# How to never have a public S3 bucket

Teri Radichel Follow
Jun 21 · 5 min read ★

I was creating a simple website for my nephew's painting business in Tigard, Oregon in an S3 bucket, and also handled a consulting call on this topic today, so I thought I'd write a quick blog post about it. Do you ever need a public S3 bucket? In a large company, I would say no.

If you aren't aware, you can host a website in an S3 bucket. It's really simple and by doing so you don't have to set up a server. It works well for static websites that don't need a back end web server or pushing out static files from a dynamic website. You can set up a domain name and point it at the bucket. In this case, I set up http://rodmyre-house-painters.com to display files from a bucket with the same name. With just a couple of configuration changes the website is up and running. At this moment, I'm waiting for the

DNS to propagate so by the time you read this, the website might not yet be available. By the way, when I said simple website I wasn't kidding. I just got it online and told my nephew he can learn HTML if he wants to change it and I would help him out. Motivation!

## Tigard College Pro House Painters

Looking for a professional house painter in Tigard, Beaverton, or Tualatin? You've found us! We are professionally trained house painters working through College Pro. Our services are top-notch. We work hard and deliver excellent service at a reaonsable price.

Not only will you get the best painting services around, you'll be helping Lucas Rodmyre and his hardworking employees get through college. College Pro has transformed over 2,000,000 houses since 1971 and developed over 15,000 entrepreneurs.

More about College Pro

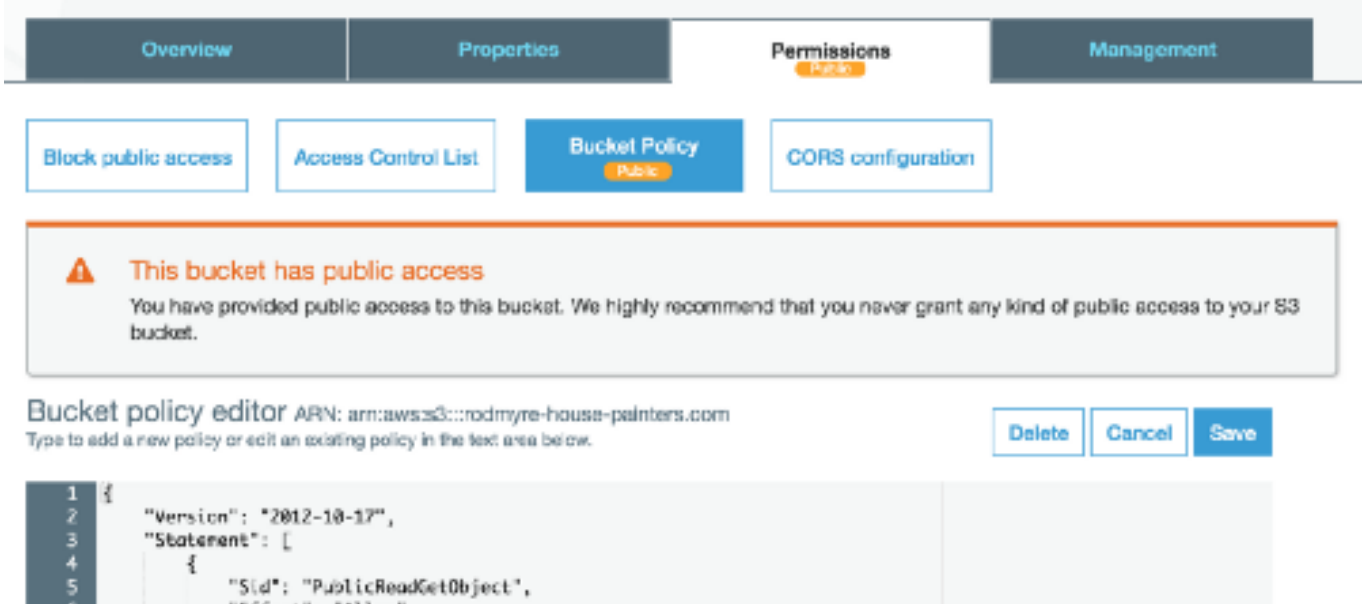
See our work and like us on Facebook at: Tigard College Pro Painters

For a free estimate, send us a message on Facebook or give us a call:

**206-430-0196**

Serving customers needing **house painting services in Tigard, Beaverton, and Tualatin.**

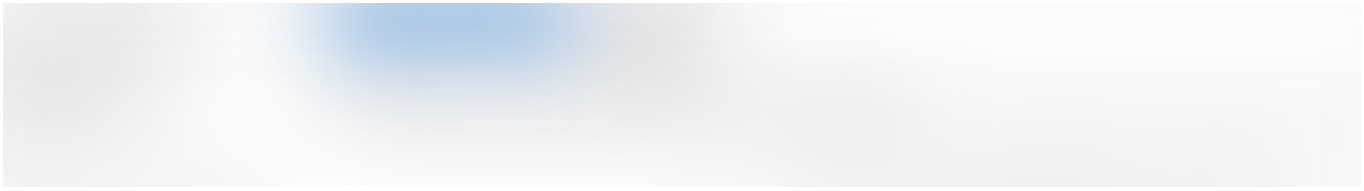
For this site, I did use a public bucket. First of all, my nephew is in college and painting houses over the summer through a company called College Pro. I'm not sure if he's going to continue doing it after this summer. He doesn't need CloudFront to distribute the content closer to web site visitors or the expense. After all, the bucket is in us-west-2 (Oregon) where his customers exist, so I figure the latency will be fine. He's not targeting people outside that area. There will only be a couple of people accessing the account and access to edit the bucket configuration is limited. So in this very simple case, perhaps a public S3 bucket to host his web site is fine, but only for reading files, of course.



```
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::rodmyre-house-pointers.com/*"
        }
    ]
}
```

As you can see in the image, AWS is giving me a big warning that this bucket is accessible from the Internet by telling me that I should never grant public access to my S3 bucket. Consider a larger organization where you need some governance to maintain your desired level of risk. In this case, I would say you never need a public S3 bucket. In that scenario, I could have put **CloudFront** in front of my S3 bucket to act as a **CDN**. I could create a bucket policy that only allows access from CloudFront. I could even put an AWS **WAF** in front of my bucket if it is hosting dynamic content. No one from the Internet would ever have direct access to the bucket, and the website would be more secure.

In addition to those options, you could configure permissions in your account to limit who can make buckets public. AWS made this easier by adding a new screen in S3 that allows you to lock down the ability to create public **bucket policies** or change **S3 ACLs** to allow public access. You can limit who has permission to change these settings and prevent any changes that would cause a bucket to become public and expose data.



What else could a large company do to prevent unwanted changes to S3 buckets? There's a feature called **VPC endpoints** (formerly I have referred to these as S3 endpoints as that was the first service that used them). You can set up VPC Endpoints to restrict access to all your S3 buckets from your AWS account over the AWS network and restrict access to the bucket only from specific endpoints. The endpoints could be configured by a team that understands networking and security, while developers would be allowed to create new buckets through restrictive IAM policies and **segregation of duties** with security checks that enforce VPC Endpoints to access S3 buckets.

S3 buckets used to require traversal over the Internet to access files in them. While on the Capital One cloud team, I helped manage the feature requests. One of them was private access S3 buckets. VPC Endpoints is the solution to that problem. VPC endpoints limit the traffic to the AWS backbone. You can also create restrictions in **VPC endpoint policies** on top of your **IAM policies** that can restrict which buckets a user or application can access, and S3 bucket polices that limit who can access the bucket.

In summary, if you set up your policies correctly and leverage all the tools provided by AWS, you can implement automated governance to prevent people from making mistakes, and any malware that might gain developer or application credentials from opening up private S3 buckets to the Internet. The same principles apply to similar services with different names on Azure and GCP. There's a lot more to a solid governance and deployment strategy, but those are a few things that will get you headed down the right path!

Teri Radichel — Follow me: @teriradichel

---

Check out the book I'm writing: Cybersecurity for Executives

---

*Upcoming events where you can hear Teri Radichel speak about Ot teach cloud security:*

*Cloud Security Training in Seattle*

*AWS RE:INFORCE ~ Are you ready for a cloud pentest? (June 25–26)*

Serverless Days ~ London (July 11)

*IANS Charlotte Information Security Forum (September 25–26)*

*IANS Houston Information Security Forum (September 11)*

Bienvenue au congrès ISACA Québec 2019

…and of course she's usually at the Seattle AWS Architects and Engineers Meetup sponsored by 2nd Sight Lab!

Past Cloud Security Presentations (Videos and Podcasts)

RSA ~ Red Team vs. Blue Team on AWS with Kolby Allen

AWS re:Invent ~ RedTeam vs. Blue Team on AWS with Kolby Allen

Microsoft Build ~ DIY Security Assessment with SheHacksPurple

Masters of Data ~ Sumo Logic Podcast

*Follow me for future blog posts on cloud security, or sign up for **cloud security training** to learn more.* 

AWS | S3 Bucket | Data Breach | Cloud Security | Cybersecurity Training

57 claps

WRITTEN BY

**Teri Radichel**

Cloud Security Training and Consulting | GSE 240, GSEC, GCIH, GCIA, GCPM, GCCC, GREM, GPEN, GXPN | AWS Hero | Infragard | IANS Faculty | 2ndSightLab.com

Follow

## Cloud Security

Follow

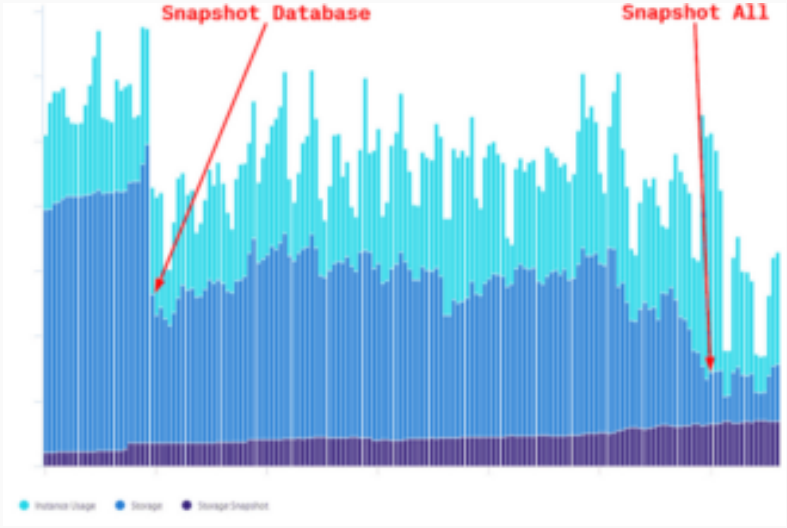
## More From Medium

Related reads

### Reducing AWS Costs With Step Functions

Chad Van Wyhe in PCI TechBlog
Nov 15, 2018 · 5 min read

413

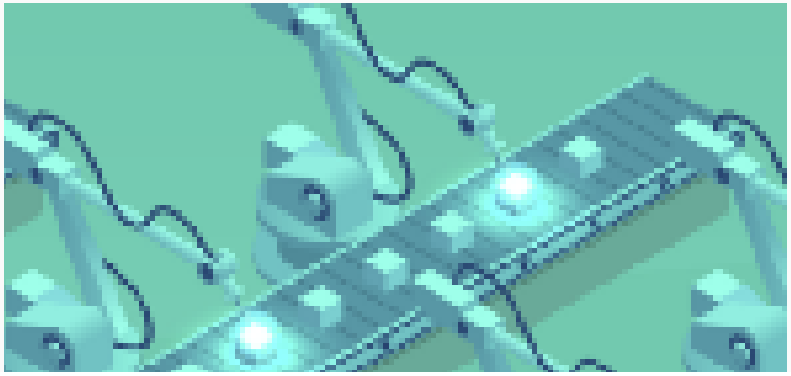



Related reads

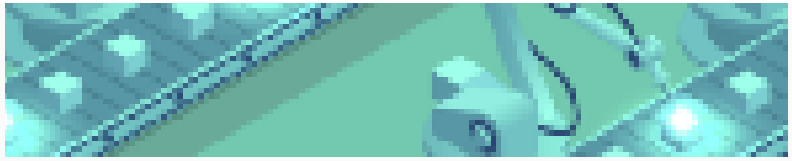
### AWS S3 Batch Operations: Beginner's Guide

Simon-Pierre Gingras in poka-...

210



Feb 18 · 6 min read



Related reads

## Store & Fetch from DynamoDB with AWS Lambda


Luke Mwila in HackerNoon.com
May 27 · 7 min read ★

195