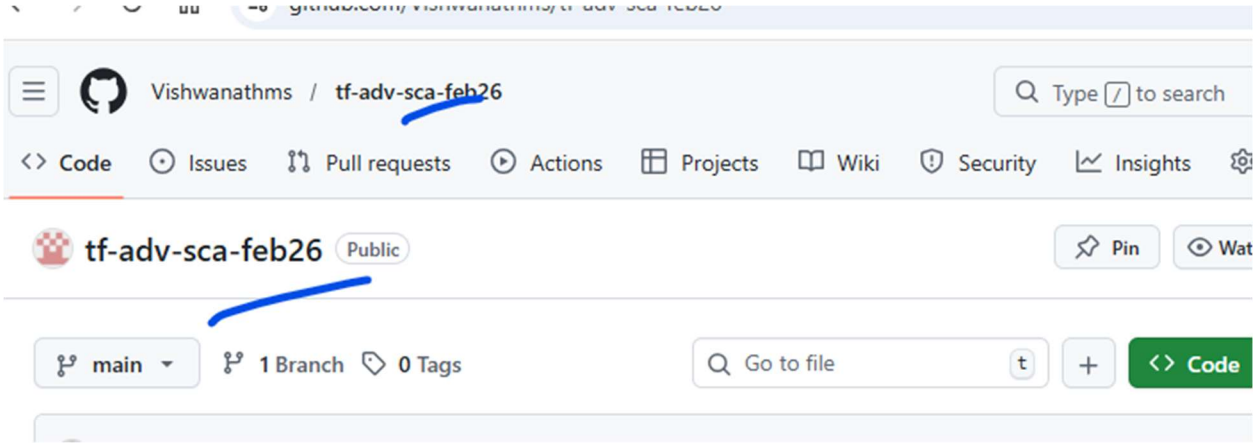
Tf-adv-lab1-Steps

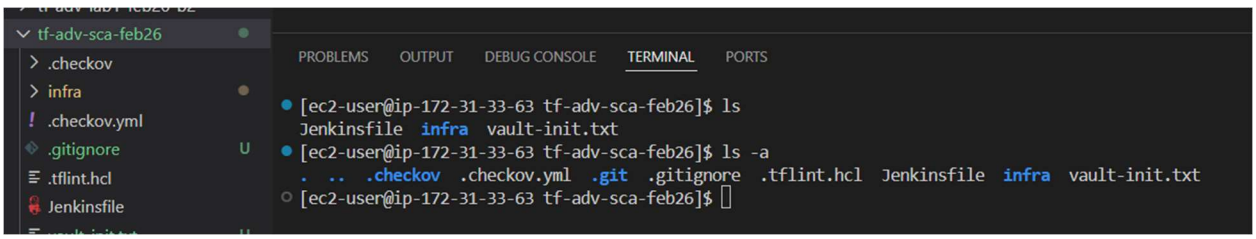
Steps:

1. Create github repo
2. Clone on the vs code
3. Copy the lab2 content to the new repo folder on vs code
4. Git commands to push to the github
5. Create an Jenkins pipeline (normal)
6. Run the Jenkins pipeline to check the output of “checkov”
7. Comment the checkov and uncomment the tflint , save the file, push the code
8. Run the Jenkins pipeline to check the output of “tflint”

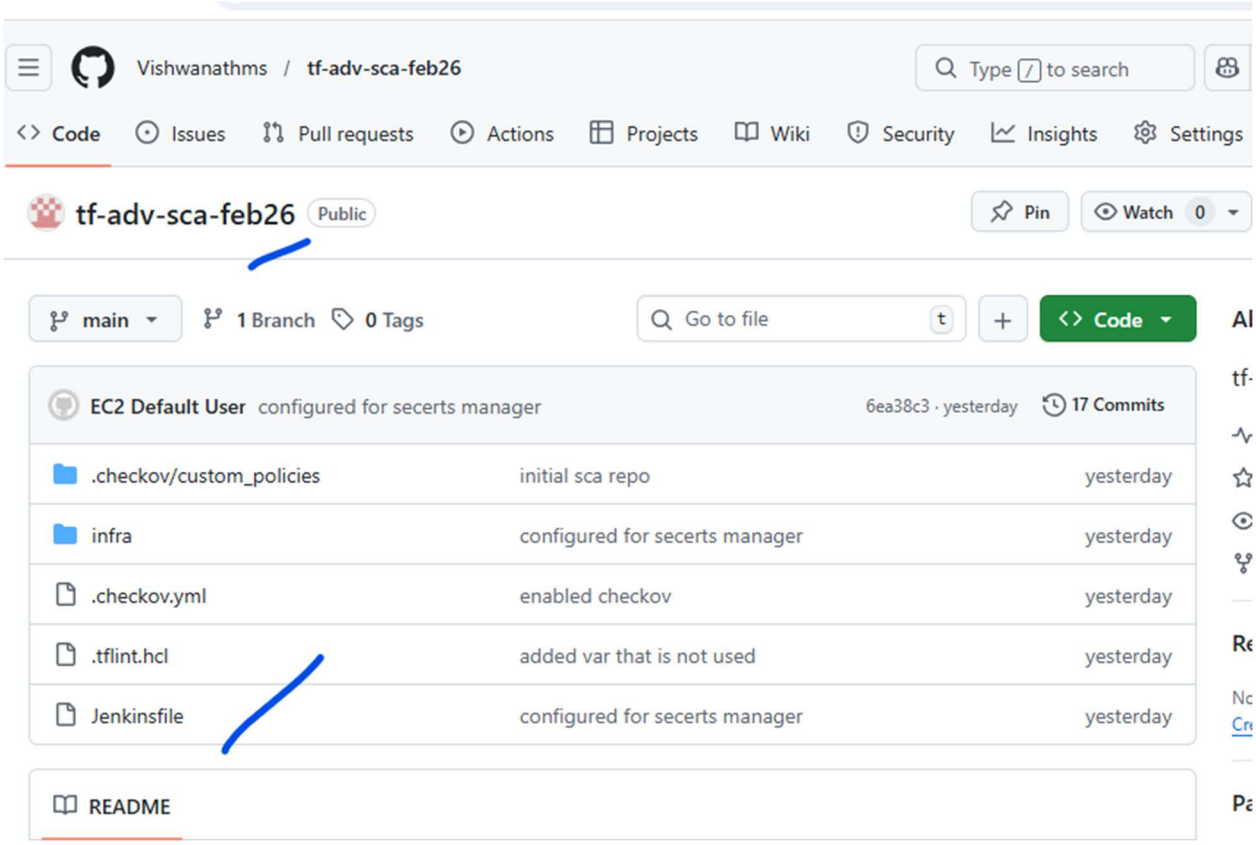
1. Create github repo



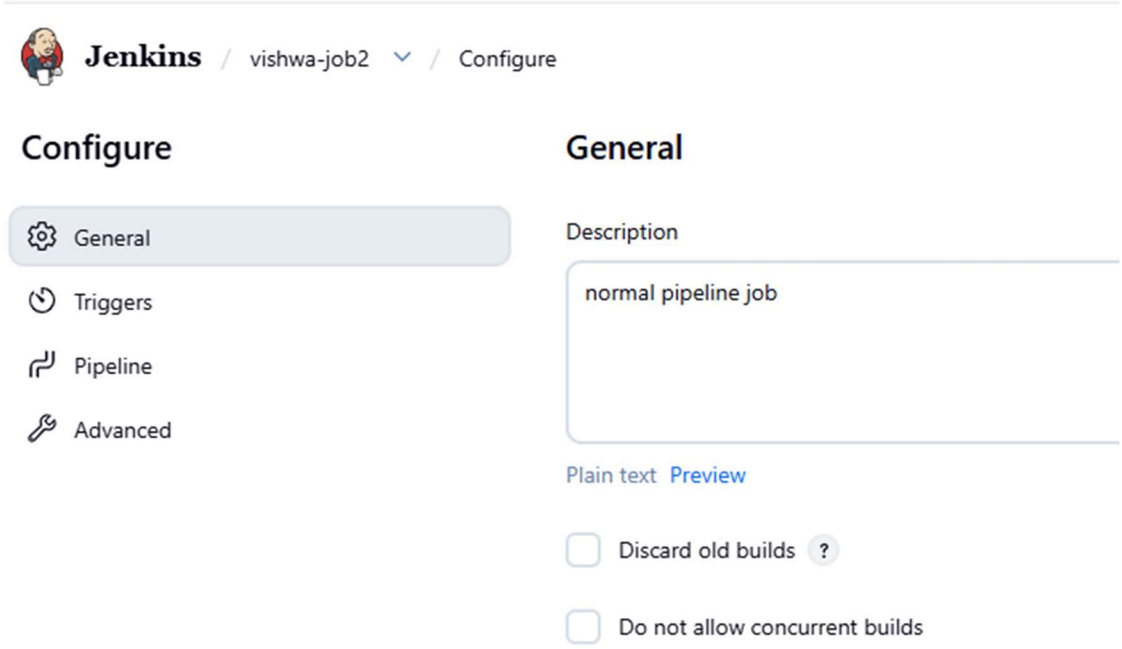
2. Clone on the vs code and Copy the lab2 content to the new repo folder on vs code

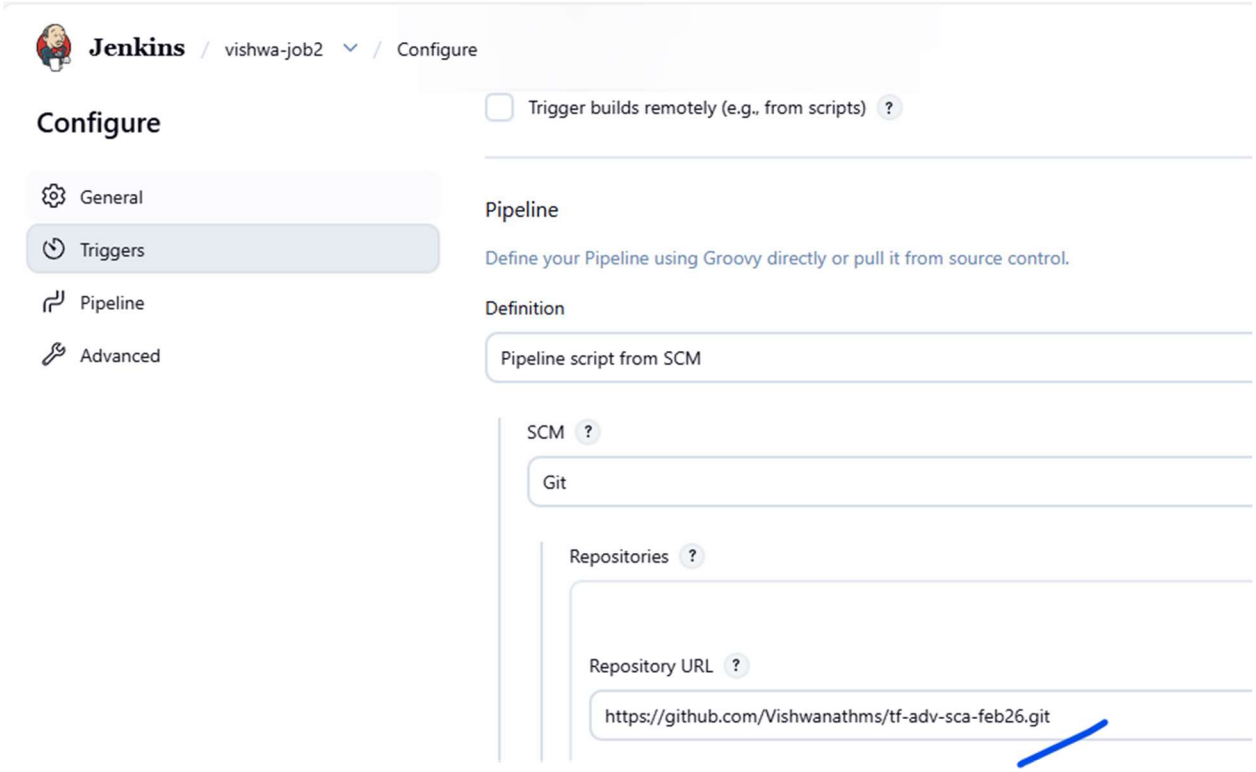


3. Git commands to push to the github

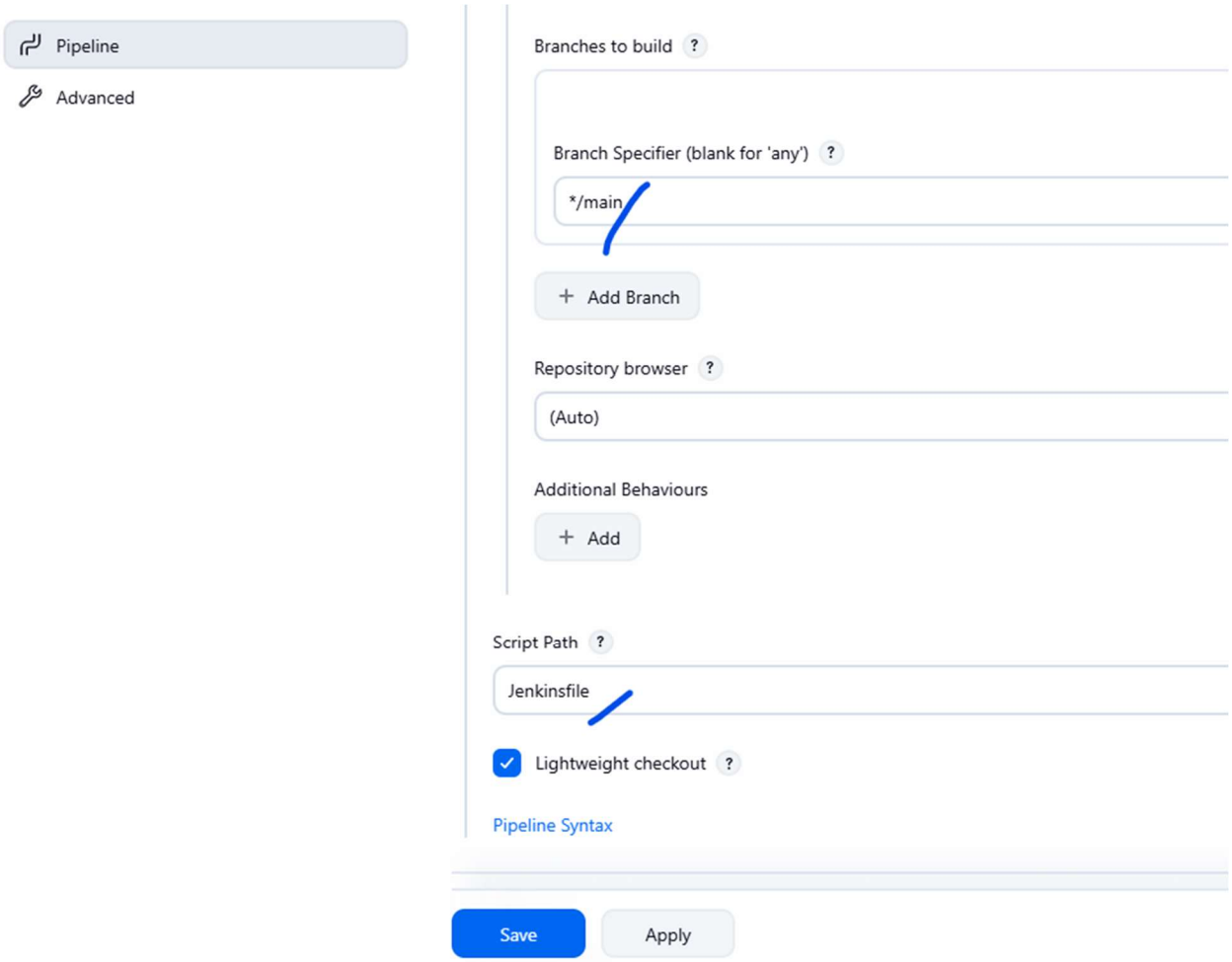


4. Create an Jenkins pipeline (normal)





Use the https, to avoid creds

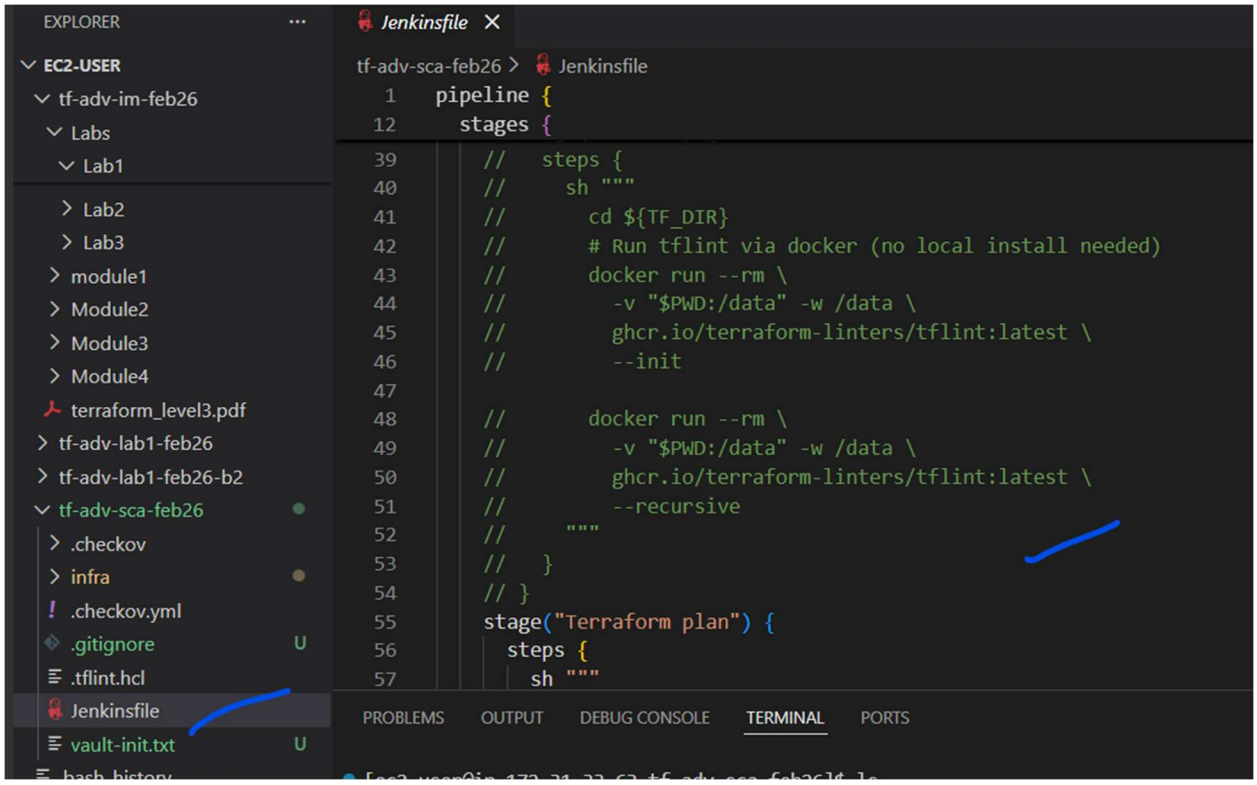


Change the branch to main and

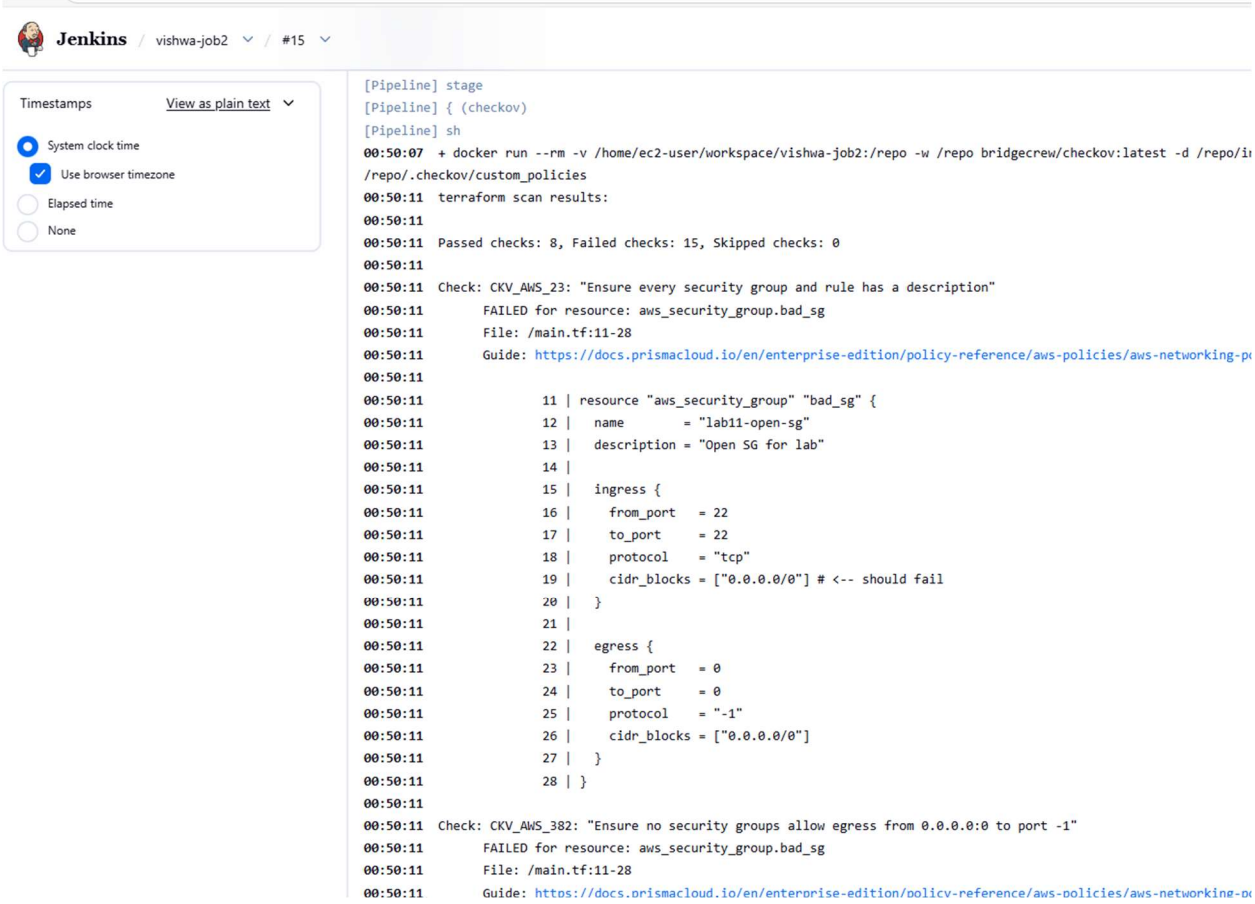
Give the right jenkinfile

5. Run the Jenkins pipeline

Note: for first time we will see the output of “Checkov”, so the tflint is commented.



Once we run the job


Jenkins / vishwa-job2 / #15
Timestamps View as plain text
System clock time
Use browser timezone
Elapsed time
None
[Pipeline] stage
[Pipeline] { (checkov)
[Pipeline] sh
00:50:07 + docker run --rm -v /home/ec2-user/workspace/vishwa-job2:/repo -w /repo bridgecrew/checkov:latest -d /repo/i
/repo/.checkov/custom_policies
00:50:11 terraform scan results:
00:50:11
00:50:11 Passed checks: 8, Failed checks: 15, Skipped checks: 0
00:50:11
00:50:11 Check: CKV_AWS_23: "Ensure every security group and rule has a description"
00:50:11 FAILED for resource: aws_security_group.bad_sg
00:50:11 File: /main.tf:11-28
00:50:11 Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-p
00:50:11
00:50:11 11 | resource "aws_security_group" "bad_sg" {
00:50:11 12 | name = "lab11-open-sg"
00:50:11 13 | description = "Open SG for lab"
00:50:11 14 |
00:50:11 15 | ingress {
00:50:11 16 | from_port = 22
00:50:11 17 | to_port = 22
00:50:11 18 | protocol = "tcp"
00:50:11 19 | cidr_blocks = ["0.0.0.0/0"] # <-- should fail
00:50:11 20 | }
00:50:11 21 |
00:50:11 22 | egress {
00:50:11 23 | from_port = 0
00:50:11 24 | to_port = 0
00:50:11 25 | protocol = "-1"
00:50:11 26 | cidr_blocks = ["0.0.0.0/0"]
00:50:11 27 | }
00:50:11 28 | }
00:50:11
00:50:11 Check: CKV_AWS_382: "Ensure no security groups allow egress from 0.0.0.0:0 to port -1"
00:50:11 FAILED for resource: aws_security_group.bad_sg
00:50:11 File: /main.tf:11-28
00:50:11 Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-p