accessed less frequently but require rapid access when needed
- Stores data in a single AZ and costs 20% less than S3 Standard-IA
- Has a low price per GB of storage
- Is ideal for customers who want a lower-cost option for infrequently accessed data
- Is good for storing secondary backup copies of on-premises data

Amazon S3 Glacier

Features of Amazon S3 Glacier

- Is a secure, durable, and low-cost storage class for archiving rarely accessed data
- Provides three configurable retrieval options varying from minutes to hours
- Has a lower per-GB storage price and per-GB retrieval fee
- Offers a secure vault lock feature that enforces compliance
- Ensures data is resilient in case of an entire Availability Zone (AZ) destruction
- Is ideal for database backups, compliance data, or audit log files that are rarely accessed

Amazon S3 Glacier Deep Archive

Features of Amazon S3 Glacier Deep Archive

- Is the lowest-cost storage class supporting long-term retention and digital preservation
- Stores data that may be accessed once or twice a year
- Is used for backup and disaster recovery
- Ensures data is replicated and stored in at least three geographically dispersed AZs
- Ensures data is retrieved within 12 hours
- Is good for customers in highly regulated industries who retain data for 7-10 years

Performance Chart

Below is the performance chart across the S3 storage classes:

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	N/A	N/A

Source: https://aws.amazon.com/s3/storage-classes/

Performance Chart

Below is the performance chart across the S3 storage classes:

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Source: https://aws.amazon.com/s3/storage-classes/

Creating an S3 Bucket

Duration:10 min

Problem Statement:

You have been assigned a task to create an S3 bucket using an AWS account.

ASSISTED PRACTICE

Assisted Practice: Guidelines

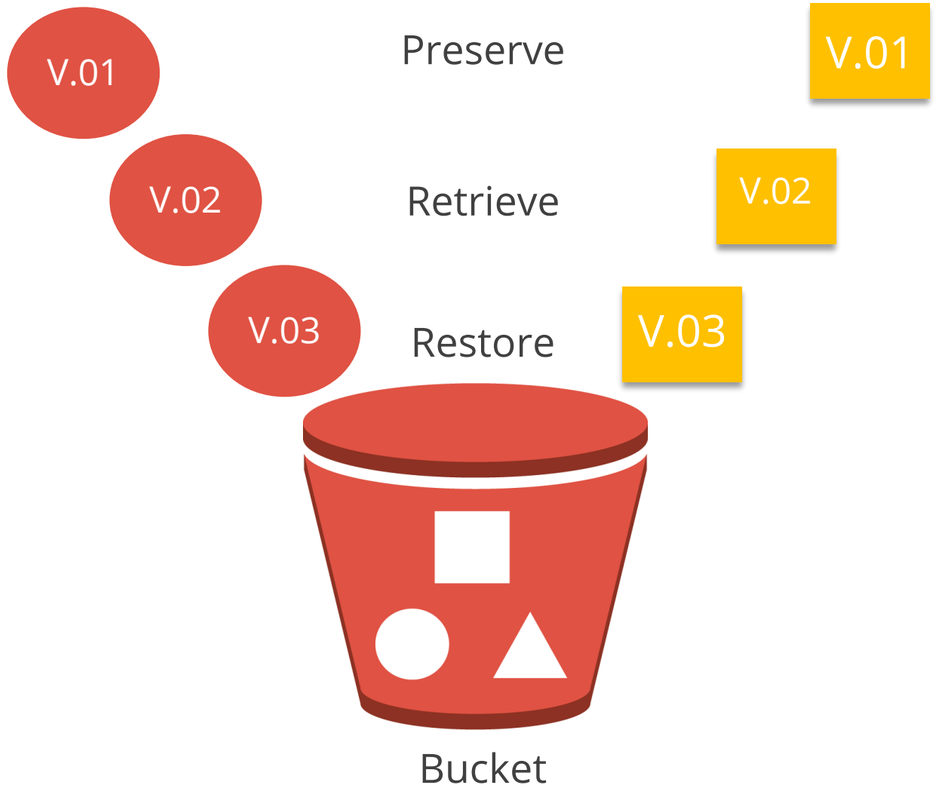
Steps to be followed are:

1. Create an S3 bucket

Version Control in Amazon S3

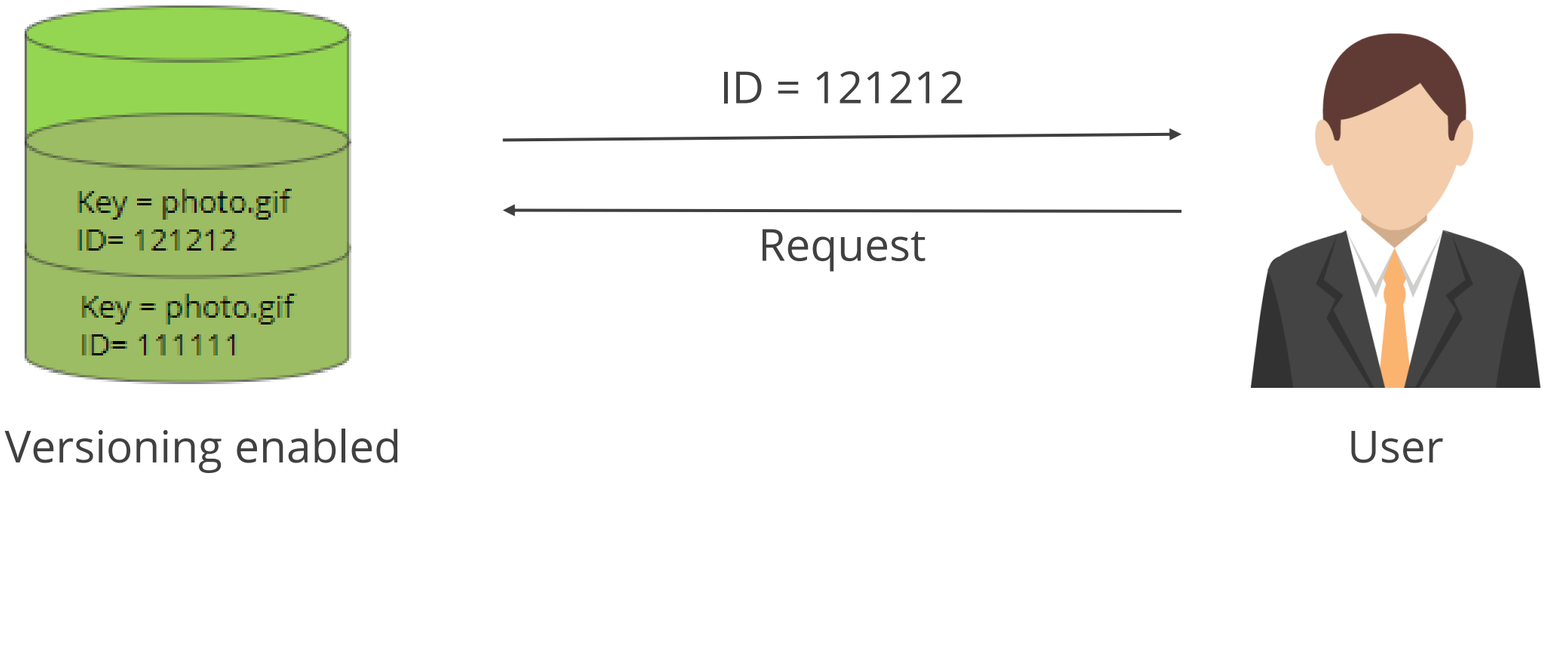
Version Control

Versioning is used to keep and maintain multiple variants of an object in the same bucket. It is also used to preserve, retrieve, and restore earlier versions of every object stored in Amazon S3 buckets.



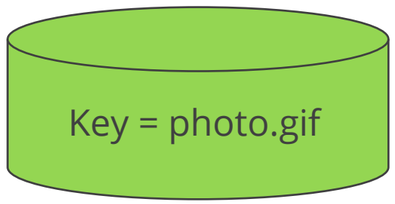
Version Control

Versioning allows users to recover their files from accidental deletions or overwrites.

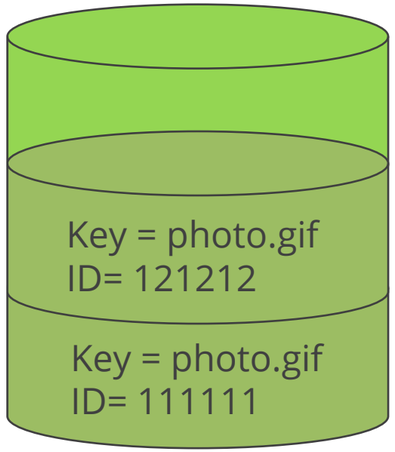


Version Control States

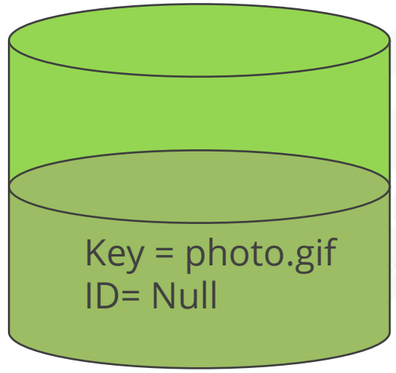
S3 buckets can be in one of the three states of versioning: unversioned, versioning enabled, or versioning suspended.



Unversioned



Versioning enabled

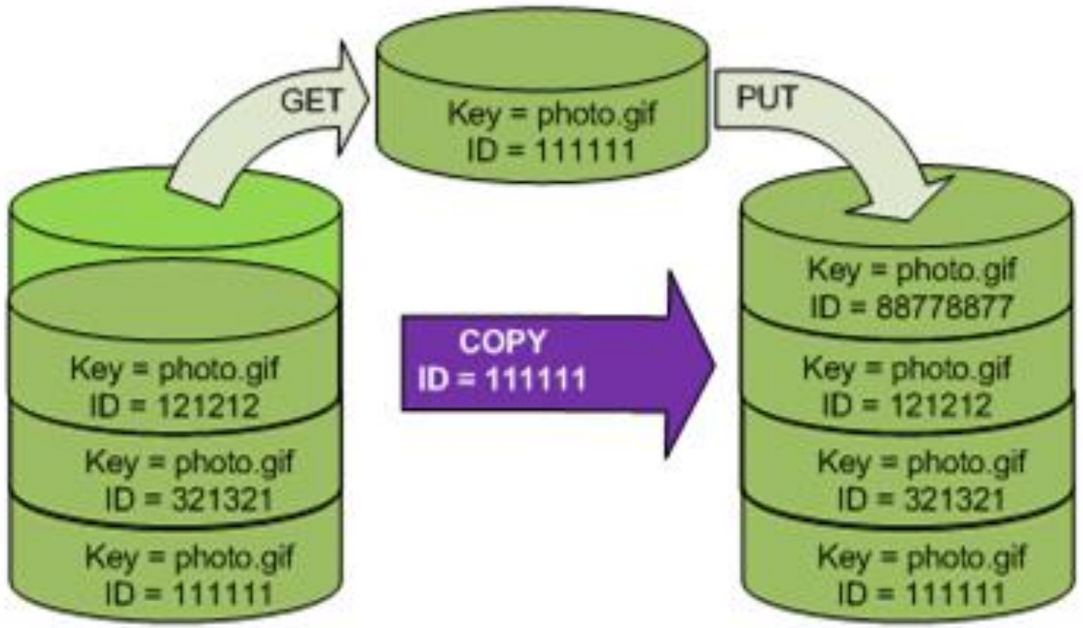


Versioning suspended

Restoring a Previous Version

There are two approaches to restoring a previous version of an object:

1. Copy the previous version of an object into the bucket



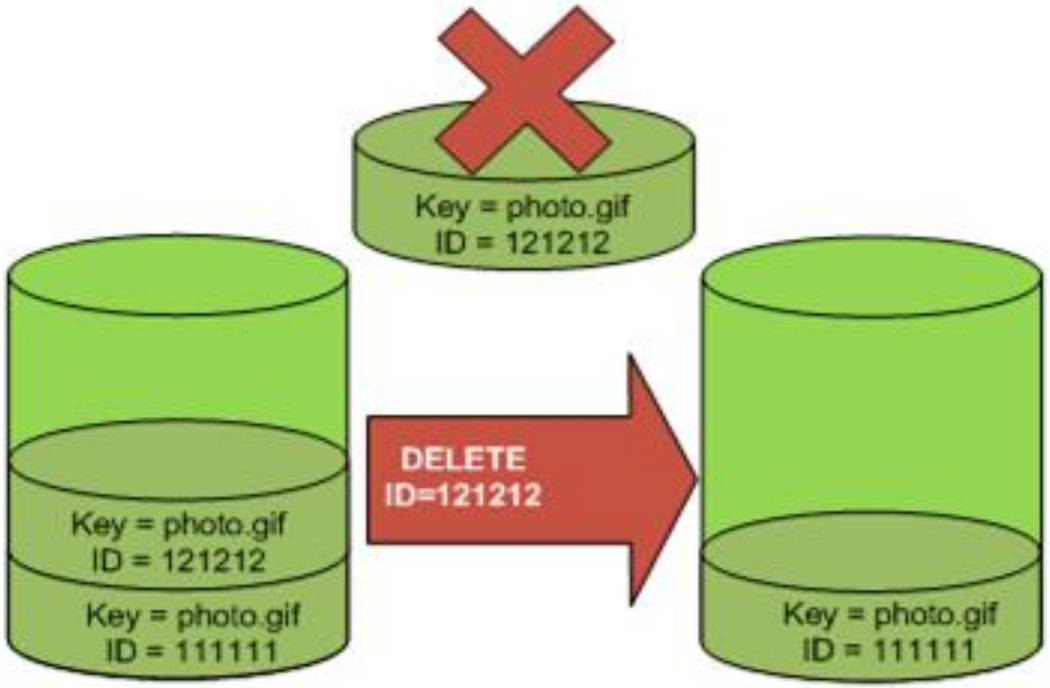
Versioning enabled

Versioning enabled

Source: https://docs.aws.amazon.com/AmazonS3/latest/dev/RestoringPreviousVersions.html

Restoring a Previous Version

2. Delete the current version of an object



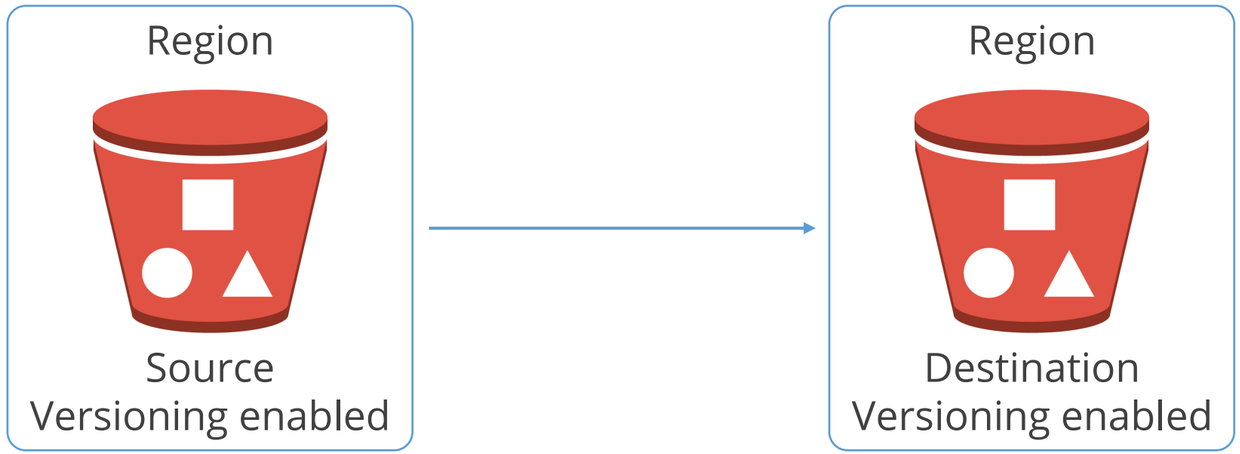
Versioning enabled

Versioning enabled

Source: https://docs.aws.amazon.com/AmazonS3/latest/dev/RestoringPreviousVersions.html

Cross-Region Replication

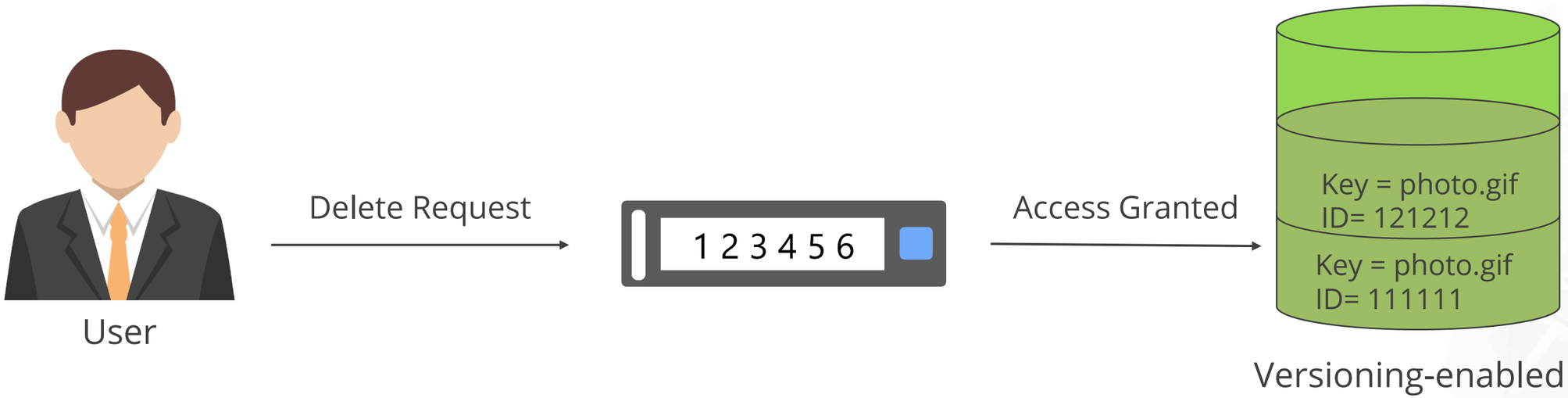
Cross-region replication is a bucket-level feature that enables automatic and asynchronous copying of objects across buckets in different AWS regions.



For cross-region replication to work, versioning should be enabled on both the source and destination buckets.

Cross-Region Replication

Amazon S3 allows users to protect their data by enabling multi-factor authentication (MFA).



This provides additional authentication for operations such as changing the versioning state of a bucket permanently and deleting an object version.

Configuring S3 Bucket Version

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the process of configuring S3 bucket versioning, uploading files to an Amazon S3 bucket, and reuploading the same files.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Enable bucket versioning for an S3 bucket
2. Upload files to the S3 bucket
3. Reupload the same files to the S3 bucket

TECHNOLOGY

S3 Lifecycle Management

S3 Lifecycle Management

S3 Lifecycle configuration is done to manage a user's objects cost-effectively throughout their lifecycles.

An S3 Lifecycle configuration is a set of rules defining actions applied to a group of objects. There are two types of actions:

01 Transition actions

02 Expiration actions

Managing Object Lifecycle

S3 Lifecycle configuration rules help manage objects by:

01	Deleting periodic logs after a set time (e.g., a month)
02	Archiving frequently-accessed documents when real-time access is no longer needed
03	Retaining data uploaded for long-term archival

Creating a Lifecycle Configuration

1. An S3 Lifecycle configuration is an XML file containing rules and predefined actions for Amazon S3 to perform on objects during their lifetime.

2. Users can configure the lifecycle through the Amazon S3 console, REST API, AWS SDKs, or the AWS Command Line Interface (AWS CLI).

3. Amazon S3 manages the lifecycle configuration of a bucket by storing it as a lifecycle sub-resource attached to that bucket.

Configuring S3 Intelligent-Tiering Archive

Duration:10 min

Problem Statement:

You have been assigned a task to set up an S3 Intelligent-Tiering Archive configuration to optimize storage costs by automatically transitioning objects to cost-effective access tiers based on changing access patterns.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a new Intelligent-Tiering Archive configuration

Configuring Age-Based Retention

Duration:10 min

Problem Statement:

You have been assigned a task to create a lifecycle rule in the S3 bucket to delete expired objects.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create an S3 bucket lifecycle rule

Access Controls

Access control lists (ACLs) grant basic read and write permissions to other AWS accounts. By default, the account that owns an object can access it and grant other users access through ACLs.

1

Users can use Object Ownership to change the default behavior of an ACL.

2

When users disable the ACLs, the bucket owner automatically owns every object in the bucket.

3

User access control is based on IAM policies, S3 bucket policies, VPC endpoint policies, and AWS Organizations' service control policies.

Sharing an S3 Bucket Between Multiple Accounts

Sharing an S3 bucket between multiple accounts can depend on the type of access a user wants to provide.

The methods to grant cross-account access for sharing objects between multiple accounts are:

- Resource-based policies and AWS IAM policies
- Resource-based access control list (ACL) and IAM policies
- Cross-account IAM roles

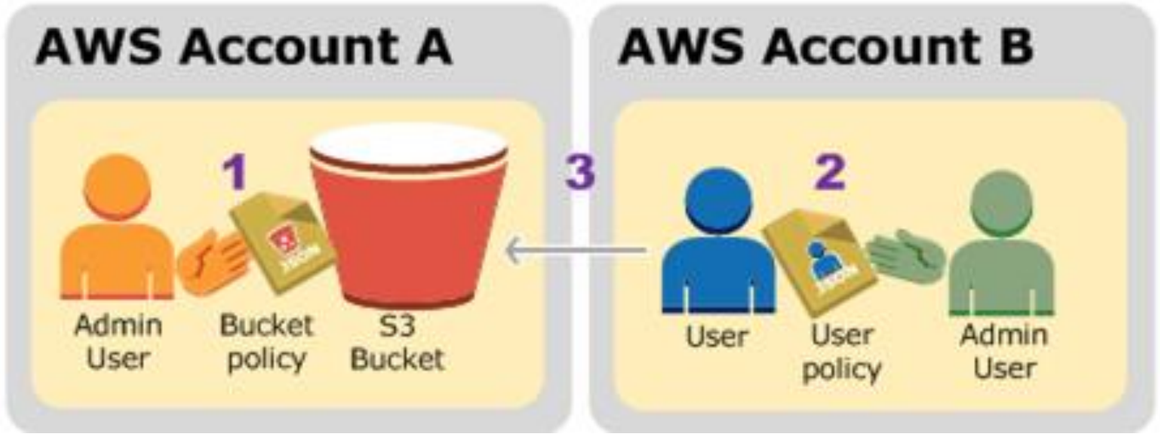
Sharing an S3 Bucket Between Multiple Accounts

The steps to share an S3 bucket between multiple accounts are as follows:

1. Account A admin user attaches a bucket policy granting cross-account permissions to Account B.

2. Account B admin user attaches a user policy authorizing the permissions it received from Account A.

3. A user in Account B verifies the permissions by accessing the bucket owned by Account A.

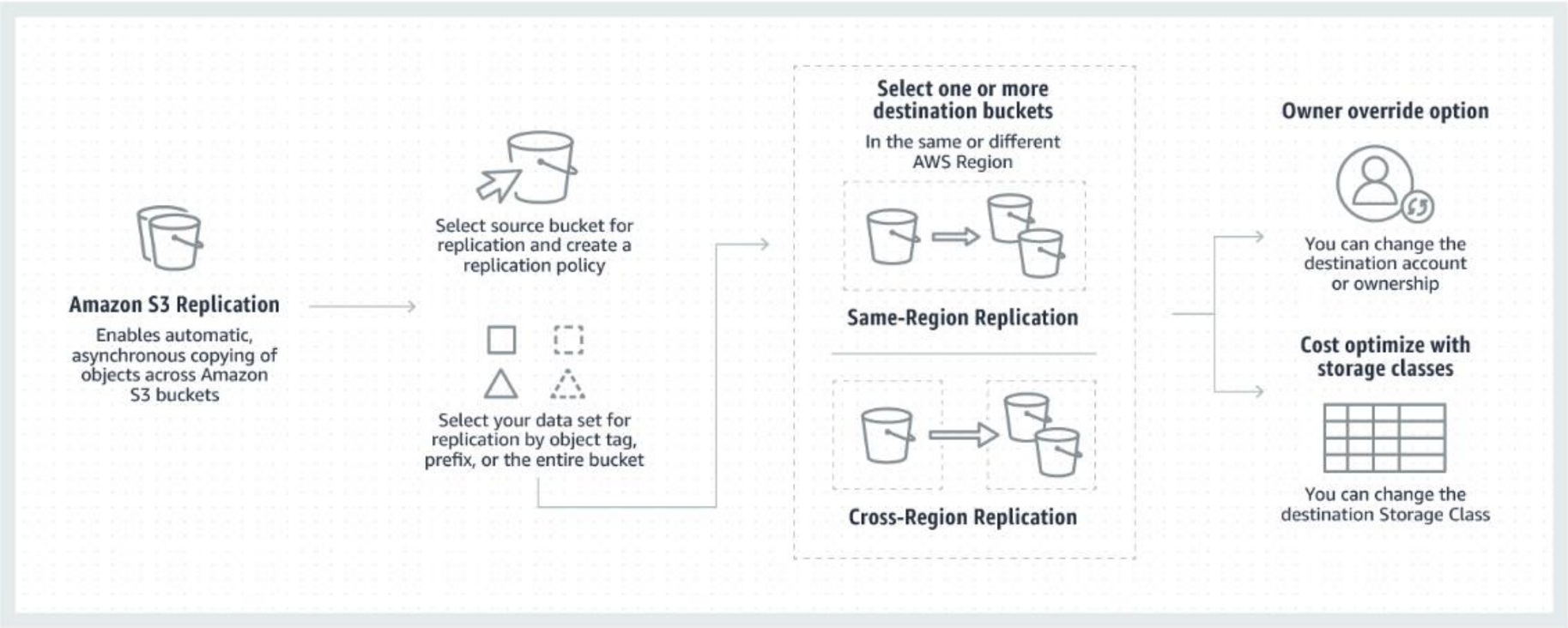


Source: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html

Amazon S3 Replication

Amazon S3 Replication

Amazon S3 Replication is an elastic, fully managed, and low-cost feature that replicates objects between buckets, providing great flexibility and functionality in cloud storage.



Working of S3 Replication

Source: https://aws.amazon.com/s3/features/replication/

S3 Replication Use Cases

These are the various use cases of S3 replication:

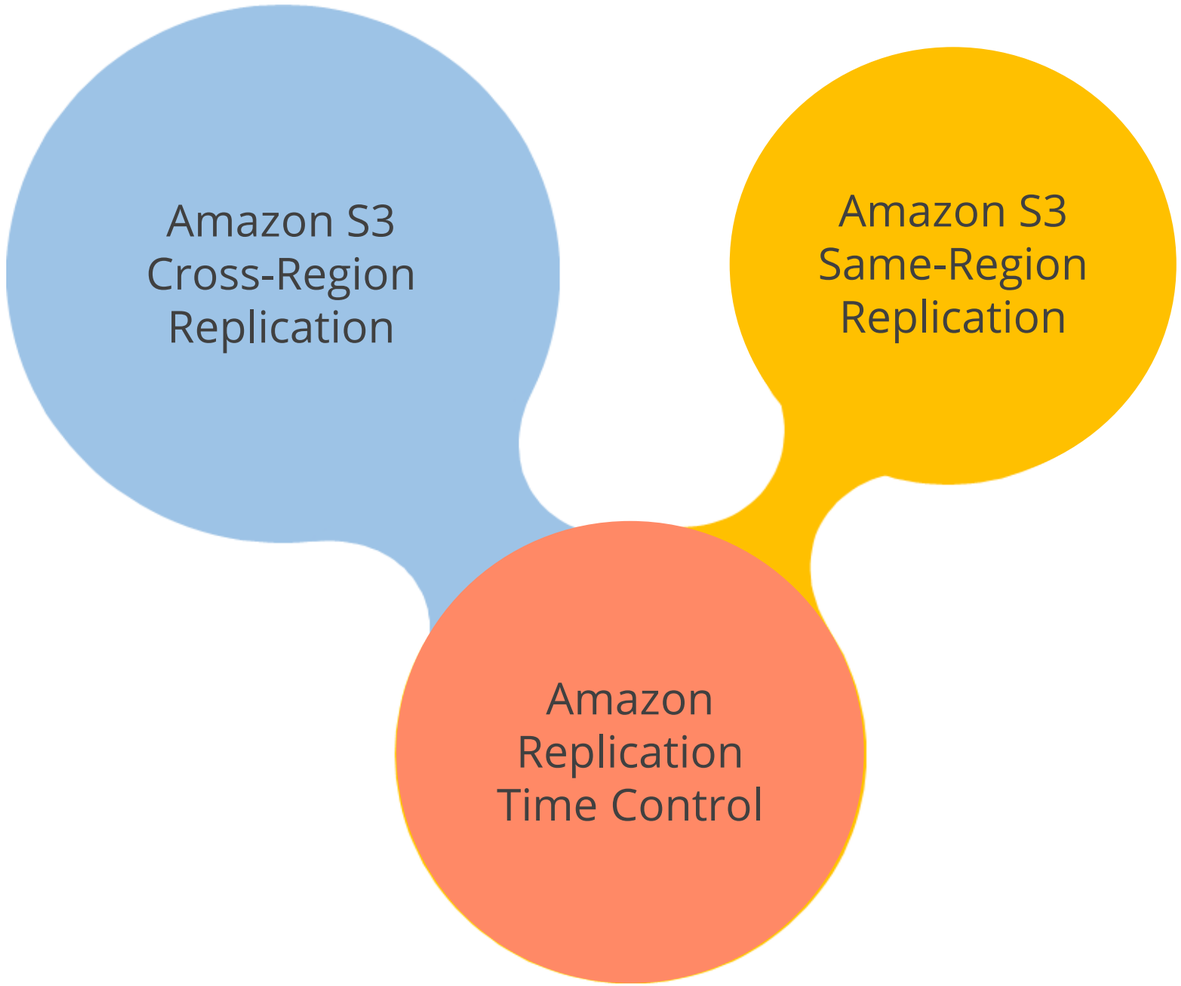
Replicate objects while retaining metadata

Replicate objects to more cost-effective storage classes

Urgent requirement of replicated buckets

Maintain object copies under different ownership

S3 Replications: Types



Types of S3 Replications

Amazon S3 Cross-Region Replication (CRR)

- Replicates data automatically between buckets across different AWS Regions
- Configures a source S3 bucket and replicates objects into a destination bucket in another AWS Region
- Replicates data at the bucket level, a shared prefix level, or an object level using S3 object tags
- Provides lower-latency data access in different geographic regions

Types of S3 Replications

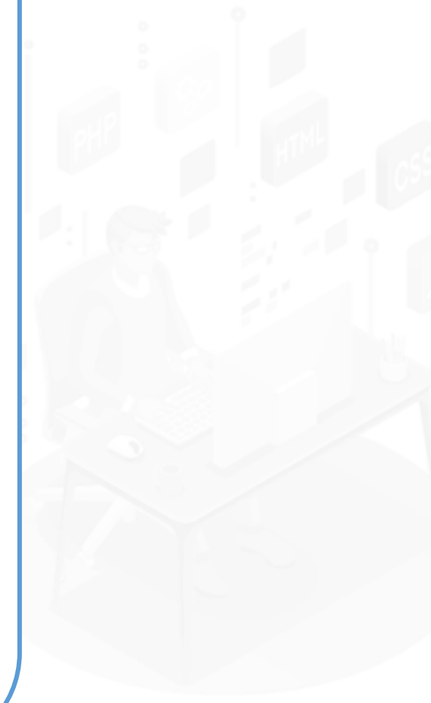
Amazon S3 Same-Region Replication (SRR)

- Replicates data automatically between buckets within the same AWS Region
- Replicates data at the bucket level, a shared prefix level, or an object level using S3 object tags
- Addresses data sovereignty and compliance requirements
- Changes account ownership for the replicated objects to protect against accidental data deletion
- Collects logs from various S3 buckets for in-region processing or configures live replication

Types of S3 Replications

Amazon Replication Time Control

- Replicates 99.99% of new objects stored in Amazon S3 within 15 minutes
- Meets compliance or business requirements for data replication and provides visibility into S3 replication activity
- Provides S3 Replication metrics that monitor:
  I. The total number of S3 API operations that are pending replication
  II. The total size of objects pending replication
  III. The maximum replication time to the destination AWS Region



Object Replication Between S3 Buckets

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the replication of an object from a source to a destination S3 bucket using replication rules.

ASSISTED PRACTICE

Assisted Practice: Guidelines

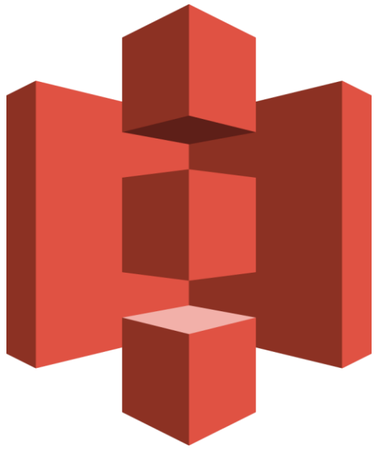
Steps to be followed are:

1. Create two S3 buckets for source and destination
2. Add a file to the source bucket
3. Create a replication rule from the source bucket
4. Replicate the object file from the source to destination bucket
5. Delete and verify the replicated object file

Storage Gateway

Performance Guidance for S3 File Gateway

Performance guidance involves the provisioning of hardware for users' S3 file gateway virtual machines.



The cache disk size must be tuned to the size of the active working set for best performance.

Performance Guidance for S3 File Gateway

The table below shows an example of S3 File Gateway performance on Linux clients:

Example configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Root disk: 80 GB, io1 SSD, 4,000 IOPS	NFSv3 - 1 thread	110 MiB/sec (0.92 Gbps)	590 MiB/sec (4.9 Gbps)	310 MiB/sec (2.6 Gbps)
Cache disk: 512 GiB cache, io1, 1,500 provisioned IOPS	NFSv3 - 8 threads	160 MiB/sec (1.3 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
Minimum network performance: 10 Gbps	NFSv4 - 8 threads	160 MiB/sec (1.3 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
CPU: 16 vCPU | RAM: 32 GB	SMBV3 - 1 thread	115 MiB/sec (1.0 Gbps)	325 MiB/sec (2.7 Gbps)	255 MiB/sec (2.1 Gbps)

Performance Guidance for S3 File Gateway

The table below shows an example of S3 File Gateway performance on Linux clients:

Example configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
NFS protocol recommended for Linux	SMBV3 - 8 threads	190 MiB/sec (1.6 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
Storage Gateway Hardware Appliance	NFSv3 - 1 thread	265 MiB/sec (2.2 Gbps)	590 MiB/sec (4.9 Gbps)	310 MiB/sec (2.6 Gbps)
Minimum network performance: 10 Gbps	NFSv3 - 8 threads	385 MiB/sec (3.1 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
	NFSv4 - 8 threads	385 MiB/sec (3.1 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)

Performance Guidance for S3 File Gateway

The table below shows an example of S3 File Gateway performance on Windows clients:

Example configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Root disk: 80 GB, io1 SSD, 4,000 IOPS	SMBV3 - 1 thread	150 MiB/sec (1.3 Gbps)	180 MiB/sec (1.5 Gbps)	20 MiB/sec (0.2 Gbps)
Cache disk: 512 GiB cache, io1, 1,500 provisioned IOPS	SMBV3 - 8 threads	190 MiB/sec (1.6 Gbps)	335 MiB/sec (2.8 Gbps)	195 MiB/sec (1.6 Gbps)
Minimum network performance: 10 Gbps	NFSv3 - 1 thread	95 MiB/sec (0.8 Gbps)	130 MiB/sec (1.1 Gbps)	20 MiB/sec (0.2 Gbps)
CPU: 16 vCPU | RAM: 32 GB	NFSv3 - 8 threads	190 MiB/sec (1.6 Gbps)	330 MiB/sec (2.8 Gbps)	20 MiB/sec (0.2 Gbps)

Performance Guidance for S3 File Gateway

The table below shows an example of S3 File Gateway performance on Windows clients:

Example configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
SMB protocol recommended for Windows	NFSv3 - 8 threads	190 MiB/sec (1.6 Gbps)	330 MiB/sec (2.8 Gbps)	190 MiB/sec (1.6 Gbps)
Storage Gateway Hardware Appliance	SMBV3 - 1 thread	230 MiB/sec (1.9 Gbps)	255 MiB/sec (2.1 Gbps)	20 MiB/sec (0.2 Gbps)
Minimum network performance: 10 Gbps	SMBV3 - 8 threads	835 MiB/sec (7.0 Gbps)	475 MiB/sec (4.0 Gbps)	195 MiB/sec (1.6 Gbps)
	NFSv3 - 1 thread	135 MiB/sec (1.1 Gbps)	185 MiB/sec (1.6 Gbps)	20 MiB/sec (0.2 Gbps)

Optimizing Gateway Performance

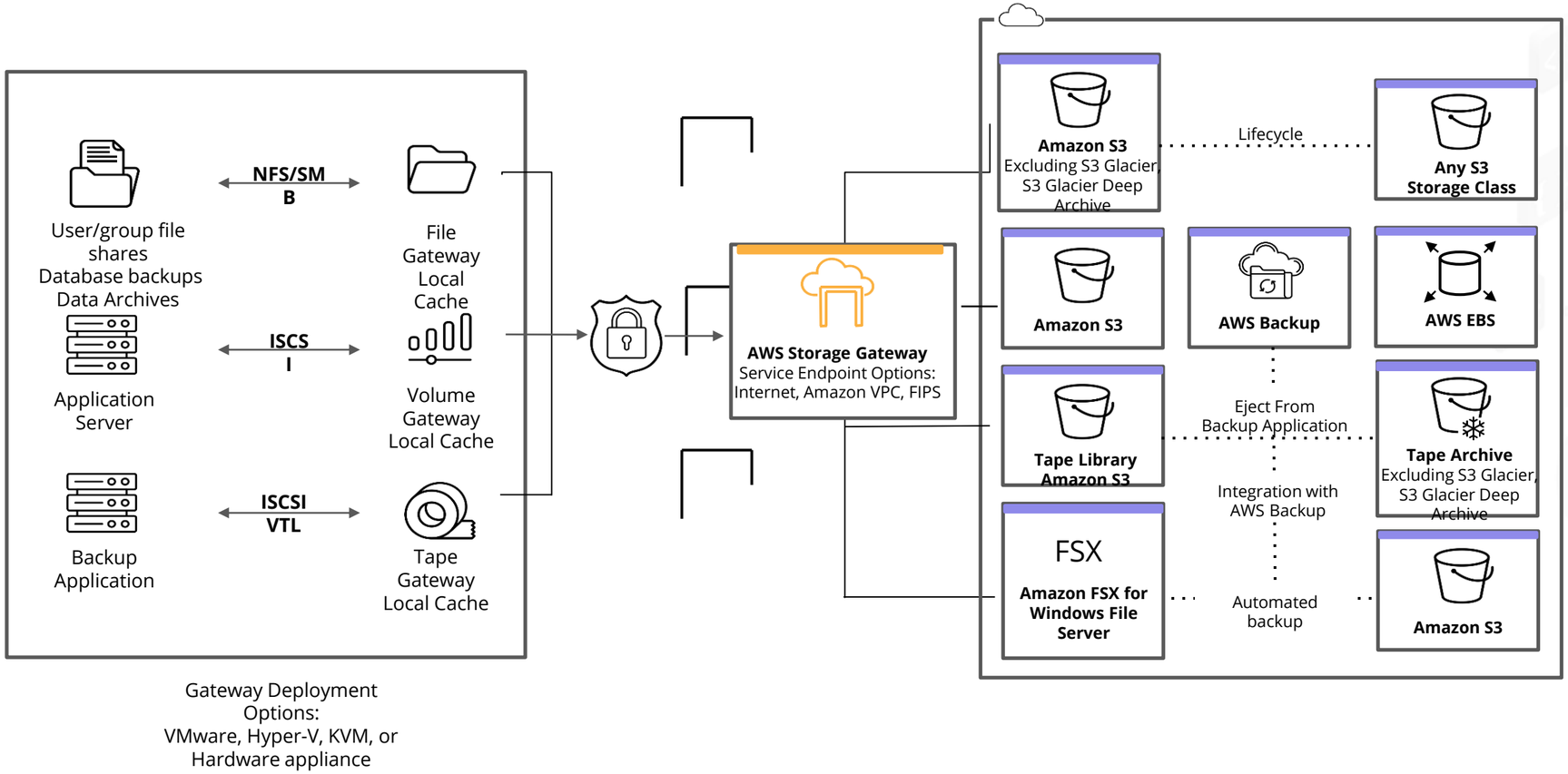
One can optimize gateway performance by adding resources to the gateway.

Here are ways to enhance gateway performance:

- Use higher-performance disks
- Add CPU resources to the gateway host
- Back gateway virtual disks with separate physical disks
- Increase the bandwidth between the application server and gateway
- Add CPU resources to the application environment

Storage Gateway

AWS Storage Gateway offers a comprehensive suite of hybrid cloud storage services, facilitating seamless access to virtually unlimited cloud storage from on-premises environments.



S3 Encryption

Server-Side Encryption (SSE-S3)

Server-side encryption protects data by encrypting each object using a unique key.

Server-Side Encryption on Amazon S3

- Amazon S3 uses the 256-bit Advanced Encryption Standard (AES-256), one of the strongest block ciphers, to encrypt data.
- Users can use server-side encryption with Amazon S3-managed keys (SSE-S3) to incur no additional charges.
- Users can use a bucket policy to encrypt all objects in a bucket.

Server-Side Encryption (SSE-S3)

An example of a bucket policy that denies permissions to upload an object unless the request includes the **x-amz-server-side-encryption** header to request server-side encryption:

Example

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    ]
}
```

Server-Side Encryption (SSE-S3)

An example of a bucket policy that denies permissions to upload an object unless the request includes the **x-amz-server-side-encryption** header to request server-side encryption:

Example

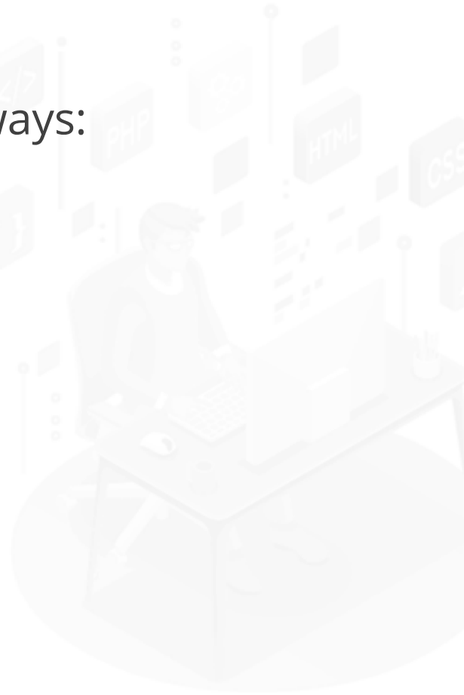
```
{
  "Sid": "DenyUnencryptedObjectUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::awsexamplebucket1/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

API Support for Server-side Encryption

To enable server-side encryption during object creation with REST APIs, include the **x-amz-server-side-encryption** request header.

Amazon S3 supports the **x-amz-server-side-encryption** header in the following ways:

- **PUT Operations:** Include this header when uploading data with the PUT API
- **Initiate Multipart Upload:** Use the header to initiate request for uploading large objects with the multipart upload API
- **COPY Operations:** Copy an object and apply the **x-amz-server-side-encryption** header to both the source and target objects



Server-side Encryption with AWS KMS (SSE-KMS)

SSE-KMS encrypts data using AWS KMS keys, enhancing the security of the data.

- Encryption can be applied either during the upload of a new object or when copying an existing object.
- SSE-KMS can be specified using various methods such as the Amazon S3 console, REST API operations, AWS SDKs, and the AWS Command Line Interface (AWS CLI).

Server-side Encryption with SSE-C

Server-side encryption with customer-provided encryption keys (SSE-C) allows users to set their encryption keys, which are used exclusively to encrypt the object data.

- Amazon S3 manages the encryption process when writing data to disks and handles decryption when objects are accessed.
- When an object is uploaded, Amazon S3 uses the encryption key that the user provides to apply AES-256 encryption to the data and remove the encryption key from the memory.

Protecting Data Using Client-side Encryption

Client-side encryption ensures the security of a user's data by encrypting it locally before transmitting it to the Amazon S3 service.

The Amazon S3 service receives only the user’s encrypted data and does not play a role in encrypting or decrypting it.

AWS Encryption SDK

The AWS Encryption SDK is a powerful client-side encryption library designed for securing data across various AWS services.

- It provides a seamless solution for client-side encryption, allowing developers to encrypt data locally before transmitting it to AWS, which ensures that data remains secure during transit and storage.
- It leverages standardized data formats to ensure compatibility with various AWS services and libraries.

AWS Encryption SDK

Some of the AWS SDKs that support client-side encryption are as follows:

- AWS SDK for .NET
- AWS SDK for GO
- AWS SDK for Java
- AWS SDK for PHP
- AWS SDK for Ruby
- AWS SDK for C++

Demonstrating Server-Side Encryption Using S3 and KMS

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the utilization of Amazon S3 buckets with different server-side encryption options, SSE-S3, and SSE-KMS.

ASSISTED PRACTICE

Assisted Practice: Guidelines

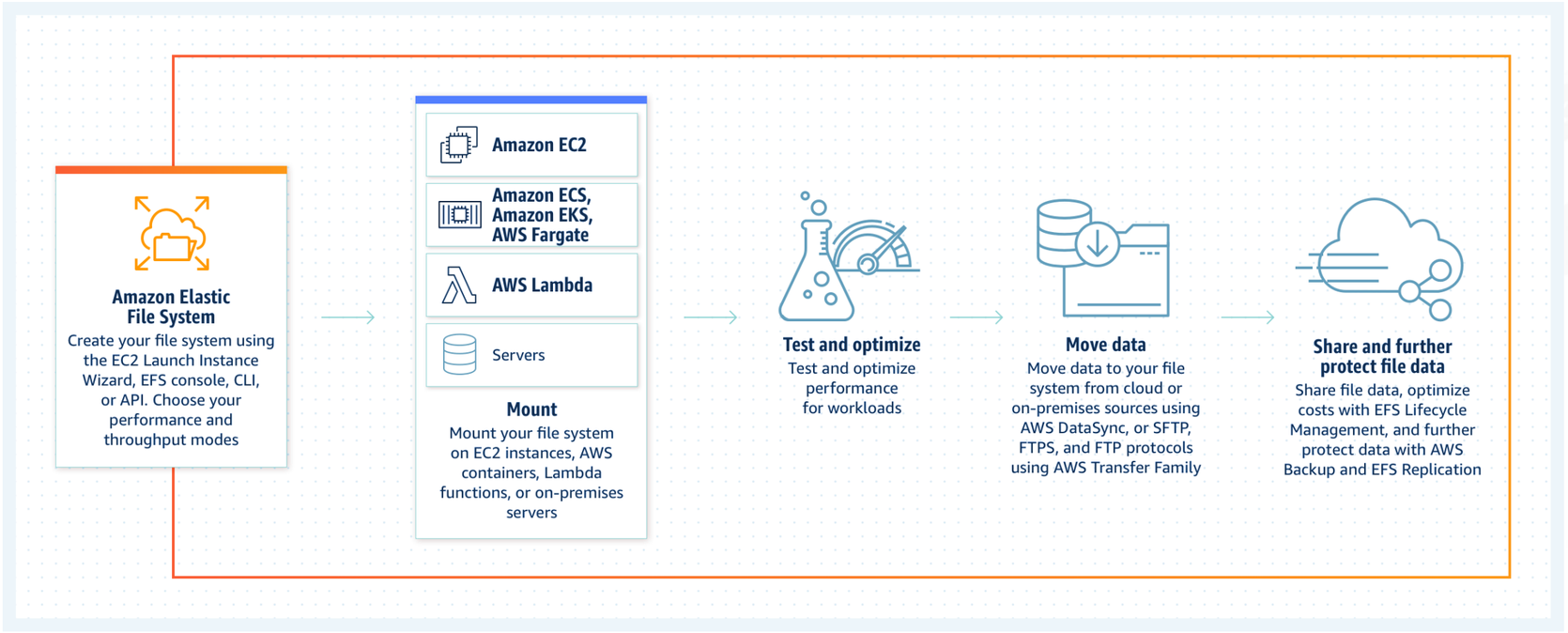
Steps to be followed are:

1. Create an S3 bucket with SSE-S3 encryption
2. Create a Key Management Service (KMS) key
3. Create an S3 bucket with SSE-KMS encryption

Elastic File System

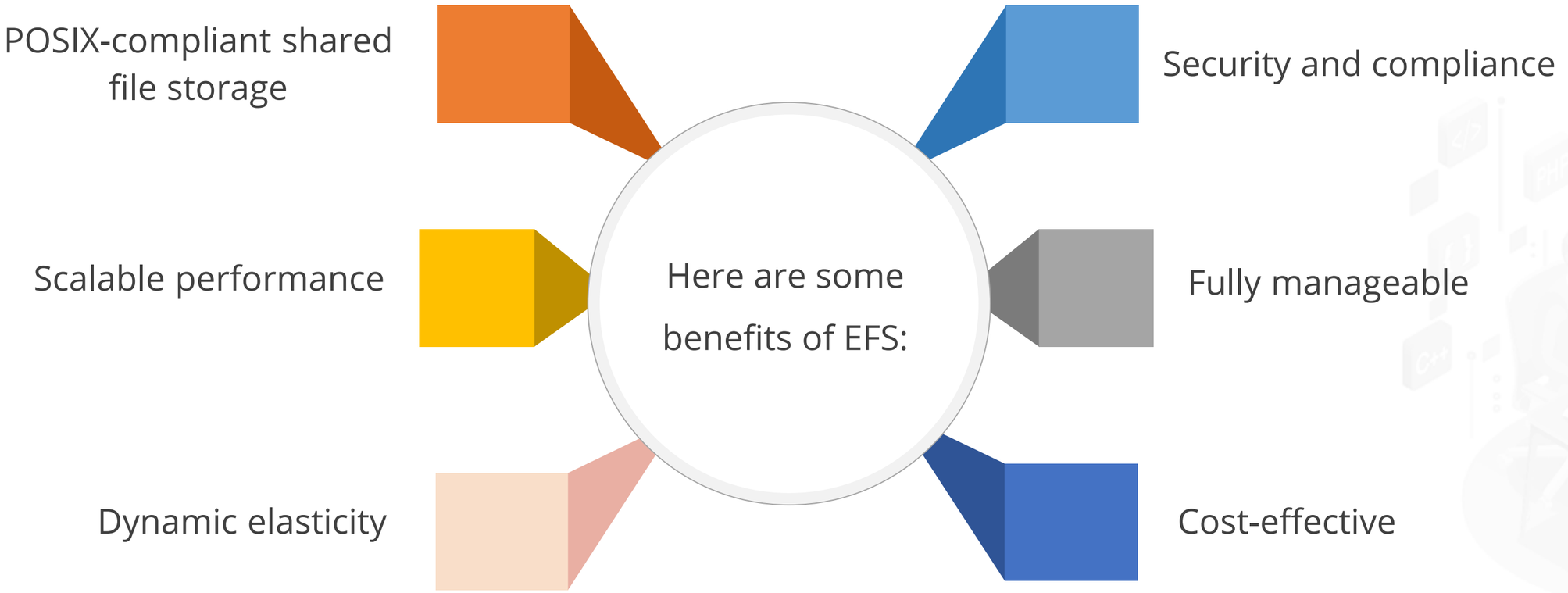
Amazon Elastic File System

Amazon EFS is a fully managed service that automatically scales based on demand.



It allows users to dynamically increase or decrease storage capacity as needed, making it suitable for a range of applications with varying storage requirements.

Elastic File System: Benefits



EFS vs. EBS

The differences between EFS and EBS are as follows:

Feature	EFS	EBS
Storage Size	No limitations	Maximum 16 TiB
Storage Type	Object storage	Block storage
Performance	Scalable	Hardly scalable
File Size Limitation	Maximum file size 47.9 TiB	No limitation
Data Throughput	Default throughput of 3 GB	SSD- and HDD-backed storage types
Data Access	Can be accessed concurrently	Limited to single EC2 instance
Availability Zone (AZ) Failure	Can survive one AZ failure	Cannot withstand AZ failure without snapshots

Creating and Mounting EFS on a Linux Server

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the creation, customization, and mounting of an Amazon Elastic File System (EFS) on multiple AWS instances.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create and customize an EFS
2. Create a security group to configure network access
3. Create AWS instances to access the EFS
4. Install EFS on the created instances

Amazon FSx

Amazon FSx

The Amazon FSx family of services makes it easy to launch, run, and scale shared storage powered by popular commercial and open-source file systems.

FSx – windows File server

FSx – Lustre

FSx Windows File server

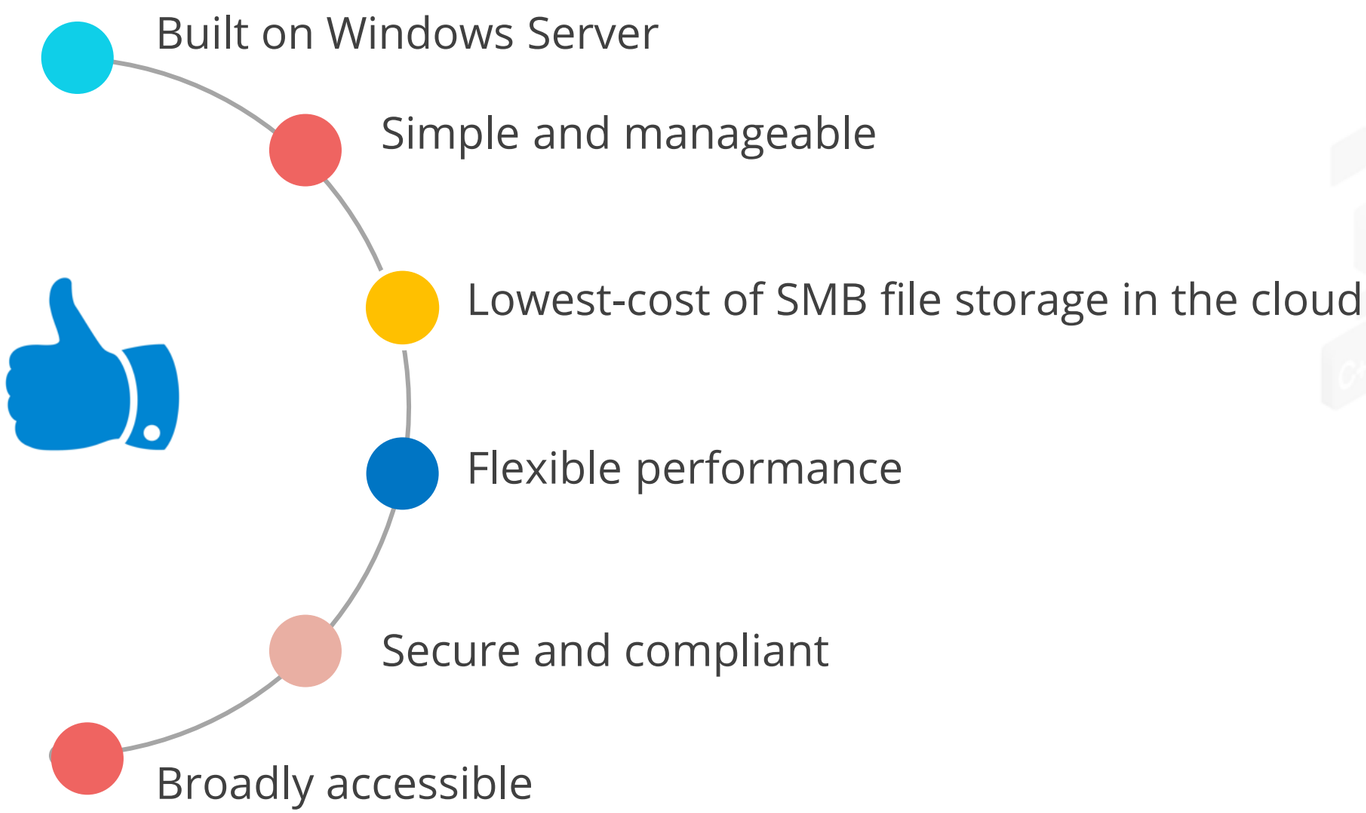
- The FSx for Windows File Server is a natively managed Windows file system that easily integrates with the entire AWS environment.
- Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage accessible over the industry-standard Server Message Block (SMB) protocol.

FSx Windows File server

- It is built on Windows Server, providing a wide range of administrative features that enhance usability and integration within the AWS environment.
- It offers single-AZ and multi-AZ deployment options, fully managed backups, and data encryption at rest and in transit.

Amazon FSx for Windows

Here are a few benefits of FSx for Windows:



Amazon FSx for Lustre

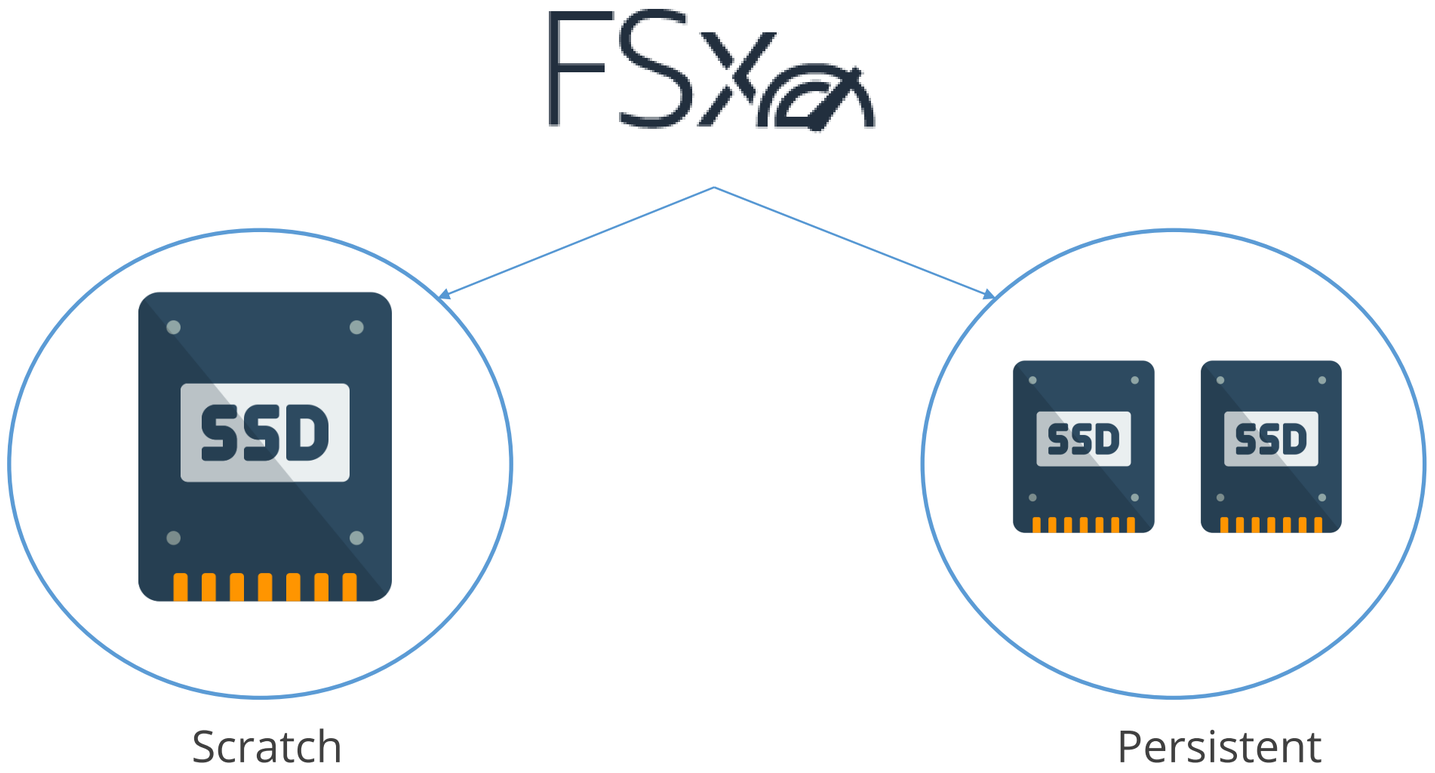
- Amazon FSx for Lustre is natively integrated and provides high-speed processing capabilities of up to 100+ GB/s.
- It leverages the open-source Lustre file system, which is specifically designed to meet the demands of applications requiring fast and high-performance storage.

Amazon FSx for Lustre

- Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system.
- Amazon FSx for Lustre integrates with Amazon S3, making it easy to use the Lustre file system to access data sets.

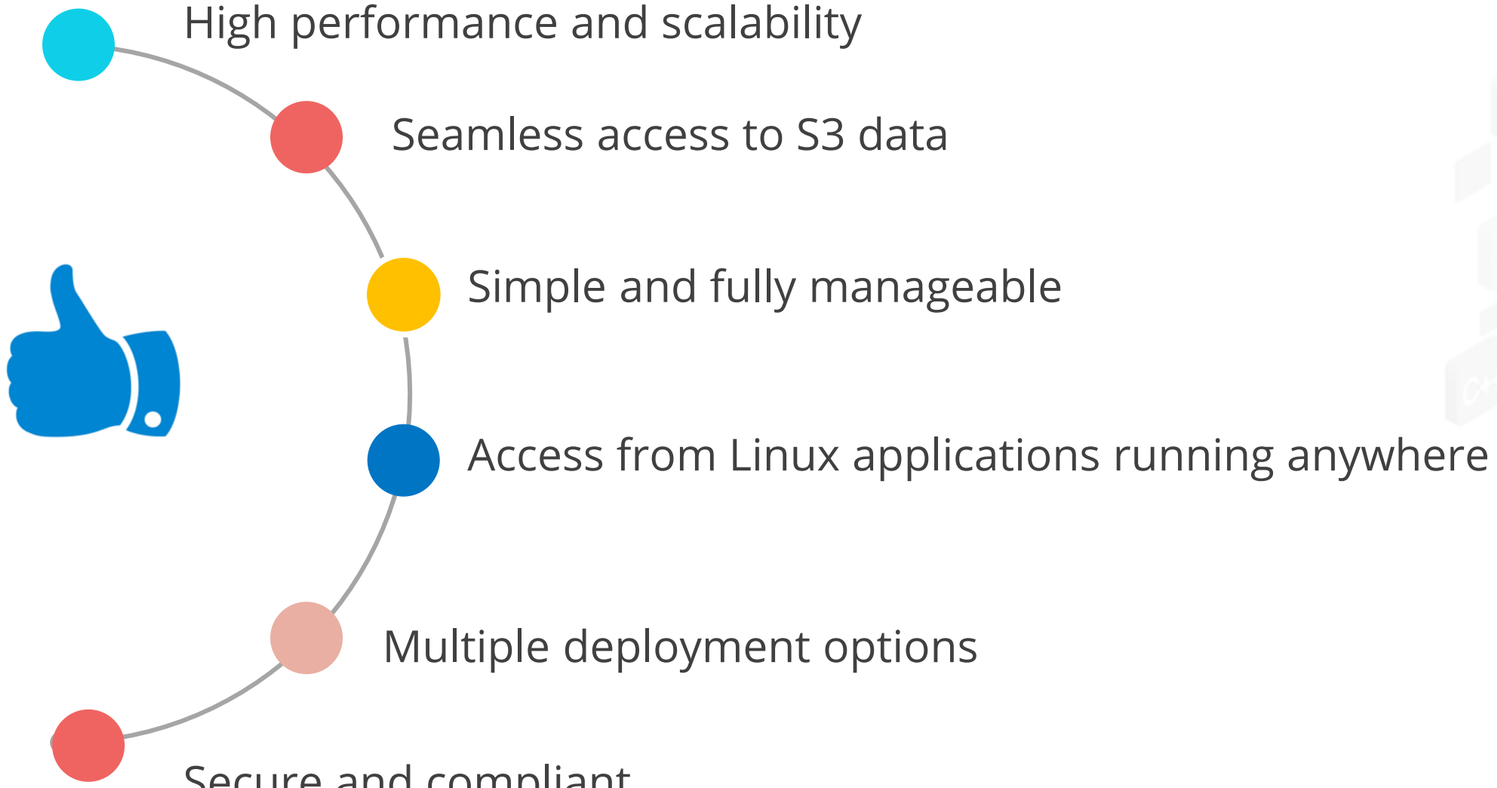
FSx Lustre Deployment Options

Amazon FSx for Lustre offers two deployment options to cater to different use cases: scratch file system and persistent file system.



Amazon FSx for Lustre

Here are a few benefits of FSx for Lustre:



Creating and Deleting Keys with Amazon KMS

Duration:15 min

Problem Statement:

You have been assigned a task to create and delete customer-managed keys using Amazon KMS.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a customer-managed key
2. Delete a customer-managed key

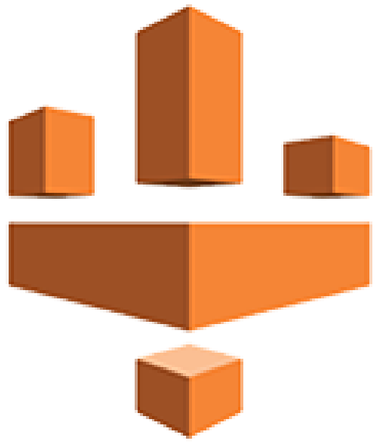
Unauthorized Link Access

Unauthorized Link Access

When a user attempts to use Amazon S3 to host a static website, there is a possibility of encountering an **Access Denied** error.

AWS Glue Data

AWS Glue is a serverless data integration service that simplifies the process of discovering, preparing, and combining data for various purposes, such as analytics, machine learning, and application development.



Amazon Glue

AWS Glue Data: Features

Faster data integration

Accelerated data integration enables diverse teams within the organization to collaboratively use AWS Glue, streamlining data tasks and expediting data analysis.

Data integration automation at scale

Utilize AWS Glue for effortless management of countless ETL jobs and data consolidation across various stores via SQL.

Serverless

AWS Glue operates serverlessly, handling resource provisioning, configuration, and scaling for your data integration tasks.

Building a Glue Data Catalog

Duration:15 min

Problem Statement:

You have been assigned a task to create a Glue Data Catalog using AWS Glue for seamless organization and efficient cataloging.

ASSISTED PRACTICE

Assisted Practice: Guidelines

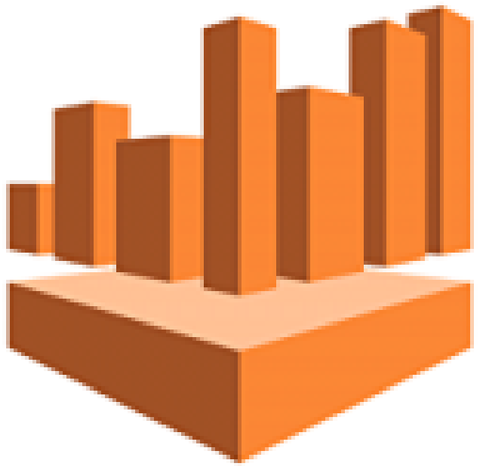
Steps to be followed are:

1. Create a VPC endpoint
2. Create a Glue Data Catalog
3. Add a data source to crawlers

Amazon Athena

Amazon Athena

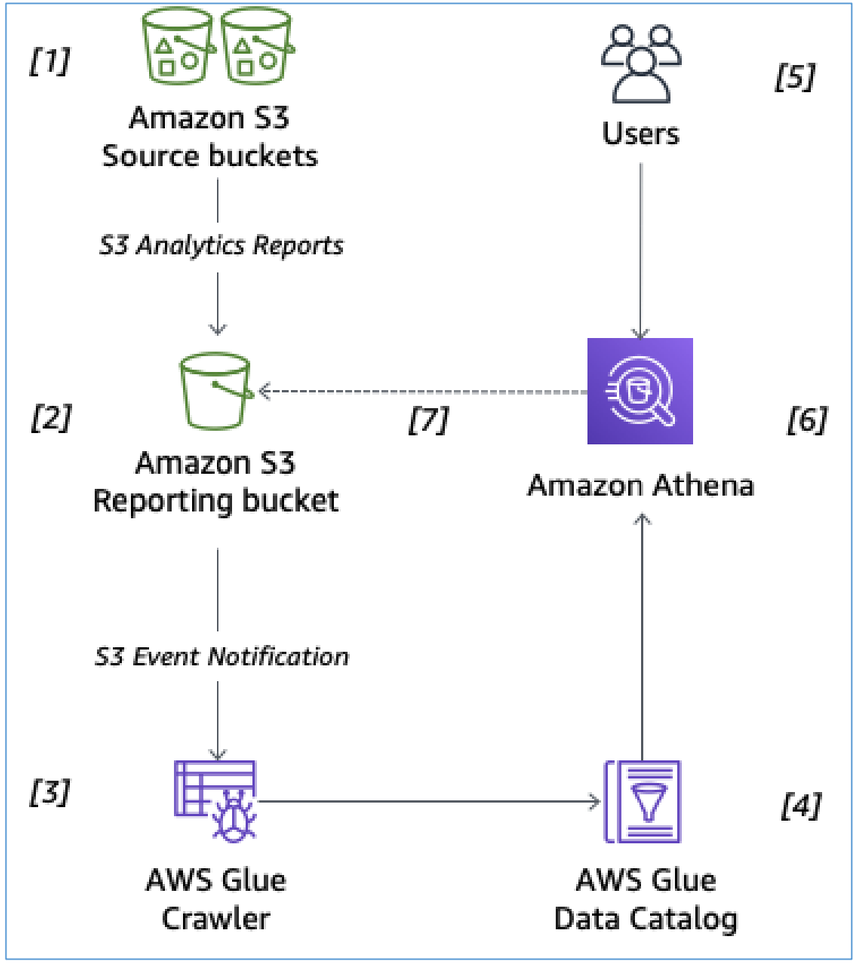
Amazon Athena is an interactive query service that enables easy data analysis of information stored in Amazon S3 using standard SQL. It operates in a serverless manner, eliminating the need for users to manage any underlying infrastructure.



Amazon Athena

Amazon Athena

Steps to query S3 analytics data with Amazon Athena:



Source: https://aws.amazon.com/blogs/storage/query-amazon-s3-analytics-data-with-amazon-athena/

Querying S3 Bucket Operations with Athena

Duration:15 min

Problem Statement:

You have been assigned a task to execute a query within AWS Athena for performing operations on a designated S3 bucket.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create S3 buckets
2. Execute queries in Athena

Key Takeaways

- The lifecycle configuration rule can be implemented in the S3 bucket to delete expired objects.
- The objects in the S3 bucket can be moved from a source bucket to a destination bucket by applying the replication rule.
- Server-side encryption can be enabled in an S3 bucket using the Key Management Service (KMS).
- EFS can be mounted on a Linux Server, and FSx can be mounted on a Windows Server with the help of a directory service.
- Amazon Athena is an interactive query service that allows easy data analysis in Amazon S3 using standard SQL.

Deploying Static Website with S3 Buckets

Duration: 30 mins

Project agenda: To demonstrate the implementation of S3 buckets for hosting static website content

Description: The organizational admin's goal is to deliver HTML content through a static website. This objective is achieved by utilizing the capabilities of an S3 bucket for seamless content deployment.

Perform the following:

1. Create an S3 bucket
2. Generate a bucket Policy
3. Enabling static website hosting
4. Test and verify the hosted website content

LESSON-END PROJECT

TECHNOLOGY

Thank You

simplilearn