S3 Permissions

As with HDFS, managing permissions is vital with S3—even more so, because as a cloud service, S3 can in many cases be more easily accessed by hackers and other bad actors. There are many stories about S3 buckets being made public and having unwanted consequences:

- [There's a Hole in 1,951 Amazon S3 Buckets](#)
- [Verizon](#) and [Viacom](#)
- [Don't panic, Chicago, but an AWS S3 config blunder exposed 1.8 million voter records](#)
- [Leaky S3 bucket sloshes deets of thousands with US security clearance](#)

If you use S3, be sure you understand the permissions issues and what is allowed. AWS provides a guide on [Setting Bucket and Object Access Permissions](#).