

## S3 Storage

# S3 Storage: The Complete Guide

**Read Next:**[S3 Storage: The Complete Guide](#)[S3 Pricing Made Simple: The Complete Guide](#)[Comparing AWS Storage SLAs: Which Protects You Best](#)[Amazon S3 Encryption: How to Protect Your Data in S3](#)December 15, 2021 | Topics: [Cloud Volumes](#) [ONTAP](#), [AWS](#), [Elementary](#)

## What is Amazon S3 Storage?

Amazon Simple Storage Service (Amazon S3) offers scalable and secure object storage. Amazon S3 can support a variety of use cases, including data lakes, mobile applications, websites, backup and restore, enterprise applications, archives, big data analytics, and Internet of Things (IoT) devices. The service enables customers to configure, optimize, and organize access to data to meet business and compliance requirements.

This is part of an extensive series of guides about [cloud storage](#).

In this article:

- [Amazon S3 Use Cases](#)
  - [Backup and Disaster Recovery](#)
  - [Analytics](#)
  - [Data Archiving](#)
  - [Security and Compliance](#)
- [How Does Amazon S3 Work?](#)
  - [Amazon S3 Objects](#)
  - [Amazon S3 Buckets](#)
  - [Amazon S3 Console](#)
- [AWS S3 Storage Classes](#)
- [S3 Tutorial: Getting Started with Amazon S3](#)
  - [Create S3 Bucket](#)
  - [Upload an Object to the Bucket](#)
- [AWS S3 Security](#)
  - [Amazon S3 Data Protection](#)
  - [Amazon S3 Data Encryption](#)

- [AWS PrivateLink for Amazon S3](#)
- [Identity and Access Management in Amazon S3](#)
- [Amazon S3 Performance Guidelines](#)
  - [Measure Performance](#)
  - [Scale Storage Connections Horizontally](#)
  - [Use Amazon S3 Transfer Acceleration](#)
  - [Retry Requests for Latency-Sensitive Applications](#)
- [AWS Storage Optimization with Cloud Volumes ONTAP](#)

## Amazon S3 Use Cases

### Backup and Disaster Recovery

Amazon S3 can automatically replicate data across regions while maintaining maximum durability and availability. This capability makes Amazon S3 ideal for archiving and storing highly critical backups and data.

Amazon S3 versioning can store multiple versions of each of your files, to make it easier to recover these files or older versions. This feature offers S3 customers a greater level of protection.

### Analytics

Amazon S3 offers in-place querying functionality, which you can use to run powerful analytics on data stored in S3. This feature supports most third-party service integrations and does not require moving data elsewhere.

### Data Archiving

Amazon S3 offers several storage class tiers, including Amazon S3 Glacier, a durable and cost-effective archiving solution. You can move terabytes of data from standard S3 storage and store it for compliance purposes in Glacier. To save time, you can use a lifecycle policy to automate the process. You specify when you want the system to archive data and the policy performs the action.

### Security and Compliance

Amazon S3 offers several compliance and encryption features that can help meet requirements set by the PCI-DSS, FedRAMP, FISMA, HIPAA/HITECH, the Data Protection Directive, and other standards. In addition to satisfying security and compliance requirements, these features can also help you limit access to critical data, for example by using bucket policies.

## How Does Amazon S3 Work?

Amazon S3 lets you store data files as objects, which you can organize in S3 buckets. You can manage objects and buckets through the Amazon S3 console.

### Amazon S3 Objects

An Amazon S3 object consists of a data file and its associated metadata. You can store any file type as an object, including images, documents, and videos. Amazon S3 limits the maximum object file size to 160 GB per upload. However, AWS provides several tools to help you add larger files.

Objects are the fundamental entity you can store in S3. Each object has a unique key used to uniquely identify it within the designated S3 environment.

### Amazon S3 Buckets

---

S3 objects are organized by storing them in buckets, which serves as storage containers. You can use the Amazon S3 API to upload multiple objects to one bucket.

AWS lets you create a maximum of 100 buckets for each AWS cloud account. You can submit a service limit increase to request additional buckets. AWS does not limit the number of objects you can store within each bucket.

Here are several aspects to consider when creating buckets:

- **Choose a suitable AWS region—unless** you transfer your objects, they remain in a bucket placed within a certain region. However, AWS lets you choose a region when you create a new bucket. You can minimize costs and address latency concerns by choosing the closest region.
- **Amazon S3 buckets are globally unique**—other AWS accounts within the same AWS region cannot use the same bucket names. These names can become available only if you delete these buckets.

*Related content: [Read our guide to S3 configuration](#)*

## Amazon S3 Console

AWS lets you manage buckets and objects through the Amazon S3 Console. You can access it from the AWS Management Console. The S3 console offers a browser-based graphical user interface.

The S3 console lets you configure, create, and manage your buckets, as well as download, upload, and manage your storage objects. The console enables you to employ a logical hierarchy to organize your storage.

The logical hierarchy uses keyword prefixes and delimiters to form a folder structure within the console. This structure can help you easily locate files, by using a combination of features (bucket name, keys, web service endpoint, and a version when needed) to address each S3 object uniquely.

*Related content: [Read our AWS S3 cheat sheet](#)*

## AWS S3 Storage Classes

Amazon S3 offers seven storage classes, including:

- **S3 Standard**—supports frequently-accessed data that require low latency and high throughput. This tier is ideal for content distribution, dynamic websites, big data workloads, and applications.
- **S3 Intelligent-Tiering**—supports data with either unknown or changing access needs. This tier provides four types of access, including Frequent Access, Archive, Infrequent Access (IA), and Deep Archive. The tier analyzes customer access patterns and then automatically moves data to the least expensive tier.
- **S3 Standard-IA**—supports infrequently-access data that require quick access. This tier offers lower storage prices, ideal for long-term storage, backup, and data recovery (DR) scenarios.
- **S3 One Zone-IA**—supports infrequently-access data that requires rapid access when needed. This tier does not offer high resilience and availability, which is why it is only suitable for data you can easily recreate, or is already saved in other locations.
- **S3 Glacier**—supports primarily archival storage scenarios. This tier offers cost-effective storage for data that can suffer long retrieval times. It offers variable retrieval rates ranging between minutes and hours.
- **S3 Glacier Deep Archive**—supports data that requires access only once or twice per year. This tier offers the lowest storage S3 prices.
- **S3 Outposts**—adds APIs and S3 object storage features to an on-site AWS Outposts environment. You can use S3 Outposts when your performance requirements call for data to be retained near on-site applications or to meet specific data residency stipulations.

AWS offers the use of lifecycle management policies. You can use this feature to curate data and shift it to a more suitable tier.

# S3 Tutorial: Getting Started with Amazon S3

AWS lets you store objects in buckets. Here is a quick tutorial that can guide you through the process of creating a bucket and then uploading an object into this bucket:

## Create S3 Bucket

Prerequisites: An active AWS account.

To create a bucket:

1. Sign into your account and access the AWS Management Console, where you can locate the Amazon S3 console. For quick access, you can use this URL: <https://console.aws.amazon.com/s3/>.

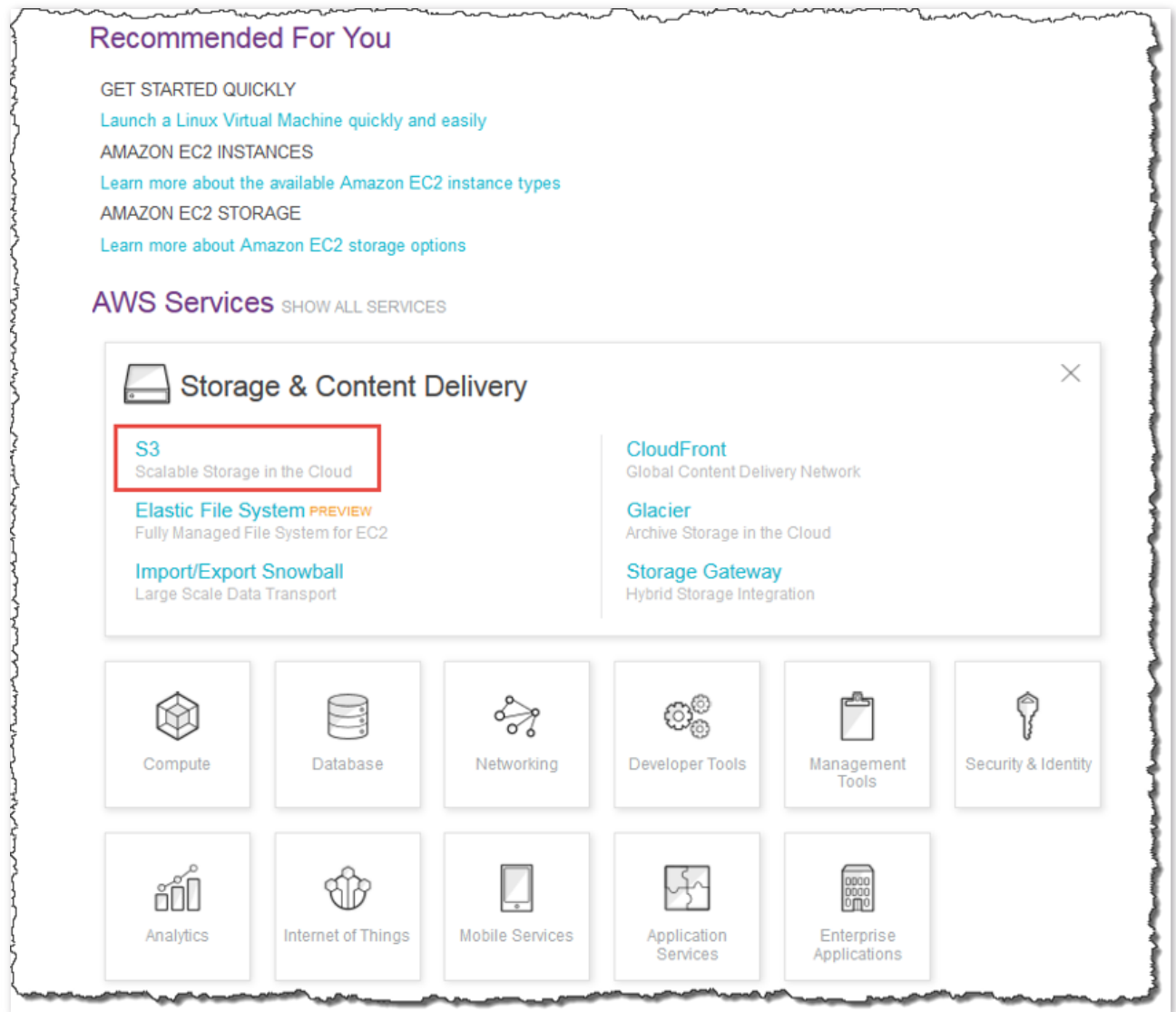
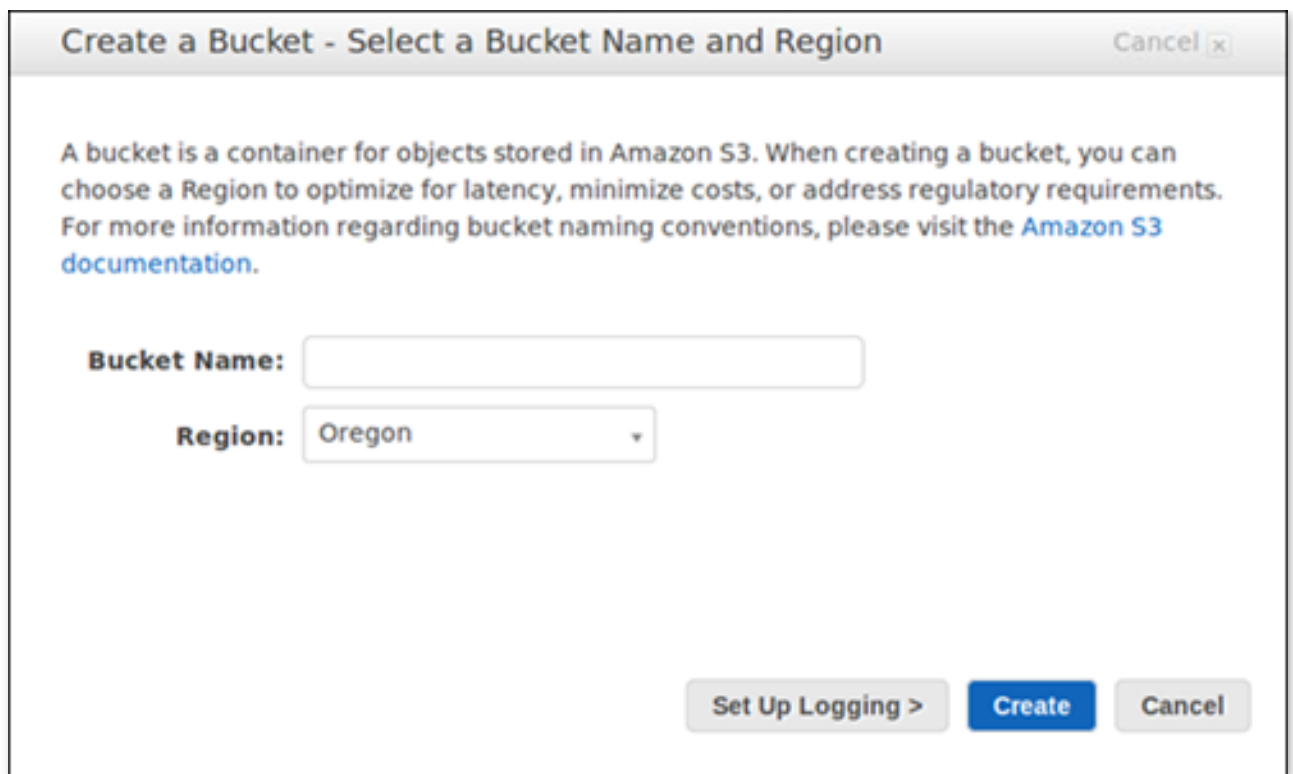


Image Source: AWS

2. Select the **Create bucket** option.
3. Go to **Bucket name**, and enter a DNS-compliant name for the new bucket.



**Create a Bucket - Select a Bucket Name and Region** Cancel

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the [Amazon S3 documentation](#).

**Bucket Name:**

**Region:** Oregon

Set Up Logging > Create Cancel

Image Source: AWS

4. Go to **Region**, and select an AWS Region for your bucket. It would be best to choose the most geographically close region to address regulatory requirements and minimize latency and costs.
5. Select the **Create bucket** option.

## Upload an Object to the Bucket

Once you create a bucket, you can start uploading objects.

### To upload an object to a bucket:

1. Go to the Amazon S3 console, using this URL: <https://console.aws.amazon.com/s3/>.
2. Go to the **Buckets** list, and select the name of the target bucket.
3. Go to the **Objects** tab of the target bucket, and select the **Upload** option.

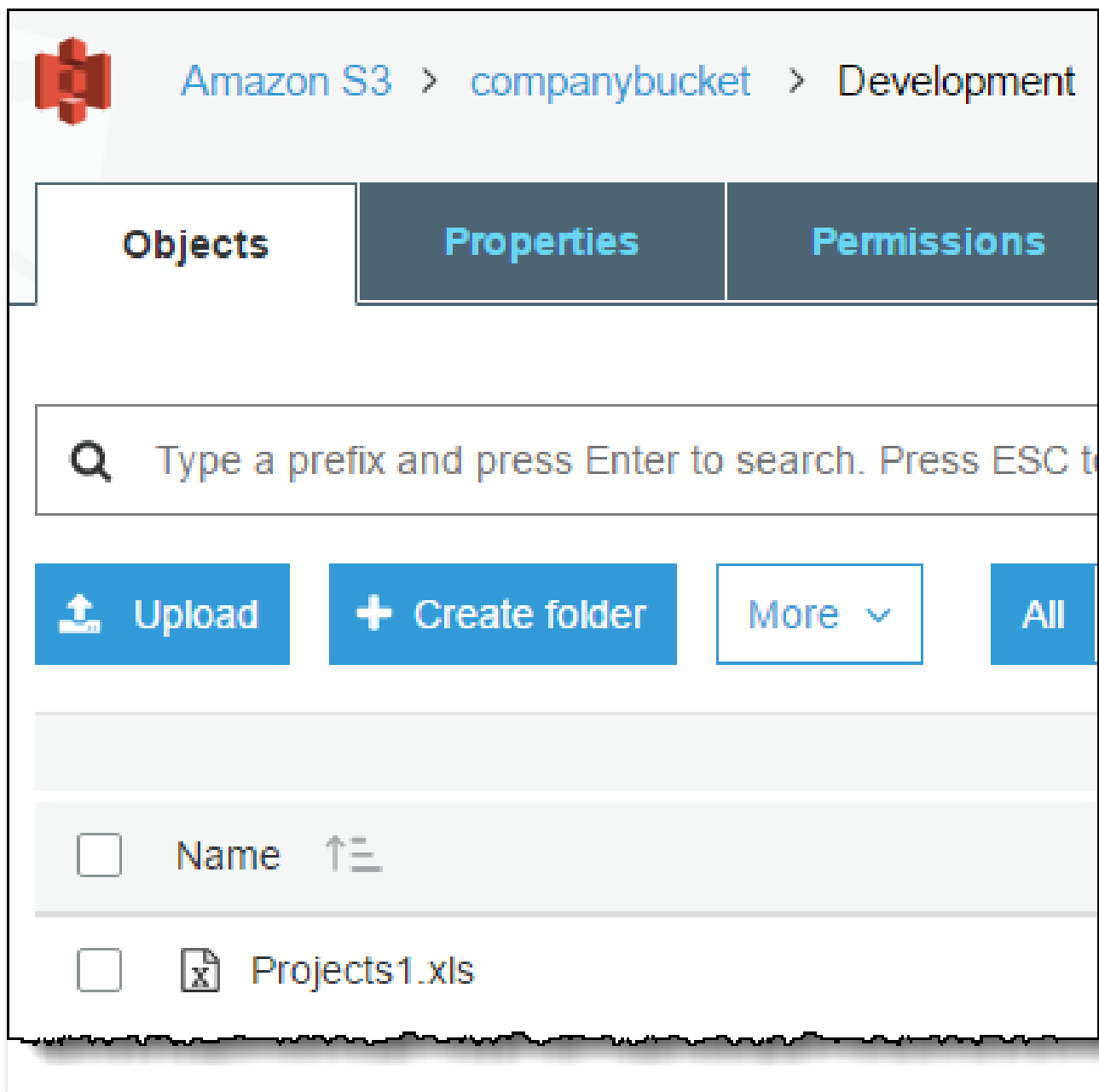


Image Source: [AWS](#)

4. Go to **Files and folders**, and select the **Add files** option.
5. Select the file you want to upload, and then select the **Open** option.
6. Select the **Upload** option.

## AWS S3 Security

### Amazon S3 Data Protection

Amazon S3 offers a very sturdy storage infrastructure created for primary and mission-critical data storage. S3 lets you store objects redundantly on multiple devices over multiple facilities within an Amazon Region.

To help maintain data durability, Amazon S3 PUT and put object -copy operations synchronously retain your information over multiple availability zones. After Amazon S3 has stored the objects, it retains their durability by readily identifying and repairing any lost redundancy.

Here are the data protection features offered by Amazon S3 standard storage:

- Provides 99.99% availability and 99.99999999% durability of objects during any year

- Able to sustain simultaneous loss of data in two facilities
- Backed by the Amazon S3 Service Level Agreement

Amazon S3 also safeguards your data via versioning. You can employ versioning to retrieve, restore and preserve all versions of all objects that you store in your Amazon S3 bucket. Using versioning, you can swiftly recover from both application failures and unintentional user actions. Requests default back to the most recently written version. You can also retrieve older versions of an object by detailing the object's version via a request.

## Amazon S3 Data Encryption

Data protection covers data at rest (when Amazon S3 data centers store the information on disks) and while in transit (as the data travels from and to Amazon S3). You can safeguard data in transit through client-side encryption or Secure Socket Layer/Transport Layer Security.

You have these choices for safeguarding data at rest in Amazon S3:

- **Server-side encryption**—you can request Amazon S3 to encrypt your object before retaining it on disk in its information centers and then decrypt it once you download the objects.
- **Client-side encryption**—you can encrypt data client-side and then upload the information to Amazon S3. Here you control the encryption keys, the encryption process, and related tools.

*Related content: [Read our guide to S3 encryption](#)*

## AWS PrivateLink for Amazon S3

Using AWS PrivateLink for Amazon S3, you may provision interface VPC endpoints within your virtual private cloud. You can access these endpoints directly from on-site applications over VPN and AWS Direct Connect or via another AWS Region through VPC peering.

## Identity and Access Management in Amazon S3

By default, every Amazon S3 resource—objects, buckets, and subresources (such as website configuration and lifecycle configuration)—remain private. The resource owner (or the AWS account that created the resource) alone may access the resource. The resource owner may choose to provide access permissions to someone else by drafting an access policy.

Amazon S3 provides access policy options, categorized as user policies and resource-based policies. Access policies that you connect to your resources (objects and buckets) are called resource-based policies.

*Related content: [Read our guide to S3 bucket security](#)*

## Amazon S3 Performance Guidelines

When developing applications that retrieve and upload objects from Amazon S3, use the following guidelines to improve performance:

### Measure Performance

When accessing S3 from EC2 instances, pay attention to CPU, network throughput, and DRAM requirements. Depending on the demand for these resources, it could be worth assessing other Amazon EC2 instance types.

When assessing performance, it's also useful to examine DNS latency, lookup time, and information transfer speed via HTTP analysis tools.

### Scale Storage Connections Horizontally

Spreading requests over several connections is a typical design approach to horizontally scale performance. When developing high-performance applications, approach Amazon S3 like an extremely large distributed system rather than as a single network endpoint (as in a conventional storage server). You can attain optimal performance by issuing several simultaneous requests to Amazon S3.

You can spread such requests via separate connections to optimize the accessible bandwidth from Amazon S3. Amazon S3 doesn't cap the number of connections to a specific S3 bucket.

## Use Amazon S3 Transfer Acceleration

S3 Transfer Acceleration facilitates secure, fast transfers of files over vast geographical distances between an S3 bucket and the client. Transfer Acceleration makes use of Amazon CloudFront's worldwide distributed edge locations.

When utilizing Transfer Acceleration, you transfer information to Amazon S3 via an optimized network route as the information reaches an edge location. Transfer Acceleration is suitable for moving gigabytes to terabytes of information over continents. It is also helpful for clients that upload to a centralized bucket from all parts of the globe.

You could employ the Amazon S3 Transfer Acceleration Speed Comparison tool to contrast non-accelerated and accelerated upload speeds over Amazon S3 Regions. This tool utilizes multipart uploads to test file transfer speeds from the browser to multiple Amazon S3 Regions.

## Retry Requests regarding Latency-Sensitive Applications

Aggressive retries and timeouts help promote consistent latency. Because of the considerable scale of Amazon S3, if the initial request is slow, a retried request will probably adopt another path and succeed. The AWS SDKs possess configurable retry and timeout values. You can tune these values to the tolerance of your particular application.

*Related content: [Read our guide to S3 performance](#)*

## AWS Storage Optimization with Cloud Volumes ONTAP

NetApp [Cloud Volumes ONTAP](#), the leading enterprise-grade storage management solution, delivers secure, proven storage management services on AWS, Azure and Google Cloud. Cloud Volumes ONTAP capacity can scale into the petabytes, and it supports various use cases such as file services, databases, DevOps or any other enterprise workload, with a strong set of features including high availability, data protection, storage efficiencies, Kubernetes integration, and more.

In particular, Cloud Volumes ONTAP provides [storage efficiency features](#), including thin provisioning, data compression, and deduplication, reducing the storage footprint and costs by up to 70%.

Learn more about how Cloud Volumes ONTAP helps cost savings with these [Cloud Volumes ONTAP Storage Efficiency Case Studies](#).

Download our free guide: [The 5 Phases for Enterprise Migration to AWS](#).



## Learn More About S3 Storage

### AWS Certification Cheat Sheet for Amazon S3

There are a lot of benefits to getting your AWS certification. The first step is knowing your AWS services inside and out. In this post we'll give you an easy-to-remember cheat sheet for all of the things you'll be expected to know about Amazon S3 when you take your AWS certification exam, from use of the AWS S3 CLI to access configurations.

Read more in our [Amazon S3 Cheat Sheet](#).



## How to Secure AWS S3 Configurations

The cloud providers can protect their services, but it's up to users to ensure their data is secure when stored in the cloud. This is especially relevant when it comes to objects stored in AWS S3.

This blog post looks at some of the actions that users can take to secure AWS S3, from restricting bucket access, leveraging key management services, and adding Cloud Volumes ONTAP security capabilities.

Read more in [How to Secure Amazon S3 Configurations](#).

## Comparing AWS SLAs: EBS vs S3 vs Glacier vs All the Rest

What kind of SLAs do the different cloud storage options on AWS each provide? Is that going to affect which one will be the right storage choice for your data?

This blog post compares the block (AWS EBS), object (AWS S3), deep archive (Glacier), and other storage options offered by AWS so you can pinpoint the platform with the ideal availability and durability for your data based on its relevance to your operations.

Read more in [Comparing AWS SLAs: EBS vs S3 vs Glacier vs All the Rest](#)

## How to Secure S3 Objects with Amazon S3 Encryption

Keeping data stored on Amazon S3 is critical, which is why AWS has some powerful encryption tools for use with the popular object storage service. This post looks at these S3 encryption methods to help you find the option that will be best to protect your data.

Read more in [How to Secure S3 Objects with Amazon S3 Encryption](#)

## How to Test and Monitor AWS S3 Performance

New adopters of AWS might not be aware of all the ins and outs of the platform in order to optimize their deployments, but there are some key tips and tricks that can be used to monitor and optimize AWS S3 performance.

This post will look at a number of design principles and architectural best practices to help optimize Amazon S3 usage.

Read more in [How to Test and Monitor AWS S3 Performance](#).

## Amazon S3 Bucket Security: How to Find Open Buckets and Keep Them Safe

Open Amazon S3 buckets can expose your data—and your organization—to considerable risk. Anyone on the internet is able to access open buckets, making it critical to identify them and close them up. This post will show the steps to take to find those buckets and prevent such leaks from ever taking place.

Read more in [Amazon S3 Buckets: Security Risks with Open Buckets and How to Find Them](#).

## How to Copy AWS S3 Objects to Another AWS Account

In many large organizations, there may be more than one AWS account in use. While it's easy to move objects between buckets owned by the same account, what happens when data has to be moved between different S3 buckets between those accounts?

In this post we will demonstrate how to copy objects from a bucket in one AWS account to an S3 bucket in another AWS account.

Read more in [How to Copy AWS S3 Objects to Another AWS Account](#).

## S3 Pricing Made Simple: The Complete Guide

Amazon Simple Storage Service (Amazon S3) is an object storage solution that features data availability, scalability, performance, and security. Understand S3 pricing components with pricing examples, including cost per GB-month, data operations and data

retrieval. Get 3 tips for reducing your S3 costs.

Read more in [S3 Pricing Made Simple: The Complete Guide](#).

## **S3 Access: How to Store Objects With Different Permissions In the Same Amazon S3 Bucket**

Accessing S3 objects can be a hurdle for users who don't own the bucket where the object is stored. Buckets are private by default for a good reason—it's always important to make sure data is secure. But to make it easier within organizations to share data, it is possible to adjust permissions for individual objects to allow other users to access them.

This article will show you how to set different access options for your Amazon S3 objects that are all stored in a single bucket.

Read more in [S3 Access: How to Store Objects With Different Permissions In the Same Amazon S3 Bucket](#).

## **Amazon S3 Storage Lens: A Single Pane of Glass for S3 Storage Analytics**

In enterprise deployments, Amazon S3 usage can be highly complex. When there are multiple IT teams distributed across multiple AWS regions utilizing S3 for their own needs, it can be difficult to understand how the service is being used. To help such organizations keep track of their S3 usage, AWS has introduced Amazon S3 Storage Lens.

This single-pane-of-glass console provides free and paid service dashboards that users can leverage to gain visibility into their entire S3 storage usage throughout the organization. This can help to optimize usage and improve costs.

Read more: [Amazon S3 Storage Lens: A Single Pane of Glass for S3 Storage Analytics](#)

## **See Additional Guides on Key Cloud Storage Topics**

Together with our content partners, we have authored in-depth guides on several other topics that can also be useful as you explore the world of [cloud storage](#).

## **File Upload**

*Authored by Cloudinary*

- [Angular File Upload to Cloudinary in Two Simple Steps](#)
- [Uploading PHP Files and Rich Media the Easy Way](#)
- [AJAX File Upload - Quick Tutorial & Time Saving Tips](#)

## **Google Cloud Storage**

*Authored by NetApp*

- [Google Cloud Persistent Disk: How to Resize and Use](#)
- [Google Storage Service How-To: Switch Google Cloud Storage Class](#)
- [Google Cloud Filestore: NFS Cloud File Storage on Google Cloud](#)

## **AWS snapshots**

*Authored by NetApp*

- [AWS Snapshots: Ultimate Intro to Amazon EBS Snapshots](#)
- [Crash-Consistent Backups for Applications in the AWS Cloud](#)



Yifat Perry  
Product Evangelist