



**Poll question**

aws

What type of storage are you or your teams using in your environments? Choose all that apply.

- A. Block storage
- B. File storage
- C. Object storage
- D. I don't know

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

## Module overview

- Business requests
- Storage services
- Amazon Simple Storage Service (Amazon S3)
- Shared file systems
- Data migration tools
- Present solutions
- Capstone check-in
- Knowledge check

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Business requests**



Storage Team Lead

The storage team lead needs to know:

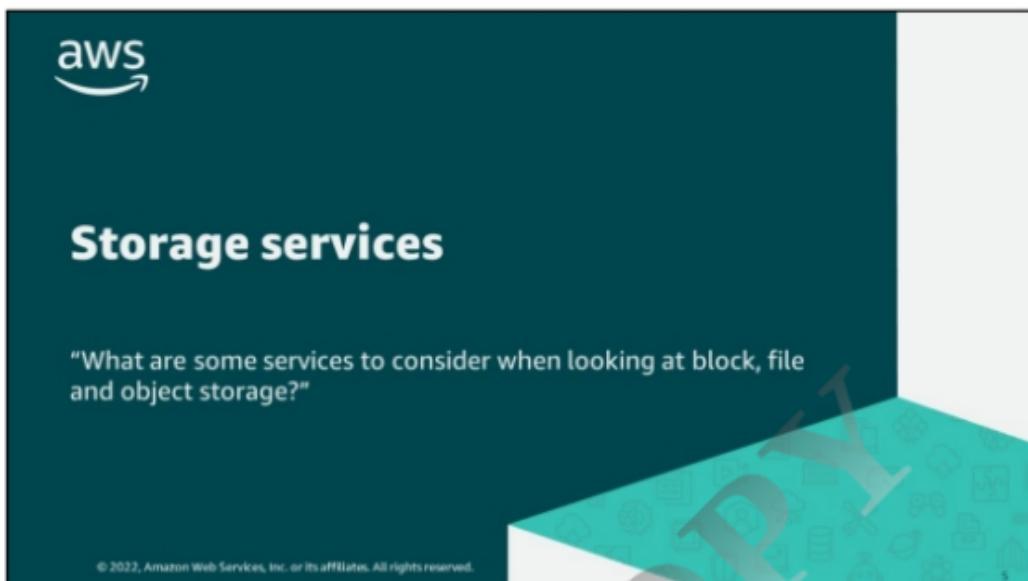
- What are some services to consider when looking at block, file and object storage?
- How do we choose the right object storage solution for my use case?
- What are some file-based options for building secure and scalable storage in the AWS Cloud?
- How can we move lots of data to the cloud in a relatively short time period?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

4

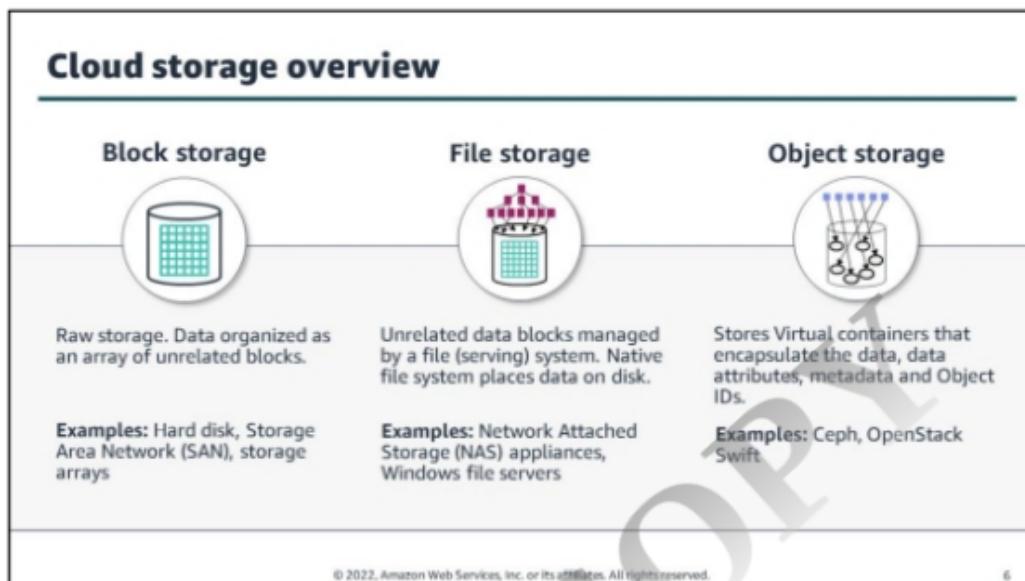
Imagine your storage team lead meets with you so they can understand how storage concepts translate to AWS. Here are some questions they are asking you.

At the end of this module, you will meet with the storage team lead and present some solutions.



The storage team lead asks, "What are some services to consider when looking at block, file and object storage?"

The storage team needs to compare and contrast AWS storage products and services, based on business scenarios.



There are three types of cloud storage: object, file, and block. Each storage option has a unique combination of performance, durability, cost, and interface.

**Block storage** – Enterprise applications like databases or enterprise resource planning (ERP) systems often require dedicated, low-latency storage for each host. This is similar to direct-attached storage (DAS) or a Storage Area Network (SAN). Block-based cloud storage solutions like Amazon Elastic Block Store (Amazon EBS) are provisioned with each virtual server and offer the ultra-low latency required for high-performance workloads.

**File storage** – Many applications must access shared files and require a file system. This type of storage is often supported with a Network Attached Storage (NAS) server. File storage solutions like Amazon Elastic File System (Amazon EFS) are ideal for use cases such as large content repositories, development environments, media stores, or user home directories.

**Object storage** – Applications developed in the cloud need the vast scalability and metadata of object storage. Object storage solutions like Amazon Simple Storage Service (Amazon S3) are ideal for building modern applications. Amazon S3 provides scale and flexibility. You can use it to import existing data stores for analytics, backup, or archive.

## AWS data building blocks

### Block Storage



Amazon Elastic  
Block Store  
(Amazon EBS)

### File Storage



Amazon Elastic  
File Service  
(Amazon EFS)



Amazon  
FSx

### Object Storage



Amazon Simple  
Storage Service  
(Amazon S3)



Amazon S3  
Glacier

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

7

AWS has solutions for your block, file and object storage needs. In this module, you will learn about the following services:

- Amazon EBS for block storage
- Amazon EFS and Amazon FSx for file storage
- Amazon S3 and Amazon S3 Glacier for object storage



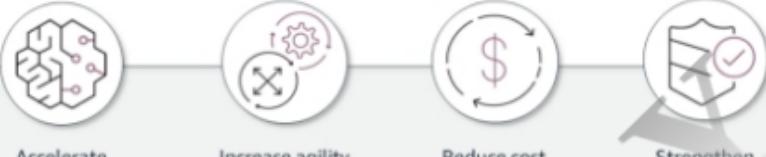
The storage team lead asks, "How do we choose the right object storage solution for my use case?"

The team needs to identify object storage classes to meet business needs.

## Amazon S3



Amazon Simple Storage Service (Amazon S3) is a durable object storage solution.



- Accelerate innovation
- Increase agility
- Reduce cost
- Strengthen security

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

9

Amazon S3 is *object-level storage*. An object includes file data, metadata, and a unique identifier. Object storage does not use a traditional file and folder structure.

Amazon S3 storage tiers are all designed to provide 99.99999999% (11 9's) of data durability of objects over a given year. By default, data in Amazon S3 is stored redundantly across multiple facilities and multiple devices in each facility. Amazon S3 can be accessed through the web-based AWS Management Console, programmatically through the API and SDKs, or with third-party solutions (which use the API and SDKs).

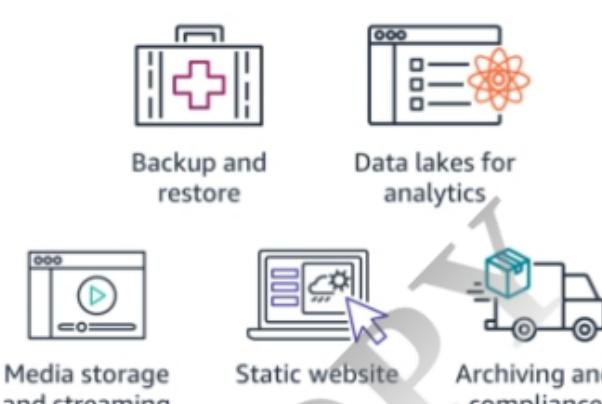
With Amazon S3, you can:

- **Accelerate innovation** – Integrate S3 buckets as storage solutions for static files and rely less on traditional file systems.
- **Increase agility** – With hosted object storage, you won't need to expand your storage as the quantity and size of data grows. Individual objects cannot be larger than 5 TB; however, you can store as much total data as you need.
- **Reduce cost** – Use the variety of storage tiers in Amazon S3 to spend less on infrequently accessed data. Archive data in S3 for your long-term storage needs.
- **Strengthen security** – Store your data in Amazon S3 and secure it from unauthorized access with encryption features and access management tools. S3 maintains compliance programs, such as PCI-DSS, HIPAA/HITECH, FedRAMP, EU Data Protection Directive, and FISMA, to help you meet regulatory requirements.

## Amazon S3 use cases

Use Amazon S3 when you have:

- Large number of users accessing your content
- Growing data sets
- Data you will write once and read many times



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

10

Amazon S3 provides you with flexible, low-cost object storage solutions. Some use cases for Amazon S3 include:

### Backup and restore

You can use Amazon S3 to store and retrieve any amount of data, at any time. You can use Amazon S3 as the durable store for your application data and file-level backup and restore processes. Amazon S3 is designed for 99.99999999 percent durability, or 11 9's of durability.

### Data lakes for analytics

Run big data analytics, artificial intelligence (AI), machine learning (ML), and high-performance computing (HPC) applications to unlock data insights.

### Media storage and streaming

You can use Amazon S3 with Amazon CloudFront's edge locations to host videos for on-demand viewing in a secure and scalable way. Video on demand (VOD) streaming means that your video content is stored on a server and viewers can watch it at any time. You'll learn more about Amazon CloudFront later in this course.

### Static website

You can use Amazon S3 to host a static website. On a *static* website, individual webpages include static content. They might also contain client-side scripts. Amazon S3's object storage makes it easier to manage data access, replications, and data protection for static files.

### Archiving and compliance

Replace your tape with low-cost cloud backup workflows, while maintaining corporate, contractual, and regulatory compliance requirements.

Consider other storage solutions when you:

- Are frequently changing the data
- Have block storage requirements

To learn more about how businesses are solving their storage challenges, see “How AWS Partners Are Utilizing Amazon S3 to Help Customers Solve for Scale” in the *AWS Partner Network (APN) Blog* (<https://aws.amazon.com/blogs/apn/how-aws-partners-are-utilizing-amazon-s3-to-help-customers-solve-for-scale/>).

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

## Buckets and objects

- Amazon S3 stores data as objects within buckets.
- An object includes a file and any metadata that describes the file.
- You can control access to the bucket and its objects.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

11

Amazon S3 stores data as objects within buckets. An *object* is composed of a file and any metadata that describes that file. To store an object in Amazon S3, upload the file into a *bucket*.

When you upload a file, you can set permissions on the object and add metadata. You can have one or more buckets in your account. For each bucket, you control who can create, delete, and list objects in the bucket. Choose the geographical AWS Region where Amazon S3 will store the bucket and its contents. You can access logs for the bucket and its objects. Amazon S3 allows up to 100 buckets in each account.

The diagram contains a virtual-hosted-style access URL made from a bucket and an object key. An object key is the unique identifier for an object in a bucket. The combination of a bucket, key, and version ID uniquely identifies each object. Every object can be uniquely addressed through the combination of the web service endpoint, bucket name, key, and optionally, a version.

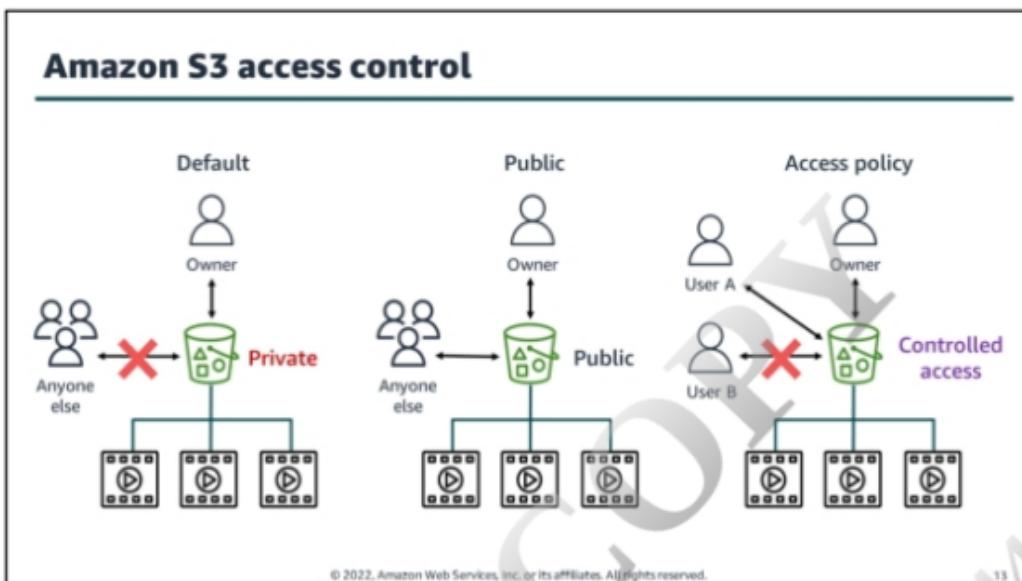
For example, in the URL <https://my-bucket.s3.amazonaws.com/2006-03-01/pup.jpg>, my-bucket is the name of the bucket and "2006-03-01/pup.jpg" is the key. The "2006-03-01/" portion of the object key is called the prefix. For more information on creating object key names, see "Creating object key names" in the *Amazon Simple Storage Service User Guide* (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-keys.html>).



Think about how physical objects in an office building or home are protected. There is more than one option for how you secure your items.

- Security guards
- A safe or a locker
- A key or key card system
- Rules for entry
- Employees only area

You use some or all of these depending on the type of objects you are caring for.



13

By default, all Amazon S3 resources—buckets, objects, and related resources (for example, lifecycle configuration and website configuration)—are private. Only the resource owner, an AWS account that created it, can access the resource. The resource owner can grant access permissions to others by writing access policies.

You can make a resource in Amazon S3 public which will allow anyone access. However, most Amazon S3 use cases do not require public access. Amazon S3 usually stores data from other applications. Public access is not recommended for these types of buckets. Amazon S3 includes a *block public access* feature. This acts as an additional layer of protection to prevent accidental exposure of customer data.

The resource owner can provide controlled access to a resource. You can grant access permissions to others by writing access policies.

For more information about Amazon S3 access control, see “[Blocking public access to your Amazon S3 storage](#)” in the *Amazon Simple Storage Service User Guide* (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>).

## Bucket policies

- Resource-based policy for an S3 bucket
- Controls access to a bucket without managing permissions in AWS Identity and Access Management (IAM)

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": "*", "Action": [ "s3>ListBucket", "s3:GetObject", ], "Resource": [ "arn:aws:s3:::doc-example-bucket", "arn:aws:s3:::doc-example-bucket/*", ] } ] }
```

Bucket policy in JSON format

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

15

You can create and configure bucket policies to grant permission to your Amazon S3 buckets and objects.

Bucket policies are resource-based policies for your S3 buckets. Access control for your data is based on policies, such as IAM policies, S3 bucket policies, and AWS Organizations service control policies (SCPs).

Use JSON-based access policy language to write your bucket policy. You can use it to add or deny permissions for the objects in your bucket.

In the example, the bucket policy allows any principal to list the bucket and get any object from the bucket. You should consider limiting public access to buckets and objects like this. Amazon S3 has tools that help you to prevent overly-permissive public buckets.

## Amazon S3 Block Public Access



**X** Block public ...

- access to buckets and objects granted through *new* ACLs
- access to buckets and objects granted through *any* ACLs
- access to buckets and objects granted through a *new* public bucket or access point policies
- cross-account access to buckets and objects through *any* public bucket or access point policies

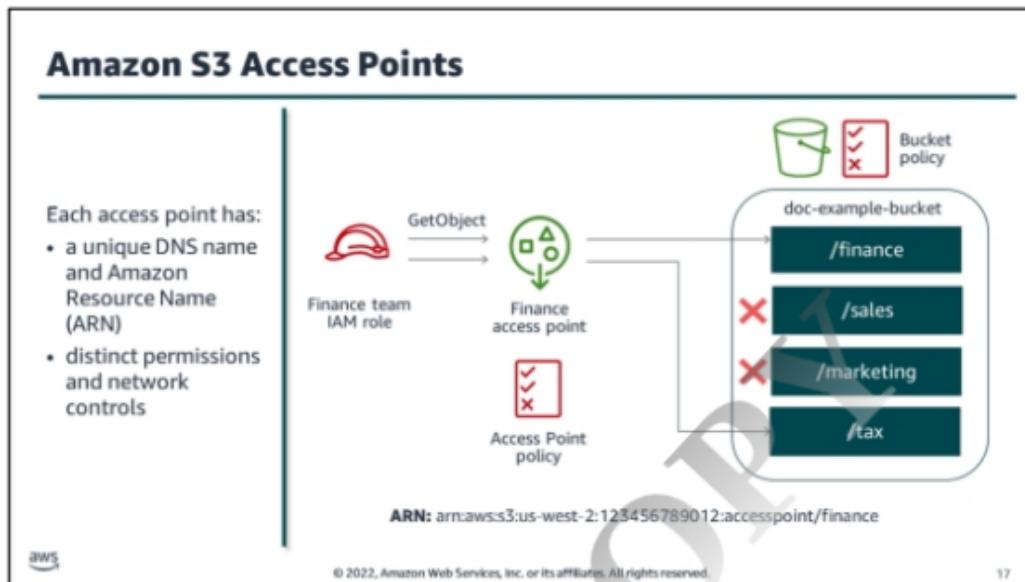
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

16

Sometimes you want to make sure that no matter what, a bucket will never see public access. Newly created Amazon S3 buckets and objects are private and protected by default. With Amazon S3 access control, you can stop all access to the bucket from ACLs, bucket policies, and cross-origin resource sharing (CORS) settings.

Public access is granted to buckets and objects through ACLs, bucket policies, or both. To avoid public access to all of your S3 buckets and objects, turn on *block all public access* at the account level. These settings apply account-wide for all current and future buckets.

You can protect yourself and your organization from information leaks by using S3 Block Public Access settings. Turn it on to prevent your operators from accidentally opening your buckets to the public.

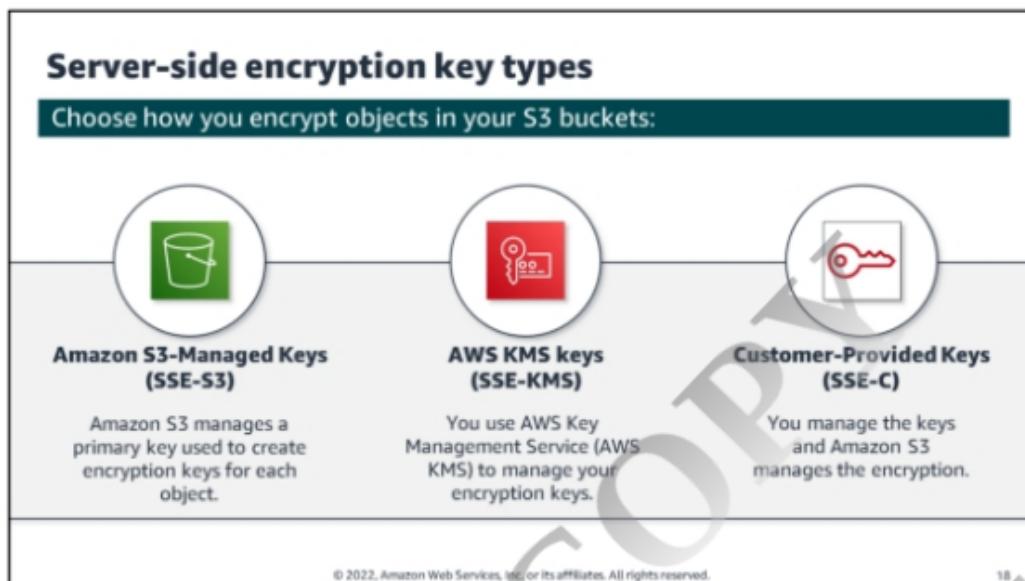


Amazon S3 Access Points simplify managing data access at scale for shared datasets in S3. S3 Access Points are named network endpoints that you can use to perform S3 object operations, such as `GetObject` and `PutObject`. Access points are attached to buckets. Each access point has distinct permissions and network controls that Amazon S3 applies for any request made through that access point.

In the example, a finance employee assumes the finance team IAM role and sends a `GetObject` request to your ‘finance’ access point. The access point policy allows the finance role to get objects in `doc-example-bucket` with the prefixes `/finance` and `/tax`. The finance role does not have access to your `sales` and `marketing` prefixed objects or any other objects in your S3 bucket. The S3 bucket policy allows the finance access point to have access to your bucket.

Each access point enforces a customized access point policy that works in conjunction with the bucket policy attached to the underlying bucket. To restrict Amazon S3 data access to a private network, you can configure an access point to accept requests only from a VPC. You can also configure custom block public access settings for each access point.

You can only use access points to perform operations on objects. You can't use access points to perform other Amazon S3 operations, such as modifying or deleting buckets. S3 Access Points work with some, but not all, AWS services and features. For example, you can't configure S3 Cross-Region Replication to operate through an access point.



Cryptographic keys are used to encrypt your data at rest. Amazon S3 offers three options for encrypting your objects:

#### Server-side encryption (SSE) with Amazon S3-managed keys (SSE-S3)

When you use SSE-S3, each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a primary key that it regularly rotates. Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard (AES-256) to encrypt your data.

#### Server-side encryption with AWS KMS keys stored in AWS Key Management Service (AWS KMS) (SSE-KMS)

KMS keys stored in SSE-KMS are similar to SSE-S3, but with some additional benefits and charges. There are separate permissions for the use of a KMS key that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you an audit trail that shows when your KMS key was used, and by whom.

#### Server-side Encryption with Customer-Provided Keys (SSE-C)

With SSE-C, you manage the encryption keys and Amazon S3 manages the encryption as it writes to disks. Also, Amazon S3 manages decryption when you access your objects.

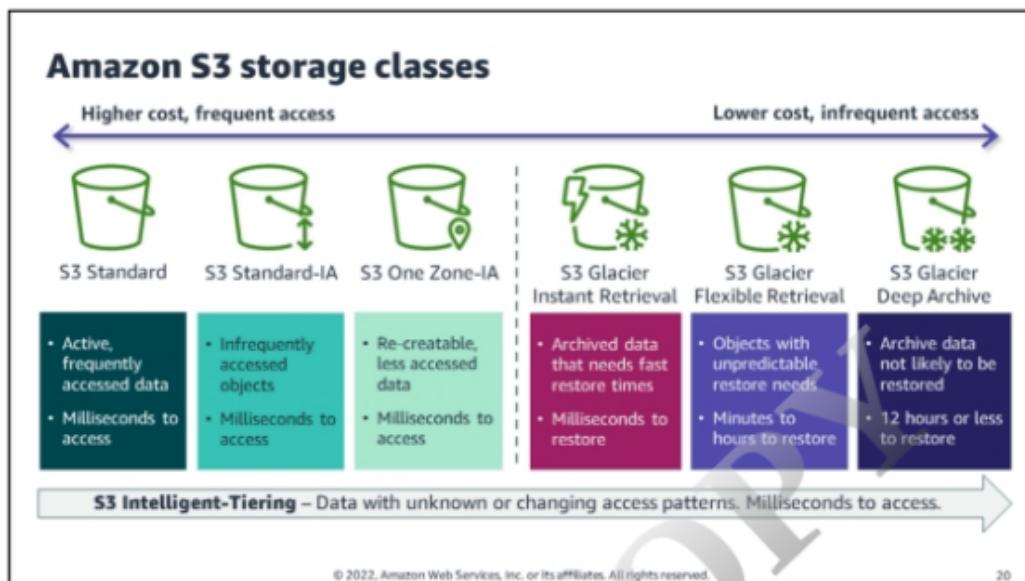
For more information on server-side encryption, see “Protecting data using server-side encryption” in the *Amazon Simple Storage Service User Guide* <https://docs.aws.amazon.com/AmazonS3/latest/userguide/server-side-encryption.html>.



Think about where you keep important objects in your office or home. There is more than one place to keep each thing.

- At your workplace
- Another room on the same floor
- The basement of the same building
- A different building near yours
- A storage unit in another location

You make decisions based on how often you use that object, and that decision can change over time. You choose Amazon S3 storage classes with similar considerations.



Each object in Amazon S3 has a storage class associated with it. All storage classes offer high durability (99.99999999 percent durability).

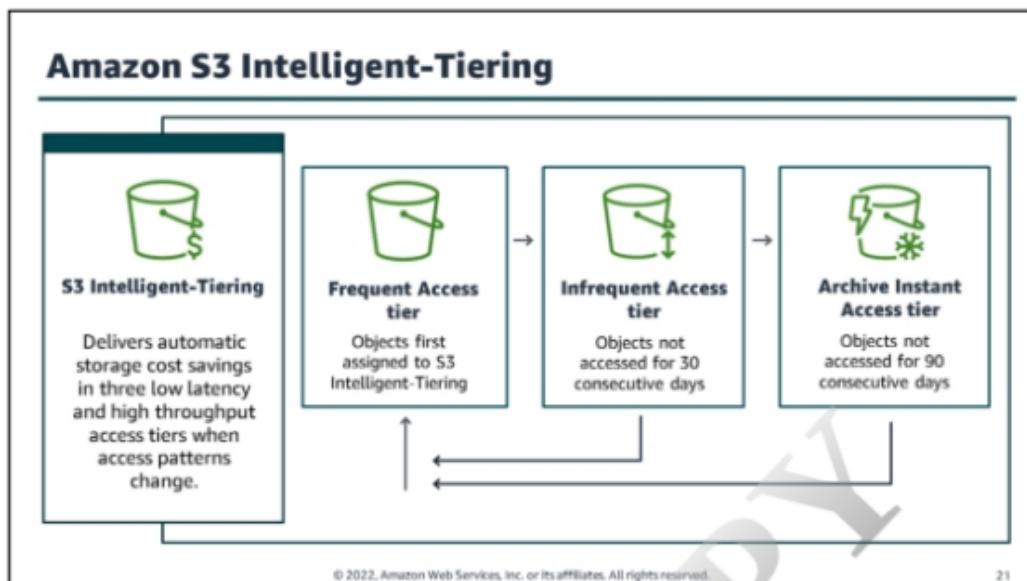
Choose a class depending on your use case scenario and performance access requirements:

- **S3 Standard** for general-purpose storage of frequently accessed data.
- **S3 Standard-Infrequent Access (S3 Standard-IA)** for long-lived, but less frequently accessed data.
- **S3 One Zone-Infrequent Access (S3 One Zone-IA)** for long-lived, less frequently accessed data that can be stored in a single Availability Zone.
- **S3 Glacier Instant Retrieval** for archive data that is rarely accessed but requires a restore in milliseconds.
- **S3 Glacier Flexible Retrieval** for the most flexible retrieval options that balance cost with access times ranging from minutes to hours. Your retrieval options permit you to access all the archives you need, when you need them, for one low storage price. This storage class comes with multiple retrieval options: expedited retrievals (restore in 1–5 minutes), standard retrievals (restore in 3–5 hours), or bulk retrievals (restore in 5–12 hours). Bulk retrievals are available at no additional charge.
- **S3 Glacier Deep Archive** for long-term cold storage archive and digital preservation. Your objects can be restored in 12 hours or less.

**S3 Intelligent-Tiering** is an additional storage class that provides flexibility for data with unknown or changing access patterns. It automates the movement of your objects between storage classes to optimize cost.

**S3 on Outposts** (not pictured) delivers object storage to your on-premises AWS Outposts environment. Outposts will be discussed later in this course.

For more information about choosing the right storage class based on your use and cost requirements, see “Amazon S3 pricing” (<https://aws.amazon.com/s3/pricing/>).



Amazon S3 Intelligent-Tiering is the only storage class that delivers you automatic storage cost savings when data access patterns change, without performance impact or operational overhead. Your data moves between access tiers as usage patterns change.

When you assign an object to S3 Intelligent-Tiering, it is placed in the Frequent Access tier which has the same storage cost as S3 Standard. Objects not accessed for 30 days are then moved to the Infrequent Access tier where the storage cost is the same as S3 Standard-IA. After 90 days of no access, an object is moved to the Archive Instant Access tier, which has the same cost as S3 Glacier Instant Retrieval.

S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period. You can use S3 Intelligent-Tiering as the default storage class for virtually any workload, especially data lakes, data analytics, new applications, and user-generated content.

## Amazon S3 Glacier storage class benefits

- 1 Cost-Effective storage**  
Lowest cost for specific data access patterns.
- 2 Flexible data retrieval**  
Three storage classes with variable access options.
- 3 Secure and compliant**  
Encryption at rest, AWS CloudTrail integration, and retrieval policies.
- 4 Scalable and durable**  
Meets needs from gigabytes to exabytes with 11 9s of durability



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. 22

Amazon S3 Glacier is a service that gives you extremely-low cost, powerful, and flexible data storage solutions. The storage is purpose-built for your archived data.

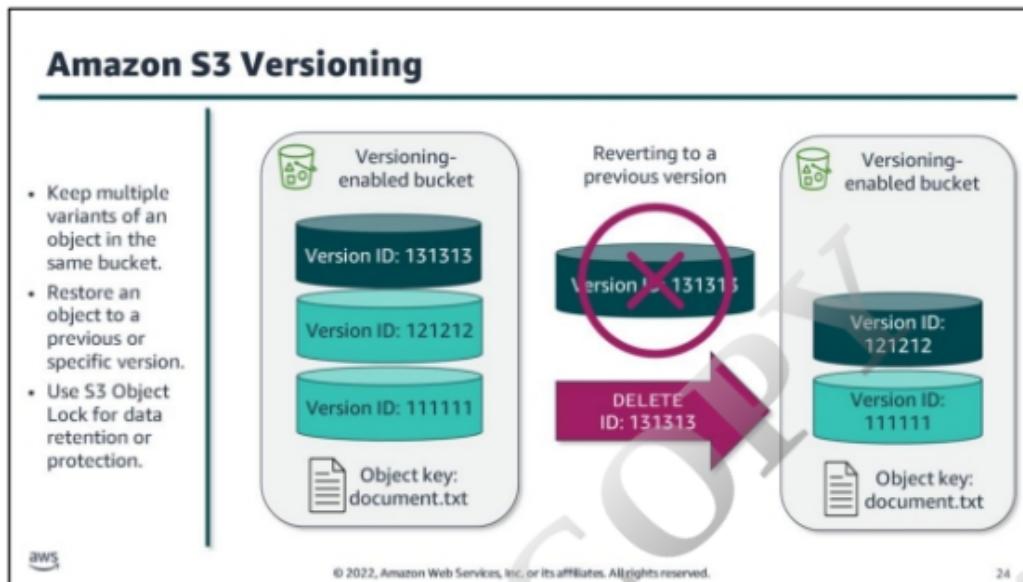
Three storage class options help optimize your cost for what you need to retrieve and how fast.

Your data in Amazon S3 Glacier can be encrypted at rest. In addition, Amazon S3 Glacier products offer you a suite of features including compliance, audit logging, and cost management. Those features may not be available to you with a traditional archiving solution.

Like other Amazon S3 storage classes, Amazon S3 Glacier products can scale from gigabytes to exabytes of your data. Amazon S3 Glacier storage classes have 99.99999999 percent durability.

In mathematical terms, 11 nines of durability means that out of 10,000 objects, you might expect to lose one every 10 million years. We asked a large Hollywood studio to run the same Markov model to determine the number of nines for two copies of data on tape and they came back with 5–6 nines. Having six more nines means that the durability of Amazon S3 Glacier is six orders of magnitude more durable than two copies of your data on tape.

For more information, see “Amazon S3 Glacier storage classes” (<https://aws.amazon.com/glacier/>).



Amazon S3 uses object storage. This means that if you want to change a part of a file, you must make the change and then re-upload the entire modified file.

Versioning-enabled buckets help you recover objects from accidental deletion or overwrite:

- If you delete an object, instead of removing it permanently, Amazon S3 inserts a *delete marker*, which becomes the current object version.
- If you overwrite an object, it results in a new object version in the bucket.

When S3 Versioning is turned on, you can restore the previous version of the object to correct the mistake.

In the diagram, a versioning-enabled bucket with an object that has three versions. The current version ID is 131313. You can restore to the previous version ID of 121212. To delete versioned objects permanently, you must use DELETE Object versionId. This example deletes version ID 131313.

You can use S3 Object Lock for data retention or protection. By using the write once, read many (WORM) model, you can prevent accidental overwrites or deletions within Amazon S3 storage. Use retention periods for locking an object for a fixed period of time, or a Legal Hold for a lock until explicitly removed.

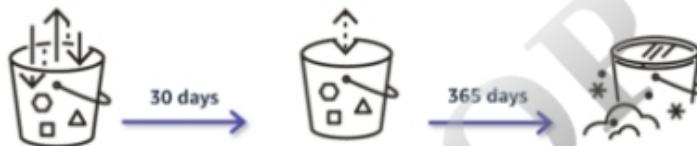
For more information on versioning, see “Using versioning in S3 buckets”  
(<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>).

For more information about S3 Object Lock, see “Using S3 Object Lock”  
(<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>).

## Lifecycle policies

Use S3 Lifecycle polices to transition objects to another storage class. S3 Lifecycle rules take action based on object age. Here's an example:

1. Move objects older than 30 days to S3 Standard-IA.
2. Move objects older than 365 days to Amazon S3 Glacier Deep Archive.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

25

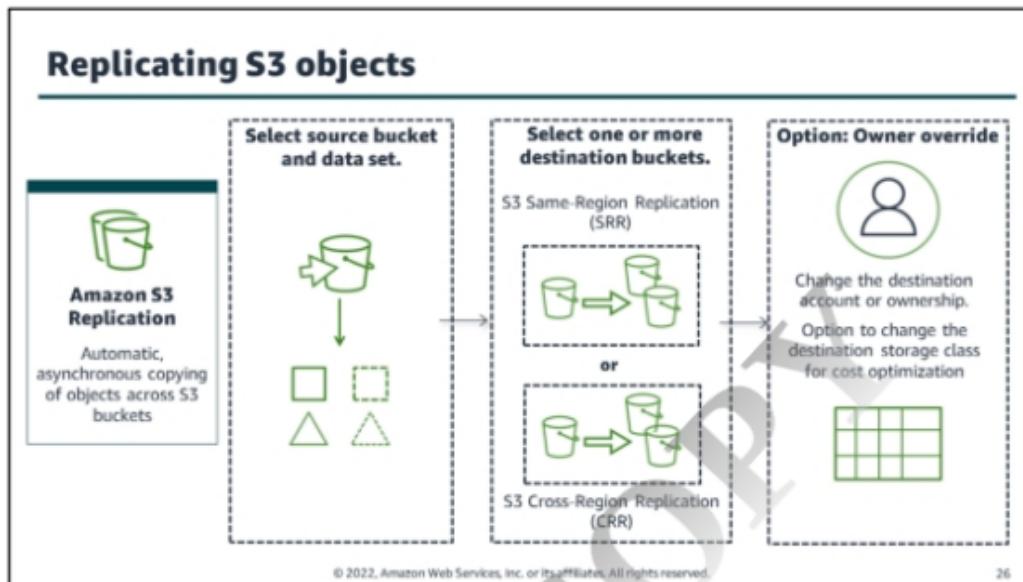
With S3 Lifecycle policies, you can delete or move objects based on age. You should automate the lifecycle of your data stored in Amazon S3. Using S3 Lifecycle policies, you can have data cycled at regular intervals between different Amazon S3 storage types.

This reduces your overall cost because you are paying less for data as it becomes less important with time. In addition to being able to set lifecycle rules *per object*, you can also set lifecycle rules *per bucket*.

Amazon S3 supports a waterfall model for transitioning between storage classes. **Lifecycle configuration** automatically changes data storage tiers.

For more information on transitioning objects and managing your storage lifecycle using S3 Lifecycle, see the following in the *Amazon Simple Storage Service User Guide*:

- “Transitioning objects using Amazon S3 Lifecycle” (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>).
- “Managing your storage lifecycle” (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>).



26

With Amazon S3, customers get a high level of availability and durability for their data in every AWS Region. Data stored in any Amazon S3 storage class is stored across a minimum of three Availability Zones, each separated by miles within a Region. For this reason, many AWS customers choose Amazon S3 to store their business-critical and application-critical data. The only exception is *S3 One Zone-IA*, which, as its name indicates, is a one-zone service.

Replication can help you do the following:

- **Replicate objects while retaining metadata** – Ensure that your replica is identical to the source object if it is necessary.
- **Replicate objects into different storage classes** – Use replication to directly put objects into S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, or another storage class in the destination buckets.
- **Maintain object copies under different ownership** – Tell Amazon S3 to change replica ownership to the AWS account that owns the destination bucket.
- **Keep objects stored over multiple AWS Regions** – Meet compliance requirements by replicating data to another AWS Region.

First, identify the source bucket and data set. Then, select one or more destination buckets. You can use Same-Region Replication (SRR) for things like log aggregation or replicating between development and production accounts. If you need to meet compliance or other requirements to have data in more than one geography, choose Cross-Region Replication.

Optionally, you can change the destination ownership of objects with an *owner override*. You might do this, for example, to restrict access to object replicas.

To learn how to meet business data resiliency, see “How to meet business data resiliency with Amazon S3 cross-Region replication” in the *AWS Public Sector Blog* (<https://aws.amazon.com/blogs/publicsector/how-to-meet-business-data-resiliency-s3-cross-region-replication/>).

To learn more about replication, see “Amazon S3 Replication” (<https://aws.amazon.com/s3/features/replication/>).

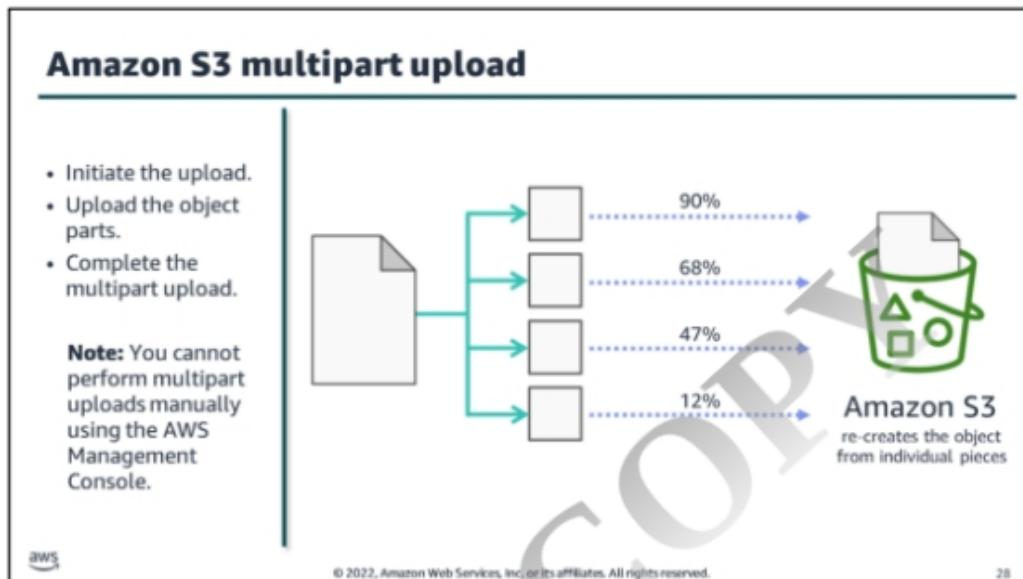
## Additional Amazon S3 features

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Earlier you were provided some examples that related to securing and storing objects. Next, think about how you might place objects into your S3 buckets. You want to be efficient with how you upload the object and use features that help you manage what happens once the object is there.

Consider the following questions:

- What if you need to upload large objects? How do you upload them and how does it work?
- How can you increase the speed at which objects are uploaded to AWS Regions that are not close to you?
- Can actions be automated based on events like when you upload an object?



With a multipart upload, you can consistently upload large objects in manageable parts. This process involves three steps:

- Initiating the upload
- Uploading the object parts
- Completing the multipart upload

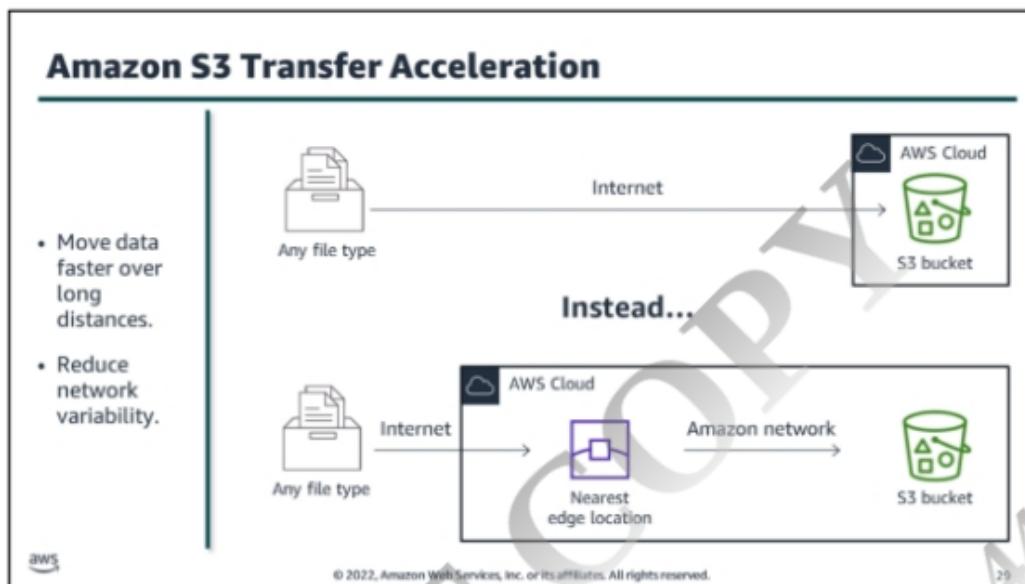
When the multipart upload request is completed, Amazon S3 will re-create the full object from the individual pieces.

Improve the upload process of larger objects with the following features:

- Improved throughput** – You can upload parts in parallel to improve throughput.
- Quick recovery from any network issues** – Smaller part sizes minimize the impact of restarting a failed upload due to a network error.
- Pausing and resuming object uploads** – You can upload object parts over time. When you have initiated a multipart upload, there is no expiration. You must explicitly complete or cancel the multipart upload.
- Beginning an upload before you know the final object size** – You can upload an object as you are creating it.
- Uploading large objects** – Using the multipart upload API, you can upload large objects, up to 5 TB.

**Note:** You cannot perform multipart uploads manually using the console.

For more information about multipart uploads, see “Uploading and copying objects using multipart upload” in the *Amazon Simple Storage Service User Guide* (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html>).



Amazon S3 Transfer Acceleration uses AWS globally-distributed edge locations to facilitate fast data transfer into an S3 bucket. The data is routed to Amazon S3 over an optimized network path.

Use Transfer Acceleration when you:

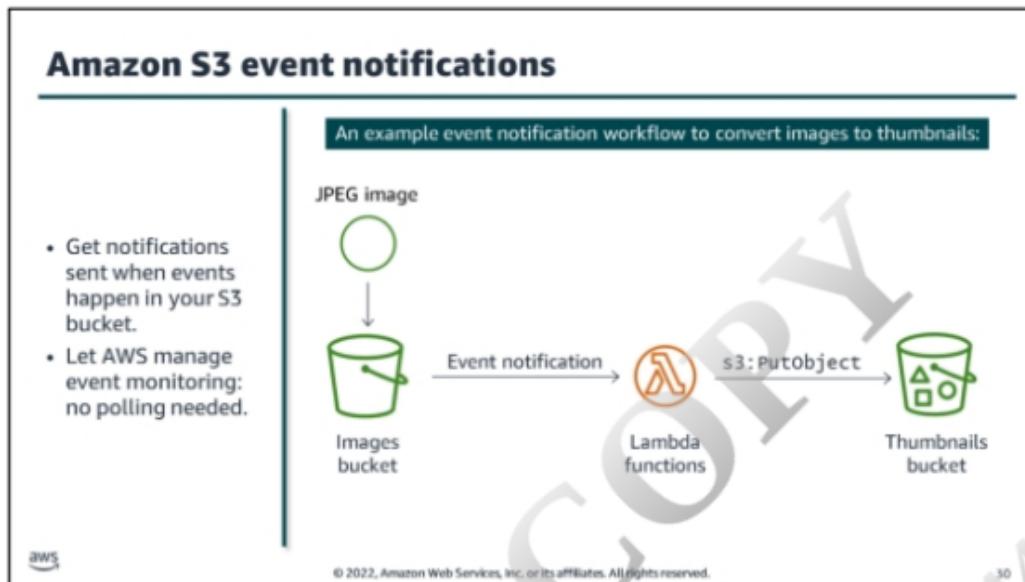
- Have customers all over the world who upload to a centralized bucket
- Transfer gigabytes or terabytes of data across continents on a regular basis
- Underutilize the available bandwidth when uploading to Amazon S3 over the internet

S3 Transfer Acceleration shortens the distance between client applications and AWS servers that acknowledge PUTS and GETS to Amazon S3 using a global network of hundreds of edge locations. AWS automatically routes your uploads and downloads through the closest edge locations to your application.

You can use the Amazon S3 Transfer Acceleration Speed Comparison tool to compare accelerated and non-accelerated upload speeds across Amazon S3 Regions.

For more information about Transfer Acceleration, see "S3 Transfer Acceleration" (<https://aws.amazon.com/s3/transfer-acceleration/>).

To learn more about the speed comparison tool, see "Using the Amazon S3 Transfer Acceleration Speed Comparison tool" in the *Amazon Simple Storage Service User Guide* (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration-speed-comparison.html>).



30

With Amazon S3 event notifications, you can receive notifications when certain object events happen in your bucket. Event-driven models like this mean that you no longer have to build or maintain server-based polling infrastructure to check for object changes. Nor do you have to pay for idle time of that infrastructure when there are no changes to process.

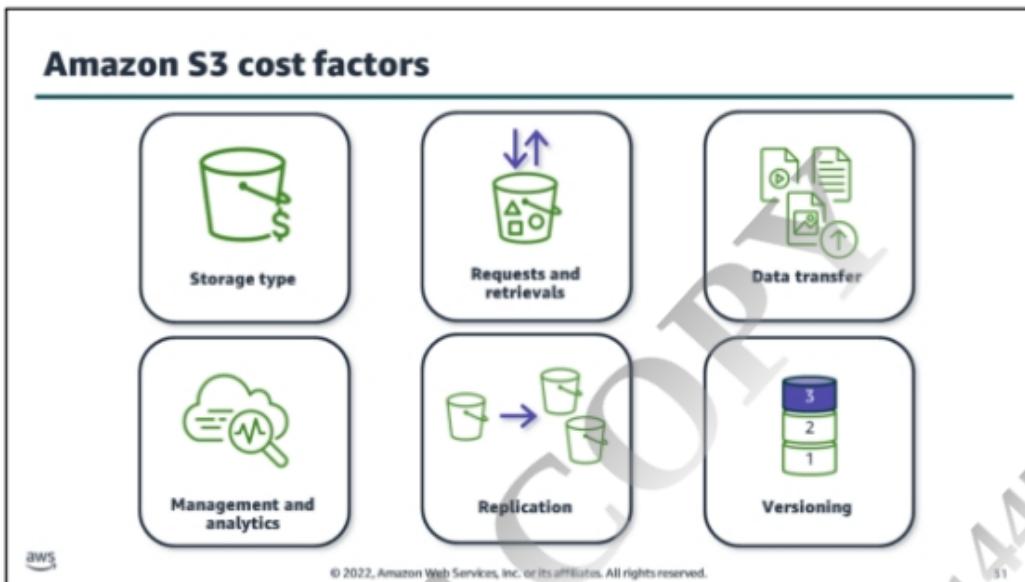
Amazon S3 can send event notification messages to the following destinations:

- Amazon Simple Notification Service (Amazon SNS) topics
- Amazon Simple Queue Service (Amazon SQS) queues
- AWS Lambda function

You specify the Amazon Resource Name (ARN) value of these destinations in the notification configuration.

In the example, you have a JPEG image uploaded to the images bucket used by your website. Your website needs to be able to show smaller “thumbnail” preview images of each uploaded file. When the image object is added to the S3 bucket, an event notification is sent to invoke a series of AWS Lambda functions. The output of your Lambda functions is a smaller version of the original JPEG image and puts the object in your thumbnails bucket. S3 event notifications manage the activity in the bucket for you and automate the creation of your thumbnail.

For more information about Amazon S3 event notifications, see “Reliable event processing with Amazon S3 event notifications on the AWS Storage Blog (<https://aws.amazon.com/blogs/storage/reliable-event-processing-with-amazon-s3-event-notifications/>).



Cost is an important part of choosing the right Amazon S3 storage solution.

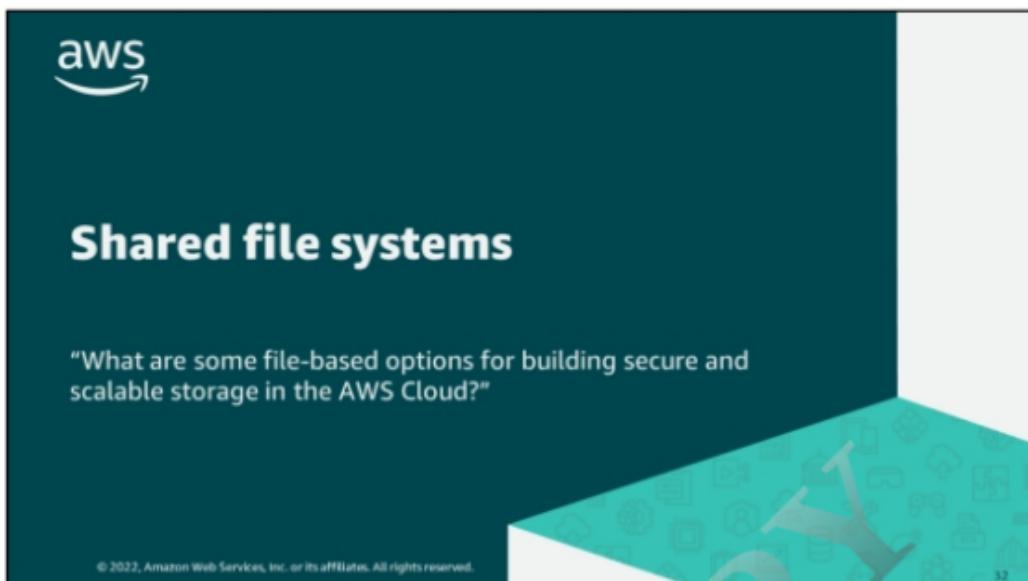
Some of the Amazon S3 cost factors to consider include:

- **Storage** – Per-gigabyte cost to hold your objects. You pay for storing objects in your S3 buckets. The rate you're charged depends on your objects' size, how long you stored the objects during the month, and the storage class. There are per-request ingest charges when using PUT, COPY, or lifecycle rules to move data into any S3 storage class.
- **Requests and retrievals** – The number of API calls: PUT and GET requests. You pay for requests made against your S3 buckets and objects. S3 request costs are based on the request type, and are charged on the quantity of requests. When you use the Amazon S3 console to browse your storage, you incur charges for GET, LIST, and other requests that are made to facilitate browsing.
- **Data transfer** – Usually no transfer fee for data-in from the internet and, depending on the requestor location and medium of data transfer, different charges for data-out.
- **Management and analytics** – You pay for the storage management features and analytics that are activated on your account's buckets. These features are not discussed in detail in this course.

**S3 Replication** and **S3 Versioning** can have a big impact on your AWS bill. These services both create multiple copies of your objects and you pay for each PUT request in addition to the storage tier charge. S3 Cross-Region Replication also requires data transfer between AWS Regions.

For more information about potential costs in Amazon S3, use the "AWS Pricing Calculator" (<https://calculator.aws/#/>).

For more information, see "Amazon S3 pricing" (<https://aws.amazon.com/s3/pricing/>).



The storage team lead asks, "What are some file-based options for building secure and scalable storage in the AWS Cloud?"

The storage team must know about AWS services that provide traditional file server solutions. The company wants your advice for how to choose the right service for their use case.

## Shared file systems

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



Amazon EBS is usually attached to one instance



Object storage is not built for file systems



Amazon EFS and Amazon FSx are ideal for this task

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

33

How do we handle an application running on multiple instances that must use the same file system?

Amazon EBS provides block storage, so it could be used as the underlying storage component of a self-managed file storage solution. Amazon EBS supports [multi-attach](#) for up to 16 Linux EC2 instance attachments, but it is a very specialized use case. In most cases, an EBS volume is attached to one EC2 instance. This limit makes it difficult to have the scalability, availability, and affordability of a fully managed file storage solution.

Amazon S3 is an option, but what if you need the performance and read/write capacity of a network file system? S3 is an object store system, not a block store, so changes overwrite entire files, not blocks of characters within files.

For high throughput changes to files of varying sizes, a file system will be superior to an object store system. Amazon Elastic File System (Amazon EFS) and Amazon FSx are ideal for this use case.

Using a fully managed cloud file storage solution removes complexities, reduces costs, and simplifies management. You will continue to learn about shared file systems in this section of the module.

For more information about the considerations and limitations of multi-attach, see “Attach a volume to multiple instances with Amazon EBS Multi-Attach” in the *Amazon Elastic Compute Cloud User Guide for Linux Instances* (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>).

## Amazon EFS

- Choose Amazon EFS for a scalable and elastic file system.
- Connect using the NFSv4 protocol.
- Access file systems across EC2 instances at the same time.

The diagram illustrates the architecture of Amazon EFS within a VPC. It shows three separate Availability Zones, each represented by a dashed box. Within each zone, there is a Private subnet (indicated by a blue lock icon) containing two EC2 instances (represented by orange square icons). Each instance is connected to a Mount Target (purple circle icon). Below the subnets, a central File system (represented by a green folder icon) is labeled "fs-12345678". Arrows indicate the connection from each Mount Target to the central file system. The entire setup is contained within a larger green box labeled "VPC".

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

34

Amazon EFS provides a scalable, elastic file system for Linux-based workloads for use with AWS Cloud services and on-premises resources.

You can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC through the Network File System (NFS) versions 4.0 and 4.1 (NFSv4) protocol. You do not need to take action to expand the file system as your storage needs grow.

Amazon EC2 instances in your VPC can access Amazon EFS file systems concurrently, so applications that scale beyond a single connection can access a file system.

Availability and durability refer to the redundancy with which an Amazon EFS file system stores data within an AWS Region. You have the following choices for your file system's availability and durability:

- Choosing a Standard storage class creates a file system that stores file system data and metadata redundantly across all Availability Zones within an AWS Region. You can also create mount targets in each Availability Zone in the AWS Region. Standard storage classes offer the highest levels of availability and durability.
- Choosing a One Zone storage class creates a file system that stores file system data and metadata redundantly within a single Availability Zone. File systems using One Zone storage classes can have only a single mount target which is located in the Availability Zone in which the file system is created.

In this example, a VPC uses Amazon EFS standard storage class. The VPC has three private subnets, each in a different AZ. With standard storage class, each subnet can have its own mount target. The EC2 instances in each subnet can access the file system through the mount target located in its AZ.

## Amazon EFS benefits

EFS uses burst throughput mode to **scale throughput** based on your storage use.



Additionally, you can **provision throughput** independent of storage.

EFS **automatically grows and shrinks** file storage without provisioning.



Monitoring is not required to avoid storage limits.

EFS managed file systems **lower your total cost of ownership (TCO)**. Pay only for what you use.



Save on cost with EFS Infrequent Access or One Zone storage types.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

35

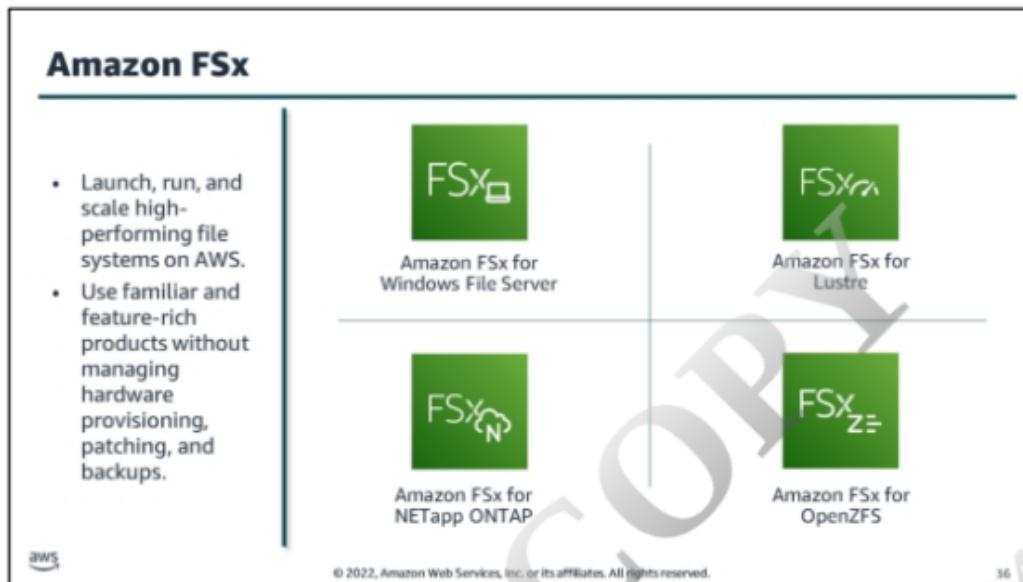
Amazon EFS provides a shared, persistent layer that allows stateful applications to elastically scale up and down. Examples include DevOps, web serving, web content systems, media processing, machine learning, analytics, search index, and stateful microservices applications. Amazon EFS can support a petabyte-scale file system, and the throughput of the file system also scales with the capacity of the file system.

Because Amazon EFS is serverless, you don't need to provision or manage the infrastructure or capacity. Amazon EFS file systems can be shared with up to tens of thousands of concurrent clients, no matter the type. These could be traditional EC2 instances, containers running in one of your self-managed clusters or in one of the AWS container services, Amazon ECS, Amazon EKS, and Fargate, or in a serverless function running in Lambda.

Use Amazon EFS to lower your total cost of ownership for shared file storage. Choose Amazon EFS One Zone for data that does not require replication across multiple Availability Zones and save on storage costs. Amazon EFS Standard-Infrequent Access (EFS Standard-IA) and Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA) are storage classes that provide price/performance that is cost-optimized for files not accessed every day.

Use Amazon EFS scaling and automation to save on management costs, and pay only for what you use.

For more information on Amazon EFS use cases, see “File Systems for Enterprise Applications” (<https://aws.amazon.com/efs/enterprise-applications/>).



With Amazon FSx, you can quickly launch and run feature-rich and high-performing file systems. The service provides you with four file systems to choose from. This choice is based on your familiarity with a given file system or by matching the feature sets, performance profiles, and data management capabilities to your needs.

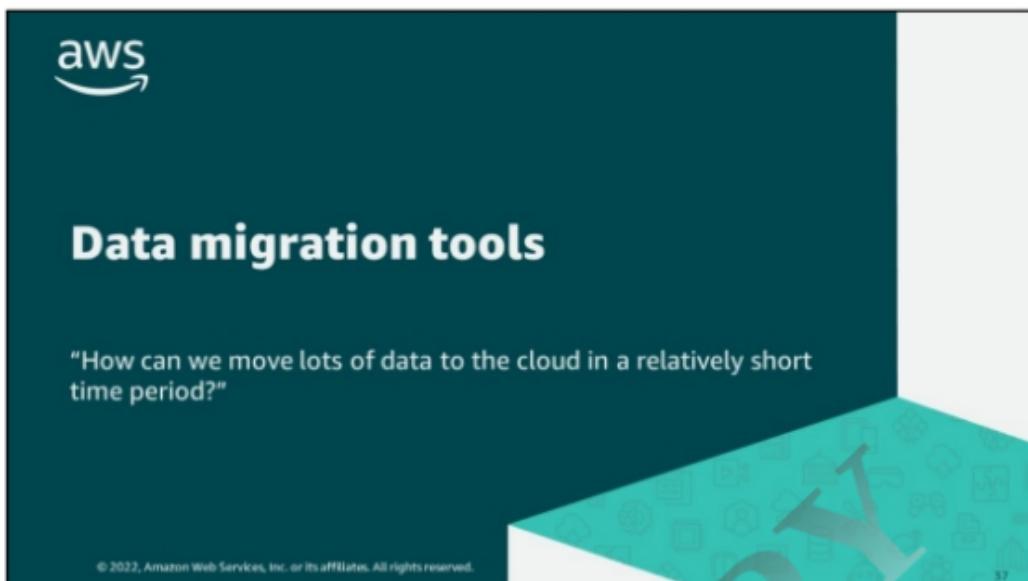
*FSx for Windows File Server* provides fully managed Microsoft Windows file servers that are backed by a native Windows file system. Built on Windows Server, Amazon FSx delivers a wide range of administrative features such as data deduplication, end-user file restore, and Microsoft Active Directory.

*FSx for Lustre* is a fully managed service that provides high-performance, cost-effective storage. FSx for Lustre is compatible with the most popular Linux-based AMIs, including Amazon Linux, Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, SUSE Linux, and Ubuntu.

*FSx for NETapp ONTAP* provides fully managed shared storage in the AWS Cloud with the popular data access and management capabilities of ONTAP.

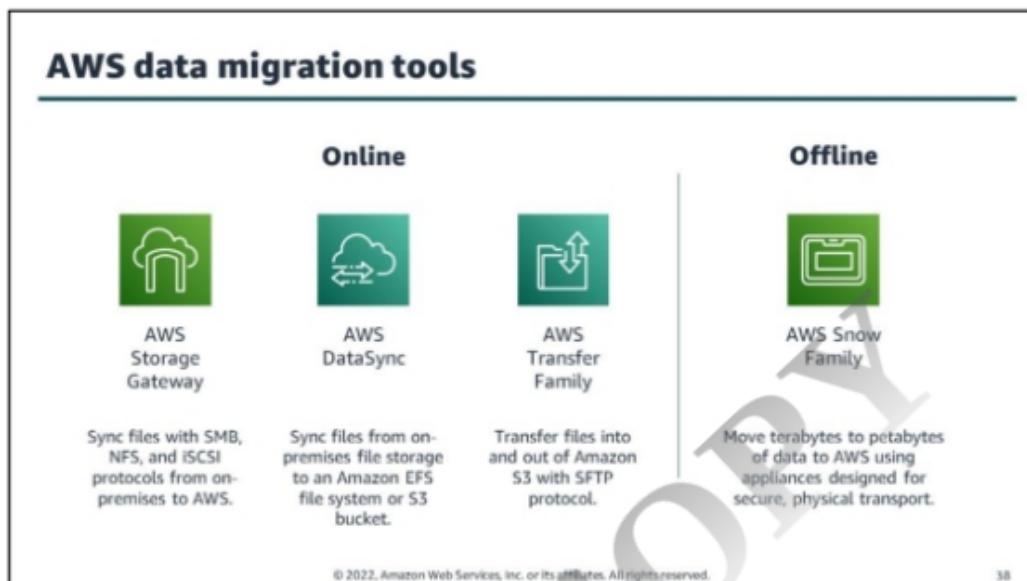
*FSx for OpenZFS* provides fully managed shared file storage built on the OpenZFS file system, powered by the AWS Graviton family of processors, and accessible via the NFS protocol (v3, v4, v4.1, v4.2).

For more information about Amazon FSx file system options, see “Choosing an Amazon FSx File System” (<https://aws.amazon.com/fsx/when-to-choose-fsx/>).



The storage team lead asks, "How can we move lots of data to the cloud in a relatively short time period?"

The storage team must plan data migrations from on-premises data centers to the AWS Cloud. The company wants your advice to choose the right tools.



Before selecting what tool to use, you should know the following:

- Where you are moving data
- For what use cases
- The types of data you are moving
- The network resources available

AWS offers a wide variety of services and Partner tools to help you migrate your data sets (files, databases, machine images, block volumes, or tape backups). In this module, you will learn about the following tools:

- *AWS Storage Gateway* simplifies on-premises adoption of AWS storage. Storage Gateway lets you seamlessly connect and extend your on-premises applications to AWS storage. It supports multiple file transfer protocols: server message block (SMB), network file sharing (NFS), and internet small computer systems interface (iSCSI).
- *AWS DataSync* is a data transfer service that facilitates moving data between on-premises storage and Amazon S3, Amazon EFS, or FSx for Windows File Server.
- *The AWS Transfer Family* permits the transfer of files into and out of Amazon S3 using the secure file transfer protocol (SFTP). The Transfer Family will not be covered in this course.
- *AWS Snow Family* is a group of edge computing, data migration, or edge storage devices designed for secure, physical transport.

For more information about on-premises AWS storage services, see “Comparing your on-premises storage patterns with AWS Storage services” in the *AWS Storage Blog*

(<https://aws.amazon.com/blogs/storage/comparing-your-on-premises-storage-patterns-with-aws-storage-services/>).

## AWS Storage Gateway



AWS Storage Gateway is a service that gives your applications seamless and secure integration between on-premises environments and AWS storage.

It provides you low-latency access to cloud data with a Storage Gateway appliance.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

39

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure.

You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security. Storage Gateway offers file-based, volume-based, and tape-based storage solutions integrated with AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), AWS CloudTrail, and Amazon CloudWatch.

## Storage Gateway types

Amazon S3  
File GatewayAmazon FSx File  
Gateway

Tape Gateway



Volume Gateway

Native file access to Amazon S3 for backups, archives, and ingest for data lakes.

Native access to Amazon FSx for Windows File Server for on-premises group file shares and home directories.

Virtual tape library using Amazon S3 archive tiers for long-term retention.

Block-level backups of volumes with Amazon EBS snapshots, AWS Backup integration, and cloud recovery.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

40

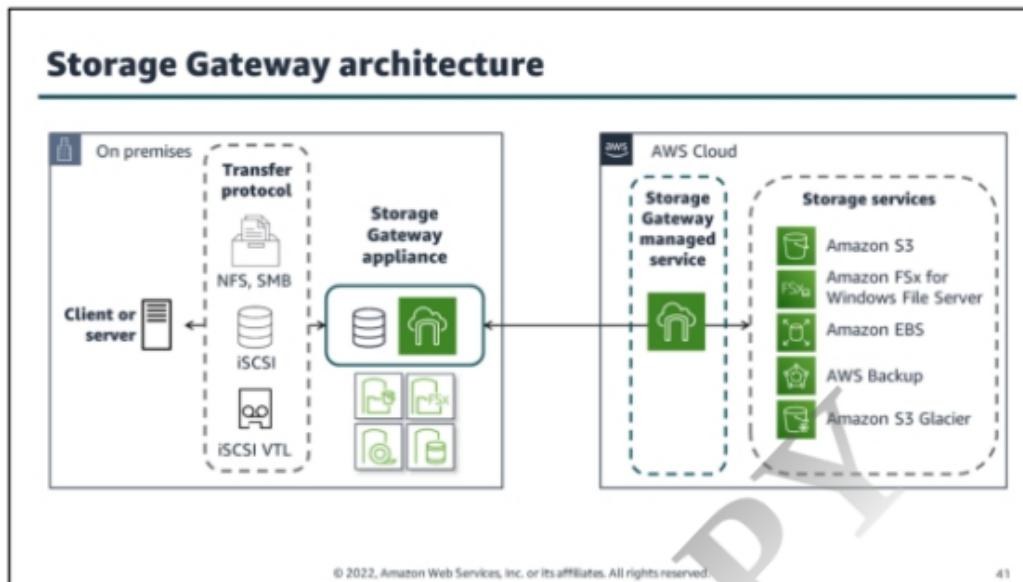
Choose a Storage Gateway type that is the best fit for your workload.

*Amazon S3 File Gateway* presents a file interface you can use to store files as objects in Amazon S3 using the industry-standard NFS and SMB file protocols. Access your files via NFS and SMB from your data center or Amazon EC2, or access those files as objects directly in Amazon S3.

*Amazon FSx File Gateway* provides fast, low-latency on-premises access to fully managed, highly reliable, and scalable file shares. It uses the industry-standard SMB protocol. You can store and access file data in Amazon FSx with Microsoft Windows features including full NTFS support, shadow copies, and Access Control Lists (ACLs).

*Tape Gateway* presents an iSCSI-based virtual tape library (VTL) of virtual tape drives and a virtual media changer to your on-premises backup application. Tape Gateway stores your virtual tapes in Amazon S3 and creates new ones automatically, simplifying management and your transition to AWS.

*Volume Gateway* presents block storage volumes of your applications using the iSCSI protocol. You can asynchronously back up data written to these volumes as point-in-time snapshots of your volumes, and store it in the cloud as Amazon EBS snapshots. You can back up your on-premises Volume Gateway volumes using the service's snapshot scheduler or by using the AWS Backup service.



41

The Storage Gateway Appliance supports the following protocols to connect to your local data:

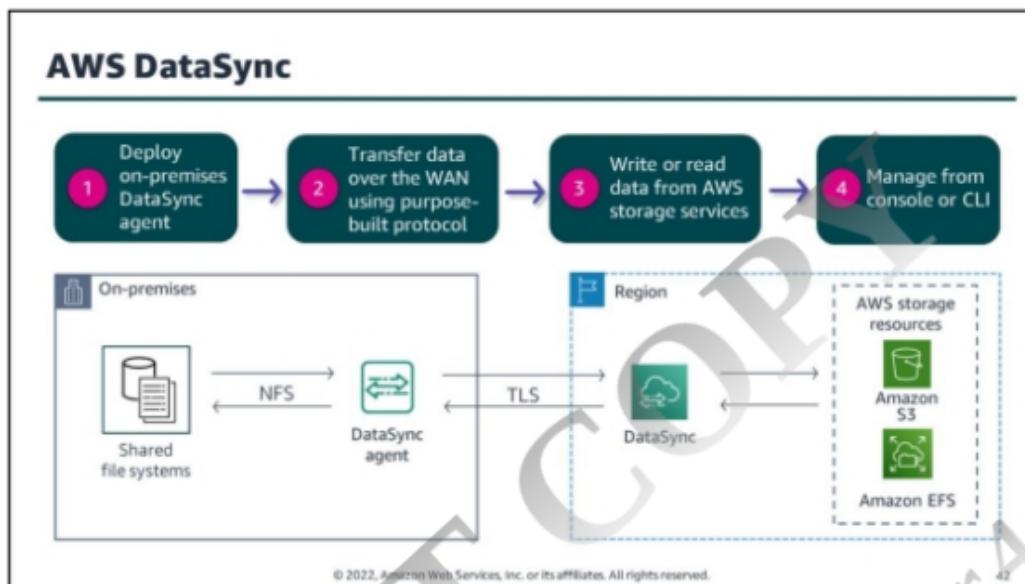
- NFS or SMB for files
- iSCSI for volumes
- iSCSI VTL for tapes

Your storage gateway appliance runs in one of four modes: Amazon S3 File Gateway, Amazon FSx File Gateway, Tape Gateway, or Volume Gateway.

Data moved to AWS using Storage Gateway can be sent to the following destinations through the Storage Gateway managed service:

- Amazon S3 (Amazon S3 File Gateway, Tape Gateway)
- Amazon S3 Glacier (Amazon S3 File Gateway, Tape Gateway)
- Amazon FSx for Windows File Server (Amazon FSx File Gateway)
- Amazon EBS (Volume Gateway)

AWS Backup can be used to schedule volume snapshots with Volume Gateway.



Manual tasks related to data transfers can slow down migrations and burden IT operations. DataSync facilitates moving large amounts of data between on-premises storage and Amazon S3 and Amazon EFS, or FSx for Windows File Server. By default, data is encrypted in transit using Transport Layer Security (TLS) 1.2. DataSync automatically handles scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network usage.

Reduce on-premises storage infrastructure by shifting SMB-based data stores and content repositories from file servers and NAS arrays to Amazon S3 and Amazon EFS for analytics.

DataSync deploys as a single software agent that can connect to multiple shared file systems and run multiple tasks. The software agent is typically deployed on premises through a virtual machine to handle the transfer of data over the wide area network (WAN) to AWS. On the AWS side, the agent connects to the DataSync service infrastructure. Because DataSync is a service, there is no infrastructure for customers to set up or maintain in the cloud. DataSync configuration is managed directly from the console.

## AWS Snow Family service models



### AWS Snowcone

Snowcone is a small, rugged, edge computing and data storage product.



### AWS Snowball Edge

Snowball Edge is an edge computing and data transfer device provided by the AWS Snowball service.



### AWS Snowmobile

Snowmobile is the first exabyte-scale data migration service to move very large datasets from on-premises to AWS.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

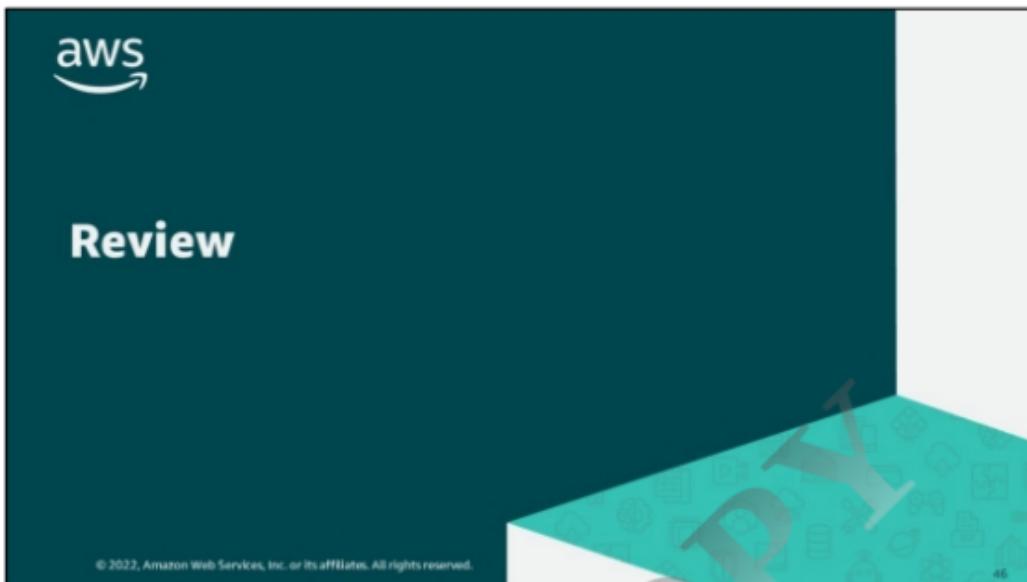
43

*AWS Snowcone* is ruggedized, secure, and purpose-built for use outside of a traditional data center. Its small size makes it a perfect fit for tight spaces or where portability is a necessity and network connectivity is unreliable. For more information, see “AWS Snowcone” (<https://aws.amazon.com/snowcone/>).

*Snowball Edge* is a petabyte-scale data transport option that doesn’t require you to write code or purchase hardware to transfer data. All you need to do is create a job in the console and a Snowball appliance will be shipped to you. Attach the appliance into your local network and transfer the files directly onto it. When the device is ready to be returned, the E Ink shipping label will automatically update the return address, ensuring that the device is delivered to the correct AWS facility. For more information, see “AWS Snowball FAQs” (<https://aws.amazon.com/snowball/faqs/>).

*Snowball Edge Optimized* is ideal for edge processing usage cases that require additional computing, memory, and storage power in remote, disconnected, or harsh environments. For more information, see “AWS Snowball Edge Specifications” (<https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html>).

*AWS Snowmobile* is a ruggedized shipping container pulled by a semi-trailer truck. You can transfer 100 PB per Snowmobile. Snowmobile uses multiple layers of security designed to protect your data. For more information, see “AWS Snowmobile” (<https://aws.amazon.com/snowmobile/>).



DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Present solutions**



Storage Team Lead

AWS

Consider how you would answer the following:

- What are some services to consider when looking at block, file and object storage?
- How do we choose the right object storage solution for my use case?
- What are some file-based options for building secure and scalable storage in the AWS Cloud?
- How can we move lots of data to the cloud in a relatively short time period?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

47

Imagine you are now ready to talk to the storage team lead and present solutions that meet their architectural needs.

Your answers should include the following solutions:

- Use Amazon EBS for block-level storage. Amazon S3 and S3 Glacier have object-level storage options to review. For file-level storage, choose Amazon EFS or Amazon FSx.
- Review the Amazon S3 storage classes. Think about the objects you are storing and how often they will be accessed. Use that information to choose a cost-effective solution. Consider using Amazon S3 Glacier for long-term archive data.
- Amazon EFS is a quick, easy, and scalable file storage solution that supports the NFS protocol. For more specialized solutions, learn more about the Amazon FSx family of services.
- To move data from one source to another destination, use AWS Datasync. For hybrid storage solutions, use AWS Storage Gateway. For an offline way to move data from on-premises to AWS Cloud destinations, use the AWS Snow Family.

## Module review

In this module you learned about:

- ✓ Storage services
- ✓ Amazon S3
- ✓ Shared file systems
- ✓ Data migration tools

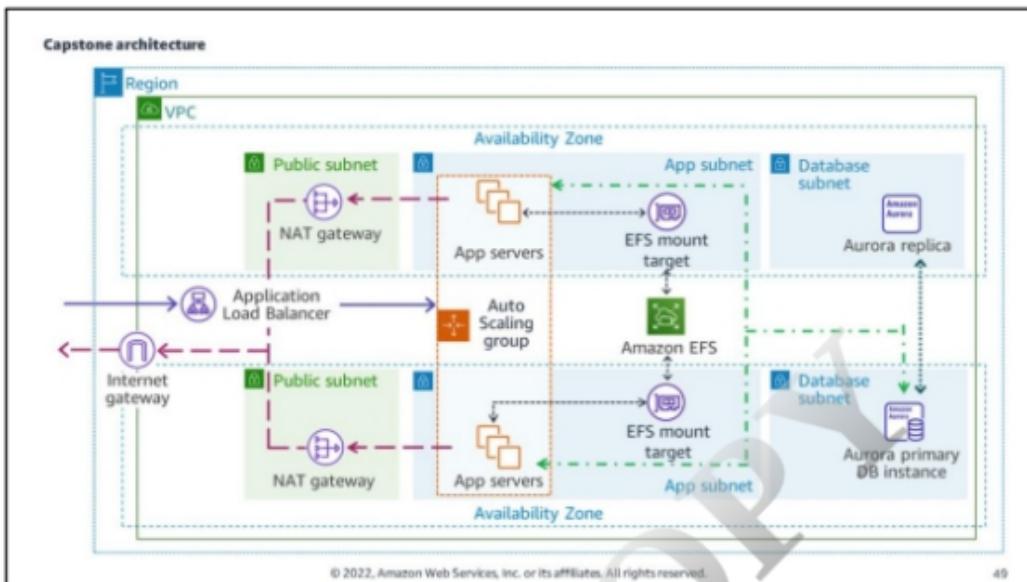
Next, you will review:

 Capstone check-in

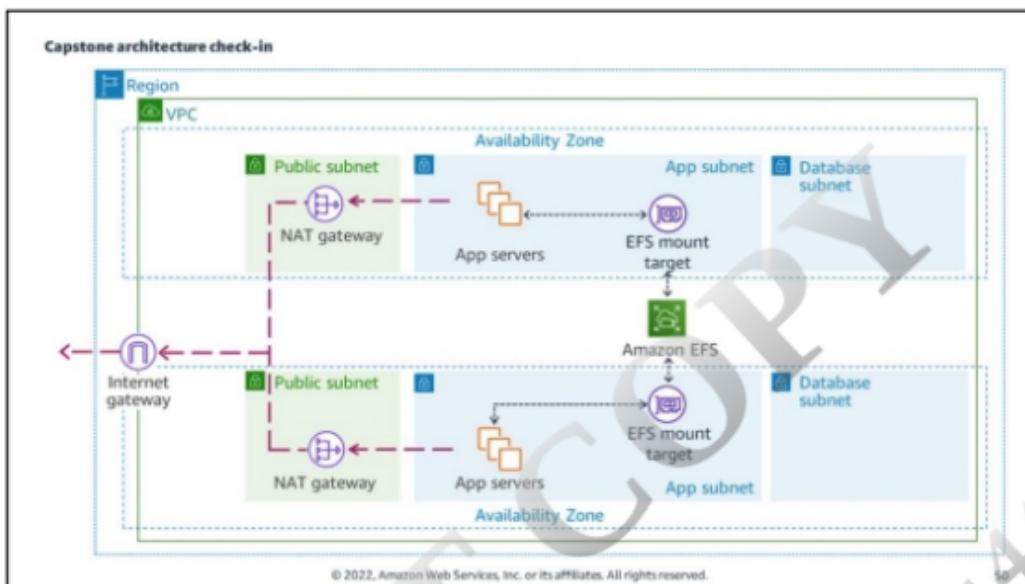
 Knowledge Check

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

48



At the end of this course is a Capstone Lab project. You will be provided a scenario and asked to build an architecture based on project data, best practices, and the Well-Architected Framework.



In this module, you explored multiple storage solutions. You are now able to build the following for the capstone project:

- A shared file storage system for your WordPress application using Amazon EFS Standard

This solution automatically creates one EFS mount target for you in each Availability Zone. The WordPress installation directory is placed on the EFS mount so that it can be read by multiple EC2 instances. In the event one instance fails and is replaced, the files already exist in an accessible and redundant file share.

The WordPress website also requires you to build a database to use for the three-tier architecture. You should think about what options there are in AWS for database services. You will explore this topic in the next module.

\*\*For accessibility: Partial selection of capstone architecture with one VPC in one Region. Two Availability Zones are shown. Each has a public subnet, app subnet, and database subnet. An internet gateway is placed at the edge of the VPC. Each Availability Zone has a NAT gateway in a public subnet. App servers and an EFS mount target are placed in each app subnet. An Amazon EFS file system is placed in the VPC but is connected to EFS mount targets in each app subnet. App servers communicate with the EFS mount targets in their own subnets to reach the EFS file system. App servers send requests to the public internet through a NAT gateway in their Availability Zone. End description.



DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

### Knowledge check question 1



Which of the following Amazon S3 features would you use to automatically copy new objects to a bucket in a different AWS Region?

- A Same-Region Replication (SRR)
- B Amazon S3 Versioning
- C AWS DataSync
- D Cross-Region Replication (CRR)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

52

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Knowledge check question 1 and answer**

Which of the following Amazon S3 features would you use to automatically copy new objects to a bucket in a different AWS Region?

A	Same-Region Replication (SRR)
B	Amazon S3 Versioning
C	AWS DataSync
D correct	Cross-Region Replication (CRR)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3

The answer is D, Cross-Region Replication.

S3 Cross-Region Replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. CRR can help you do the following:

- **Meet compliance requirements** – Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. To satisfy these requirements, use Cross-Region Replication to replicate data between distant AWS Regions.
- **Minimize latency** – If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
- **Increase operational efficiency** – If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions.

## Knowledge check question 2



Which Amazon S3 feature can force an action to occur after an event takes place within a bucket?

- A Invoking
- B Event notification
- C Lambda
- D Alarm

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

54

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Knowledge check question 2 and answer**

Which Amazon S3 feature can force an action to occur after an event takes place within a bucket?

A	Invoking
B correct	Event notification
C	Lambda
D	Alarm

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

55

The answer is B, event notification.

With Amazon S3 event notifications, you can receive notifications when certain object events happen in your bucket. These notifications can invoke actions in other AWS services like AWS Lambda.

For more information about Amazon S3 event notifications, see “Reliable event processing with Amazon S3 event notifications” in the [AWS Storage Blog](https://aws.amazon.com/blogs/storage/reliable-event-processing-with-amazon-s3-event-notifications/) (<https://aws.amazon.com/blogs/storage/reliable-event-processing-with-amazon-s3-event-notifications/>).

### Knowledge check question 3



You have two Linux applications in different Availability Zones that must share a common file system. Which of the following is the best solution for this use case?

- A Storage Gateway
- B FSx for Windows File Server
- C Amazon S3
- D Amazon EFS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

56

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Knowledge check question 3 and answer**

You have two Linux applications in different Availability Zones that must share a common file system. Which of the following is the best solution for this use case?

A	Storage Gateway
B	FSx for Windows File Server
C	Amazon S3
D correct	Amazon EFS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The answer is C, Amazon EFS.

While there are other file sharing systems to choose from like FSx for Lustre or FSx for OpenZFS, neither of these solutions are presented as possible answers. Amazon EFS presents a scalable file system that can be mounted with the NFS protocol by multiple Linux EC2 instances.

AWS Storage Gateway supports hybrid environments, which is not mentioned here. FSx for Windows File Server would allow a Linux application to mount the file system via SMB, but it is not the easiest solution to implement. Amazon S3 is an object storage solution and it does not natively present you with a mountable file system.

### Knowledge check question 4



Which of the following are modes available in the Storage Gateway appliance? (Select THREE.)

- A Memory Gateway
- B Tape Gateway
- C Volume Gateway
- D Amazon EBS File Gateway
- E Amazon S3 File Gateway
- F Amazon S3 Glacier File Gateway

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu

**Knowledge check question 4 and answer**

Which of the following are modes available in the Storage Gateway appliance? (Select THREE.)

A	Memory Gateway
B correct	Tape Gateway
C correct	Volume Gateway
D	Amazon EBS File Gateway
E correct	Amazon S3 File Gateway
F	Amazon S3 Glacier File Gateway

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. 59

The correct answer is B, C, and E: Tape Gateway, Volume Gateway and File Gateway.

There is also a fourth mode available for Amazon FSx File Gateway.



## End of Module 5

Corrections, feedback, or other questions?

Contact us at <https://support.aws.amazon.com/#/contacts/aws-training>.

All trademarks are the property of their owners.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

60

DO NOT COPY  
2d35e8483186bd2@placeholder.44518.edu