Reflection:

Bucket and IAM policies can manage permissions, but they differ in some aspects.

Bucket policies are attached directly to an S3 bucket. They can define who can access the bucket and which actions can be performed. It is useful when managing access to a certain bucket.

IAM policies are attached to the IAM users or groups. They define what the specific IAM user or role is allowed to do, and which buckets they can grant access to.

Importantly, S3 access is only granted when both bucket and IAM policies allow the actions, which means that if either action denies the access, S3 permissions cannot be granted. When managing the S3 resources, we use bucket policies to manage bucket access. In contrast, we use IAM policies to control global permissions and grant users extra policies when necessary.

In conclusion, to manage S3 resources, we should combine both bucket and IAM policies.