

# 100 Days of DevOps — Day 11- Restricting S3 Bucket Access to Specific IP Addresses

Check the updated 101 Days of DevOps Course

Course Registration link: <https://www.101daysofdevops.com/register/>

Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>

YouTube link: <https://www.youtube.com/user/laprashant/videos>

Welcome to Day 11 of 100 Days of DevOps, Let continue our journey with IAM and let discuss one of the common topic/requirement I often encounter in our daily jobs where I need to restrict S3 access from specific IP address.

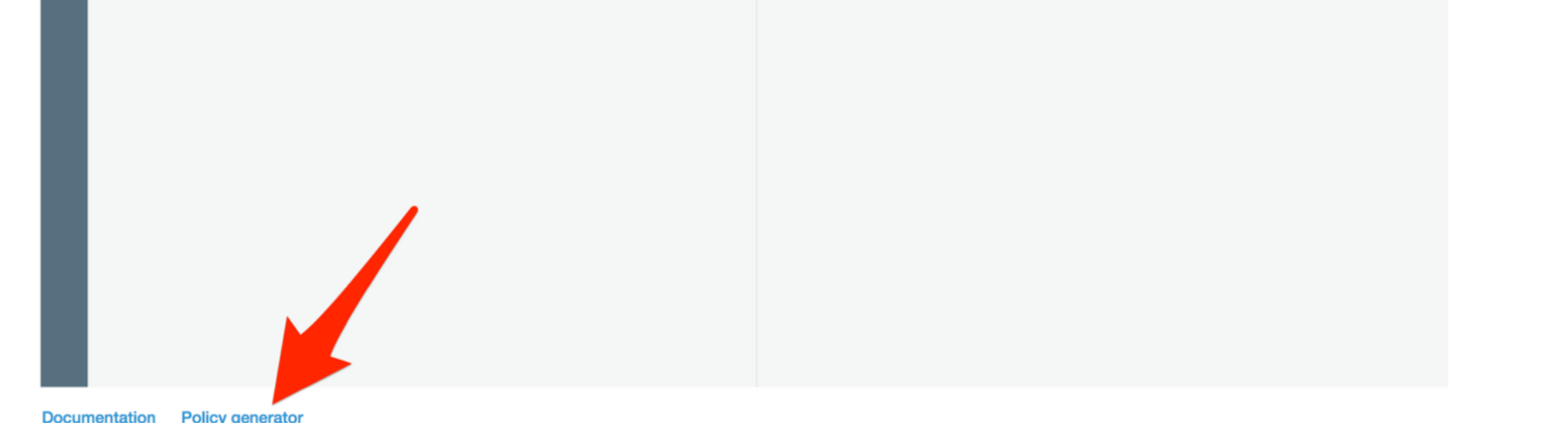
**Problem:** Restrict S3 bucket access(Get/Put Operation from specific IP)

**Solution:** This can be done using the S3 bucket policies

S3 Bucket policies come under Resource Policies that control who has access to the specific resource.

Step1:

Go to S3 console <https://s3.console.aws.amazon.com/s3/home?region=us-west-2> → Specific Bucket → Permissions → Bucket Policy → Policy



Step2: Fill all the details

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect

☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service

☐ All Services (\*)

Use multiple statements to add permissions for more than one service.

Actions

☐ All Actions (\*)

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::<bucket\_name>/<key\_name>. Use a comma to follow multiple values.

Add Conditions (Optional)

Conditions are any restrictions or details about the statement. [More Details](#).

Condition

Key

Value


Resource field is not valid. You must enter a valid ARN.

```
* Effect: Allow
* Principal: *
* AWS Service: Amazon S3
* Action: Select GetObject and PutObject
* Amazon Resource Name(ARN): <arn of your S3 bucket>/* <---Don't forget to Put /* at the end
Add Conditions
* Condition: IpAddress
* Key: aws:SourceIp
* Value: 192.168.0.2/24 (Specify your IP Address)
```

S3 Bucket action doesn't apply to any resources


Thanks for contributing an answer to Stack Overflow! Please be sure to answer the question. Provide details and share...

stackoverflow.com



Final Policy will look like this

```
1
2 {
3   "Id": "Policy1550810272864",
4   "Version": "2012-10-17",
5   "Statement": [
6     {
7       "Sid": "Stmt1550810271230",
8       "Action": [
9         "s3:GetObject",
10        "s3:PutObject"
11      ],
12      "Effect": "Allow",
13      "Resource": "arn:aws:s3:::mytests3bucketforpermissionboundaries/*",
14      "Condition": {
15        "IpAddress": {
16          "aws:SourceIp": "67.164.4.229"
17        }
18      },
19      "Principal": "*"
20    }
21  ]
22 }
```

s3bucketpolicy.json hosted with  by GitHub [view raw](#)

- Step3: Copy paste this policy to the Bucket Policy Editor and save it
- Step4: Test it

## AWS CLI

```
* Create a json file bucketpolicy.json
* aws s3api put-bucket-policy --bucket my-test-bucket --policy file://bucketpolicy.json
```

## Terraform

```
1 provider "aws" {
2   region = "us-west-2"
3 }
4 resource "aws_s3_bucket_policy" "b" {
5   bucket = "mytests3bucket"
6
7   policy = <<POLICY
8 {
9   "Version": "2012-10-17",
10  "Id": "MYBUCKETPOLICY",
11  "Statement": [
12    {
13      "Sid": "IPAllow",
14      "Effect": "Allow",
15      "Principal": "*",
16      "Action": [
17        "s3:GetObject",
18        "s3:PutObject"
19      ],
20      "Resource": "arn:aws:s3:::mytests3bucket*",
21      "Condition": {
22        "IpAddress": {"aws:SourceIp": "192.168.0.2/24"}
23      }
24    }
25  ]
26 }
27 POLICY
28 }
```

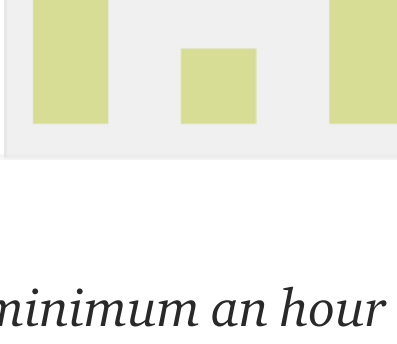
s3bucketpolicy.tf hosted with  by GitHub [view raw](#)

GitHub link

100daysofdevops/100daysofdevops

Contribute to 100daysofdevops/100daysofdevops development by creating an account on GitHub.

github.com



Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.



- Twitter: [@100daysofdevops](#) OR [@lakhera2015](#)
- Facebook: <https://www.facebook.com/groups/795382630808645/>
- Medium: <https://medium.com/@devopslearning>
- Slack: <https://devops-myworld.slack.com/messages/CF41EFG49/>
- GitHub Link:<https://github.com/100daysofdevops>



## Reference

100 Days of DevOps — Day 0

D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)

medium.com

 7  1


 

Get an email whenever Prashant Lakhera publishes.

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

- More from Prashant Lakhera

Follow



AWS Community Builder, Ex-Redhat, Author, Blogger, RHCA, RHADS, RHCE, Docker Certified,4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP


Published in FAUN Publication · Feb 20, 2019

100 Days of DevOps — Day 10- Restricting User to Launch only T2 Instance

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS

5 min read



Share your ideas with millions of readers.


Feb 19, 2019

100 Days of DevOps — Day 9-Delegate Access Across AWS Accounts Using IAM Roles

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS

3 min read




Feb 18, 2019

100 Days of DevOps — Day 8-Introduction to AWS Security Token Service(STS)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS

4 min read




Feb 17, 2019

100 Days of DevOps — Day 7(AWS S3 Event)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>...

AWS

3 min read




Feb 16, 2019

100 Days of DevOps — Day 6-CloudWatch Logs(Metric Filters)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS


3 min read




Love podcasts or audiobooks? Learn on the go with our new app.

Get started

Sign In

 Search




Prashant Lakhera


4.6K Followers

AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHADS, RHCE, Docker Certified,4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP


Follow




More from Medium

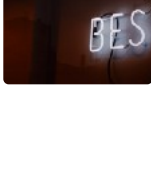
 P... in DevOps E...


How to setup AWS CodeCommit to use an SSH




 BoldLink.io


DevOps Tools in AWS




 Saka... in FAU...

Part Three of Infrastructure as Code(IAC) with...



 Prancer.io

Infrastructure As Code Best Practices



Help Status Writers Blog Careers

Privacy Terms About Knowable