S3

**S3 Use cases**

* Backup and storage
* Disaster Recovery
* Archive
* Hybrid Cloud storage
* Application hosting
* Media hosting
* Data lakes & big data analytics
* Software delivery
* Static website

**Amazon S3 Overview - Buckets**

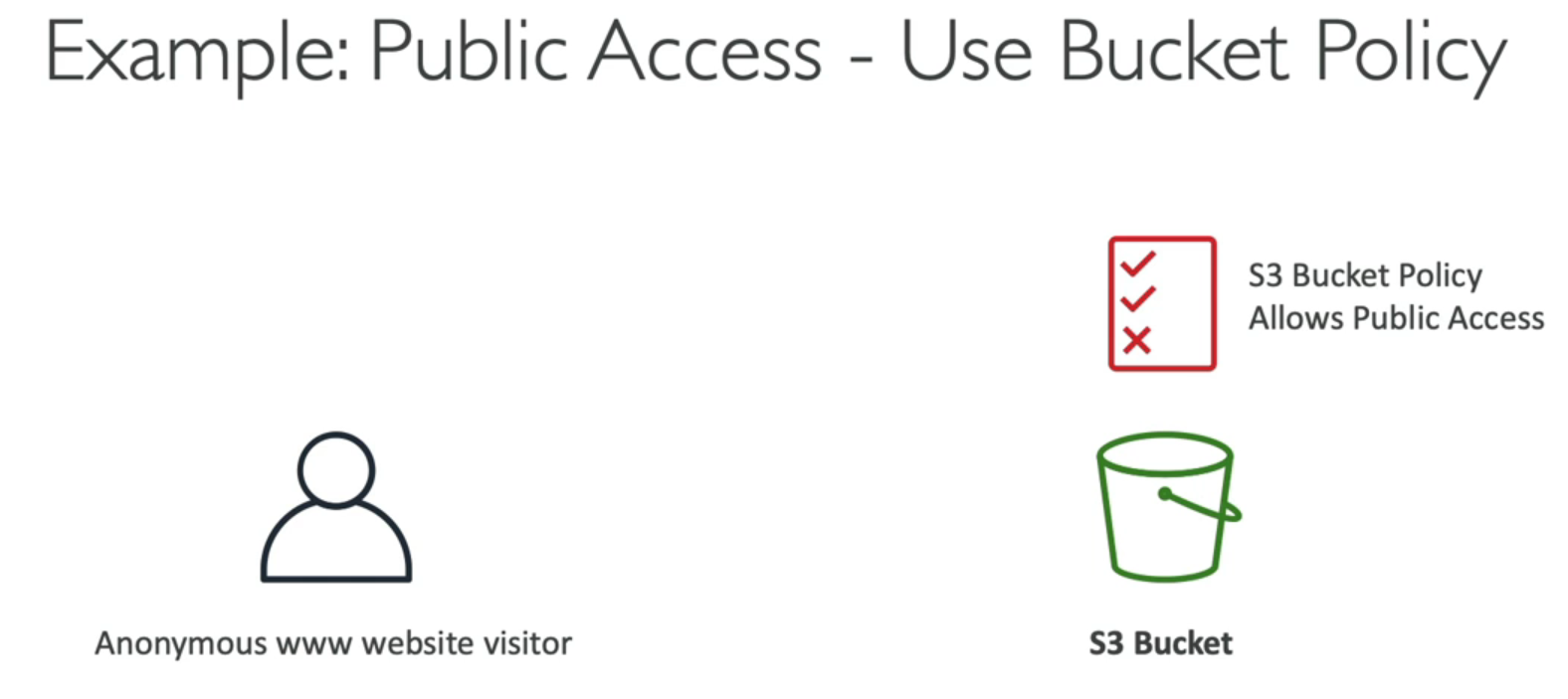
* Amazon S3 allows people to store objects (files) in “buckets” (directories)
* Buckets must have a globally unique name (across all regions all accounts)
* Buckets are defined at the region level
* S3 looks like a global service but buckets are created in a region
* Naming convention
  + No uppercase
  + No underscore
  + 3-63 characters long
  + Not an IP
  + Must start with lowercase letter or number

**S3 Security**

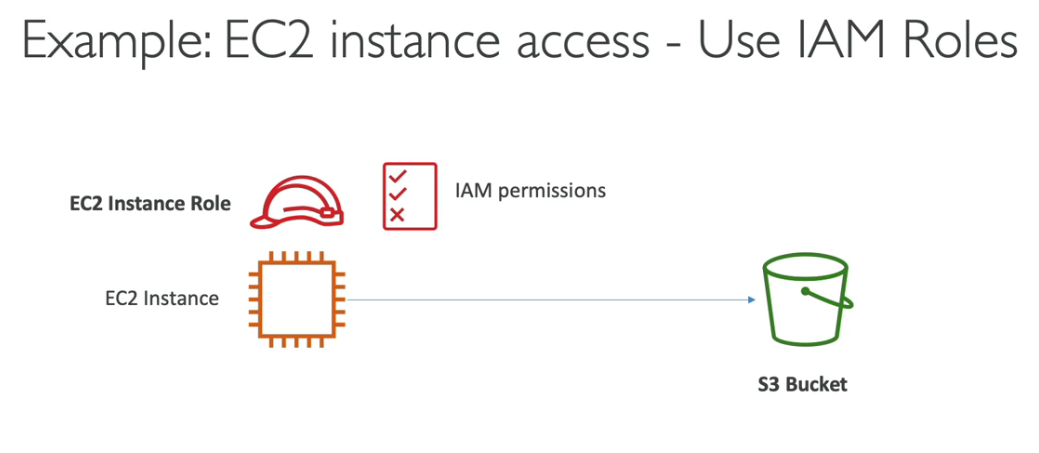
* **User based**
  + IAM policies - which API calls should be allowed for a specific user from IAM console
* **Resource Based**
  + Bucket Policies - bucket wide rules from the S3 console - allows cross account
  + Object Access Control List (ACL) – finer grain
  + Bucket Access Control List (ACL) – less common
* **Note:** an IAM principal can access an S3 object if
  + the user IAM permissions allow it OR the resource policy ALLOWS it
  + AND there’s no explicit DENY
* **Encryption:** encrypt objects in Amazon S3 using encryption key

**S3 Bucket Policies**

* JSON based policies
  + Resources: buckets and objects
  + Actions: Set of API to Allow or Deny
  + Effect: Allow / Deny Principal: The account or user to apply the policy to
* Use S3 bucket for policy to:
  + Grant public access to the bucket
  + Force objects to be encrypted at upload
  + Grant access to another account (Cross Account)







**Bucket settings for Block Public Access**

* Block Public Access is a set of controls offered by Amazon S3 to restrict public access to your S3 buckets and the objects stored within them. These settings were created to prevent company data leaks

 **Blocks ALL public access:** No one from the internet can access your S3 buckets or objects, ever.

 **Blocks public ACLs (new & old):** Prevents public access accidentally granted through access control lists.

 **Blocks public bucket/access point policies (new & old):** Stops public access set through bucket rules, even for existing policies.

*  **Blocks public & cross-account access:** Extends protection to prevent access from other AWS accounts even if granted public access through policies.If you know your bucket should never be public, leave these on
* Can be set at the account level

**S3 Websites**

* S3 can host static websites and have them accessible on the www
* The website URL will be:
* bucket-name.s3-website-AWS-region.amazonaws.com OR
* bucket-name.s3-website.AWS-region.amazonaws.com
* **If you get a 403 (Forbidden) error, make sure the bucket policy allows public reads**

**S3 Versioning** in Amazon S3 is a feature that lets you keep track of different versions of the same file (object) stored in your S3 bucket. Here's the gist:

* Same key overwrite will increment the “version”: 1, 2, 3….
* **Without Versioning:** By default, S3 overwrites the old file with a new upload, so you lose the previous version.
* **With Versioning:** Uploads create new versions, keeping the old ones intact. Each version has a unique ID for easy access.

**Benefits:**

* **Undo mistakes:** Accidentally overwrite a file? No worries, restore a previous version.
* **Track changes:** See how a file evolved over time.
* **Compliance:** Maintain historical data for regulatory purposes.

## S3 Replication (CRR & SRR)

S3 Replication in AWS lets you automatically copy objects from one S3 bucket (source) to another (destination), in the same or different regions.

 **Same-Region Replication (SRR):** Copies data within the same AWS region. Ideal for backups and redundancy within a region.

 **Cross-Region Replication (CRR):** Copies data to a bucket in a different AWS region. Useful for disaster recovery and geographically dispersed access

