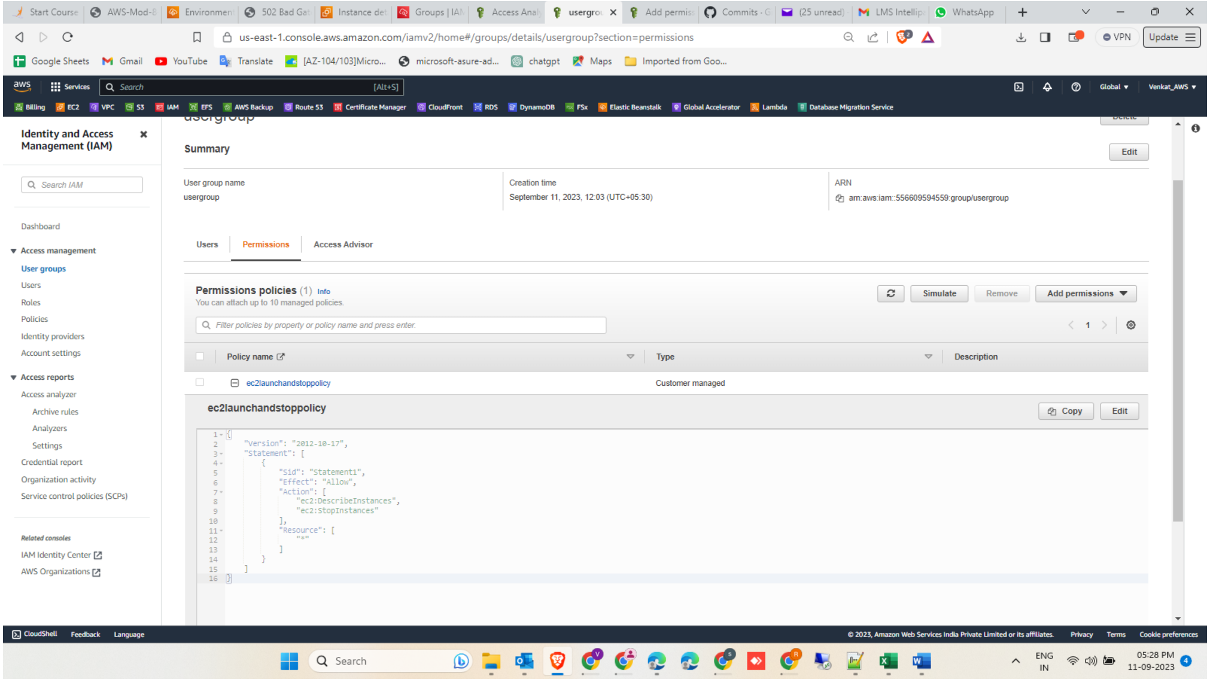
1. only launch or stop EC2 instances policy attached to the Group.



User group name: usergroup

Creation time: September 11, 2023, 12:03 (UTC+05:30)

ARN: arn:aws:iam::556609594559:group/usergroup

Permissions policies (1)

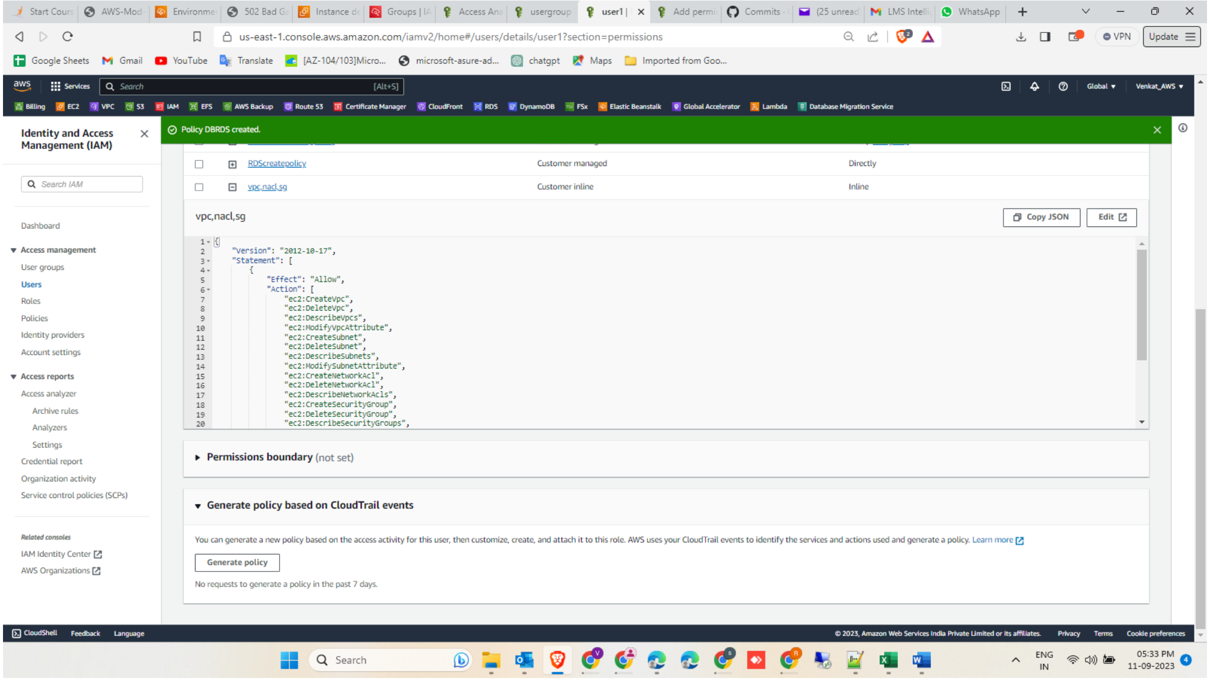
You can attach up to 10 managed policies.

Policy name	Type	Description
ec2launchandstoppolicy	Customer managed	

ec2launchandstoppolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

2. VPCs, subnets, NACL, and security groups permission attached for user.



Policy DBRDS created.

RDScreatepolicy	Customer managed	Directly
vpc,nacl,sg	Customer inline	Inline

vpc,nacl,sg

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpc",
                "ec2:DeleteVpc",
                "ec2:DescribeVpcs",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSubnet",
                "ec2:DeleteSubnet",
                "ec2:DescribeSubnets",
                "ec2:ModifySubnetAttribute",
                "ec2:CreateNetworkAcl",
                "ec2:DeleteNetworkAcl",
                "ec2:DescribeNetworkAcls",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

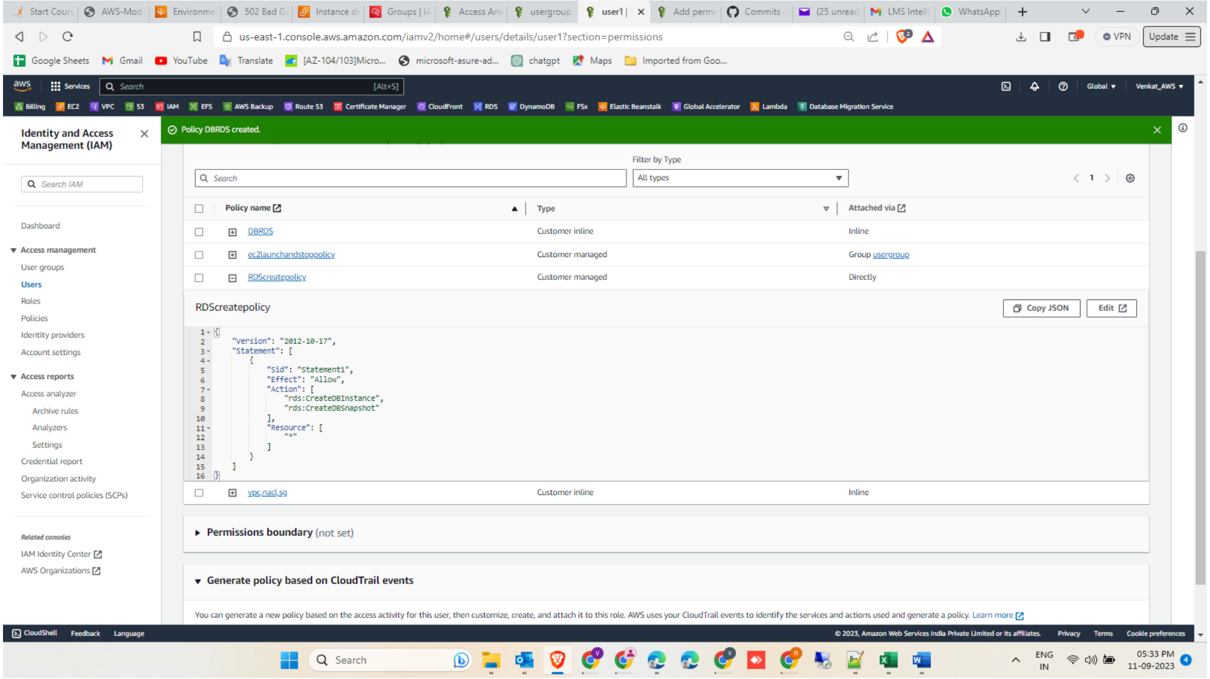
Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

3. RDS create policy permission added to the user.



Policy DBRDS created.

Policy name	Type	Attached via
DBRDS	Customer inline	Inline
ec2launchandstoppolicy	Customer managed	Group usergroup
RDScreatepolicy	Customer managed	Directly
vpc.nacl.sg	Customer inline	Inline

RDScreatepolicy

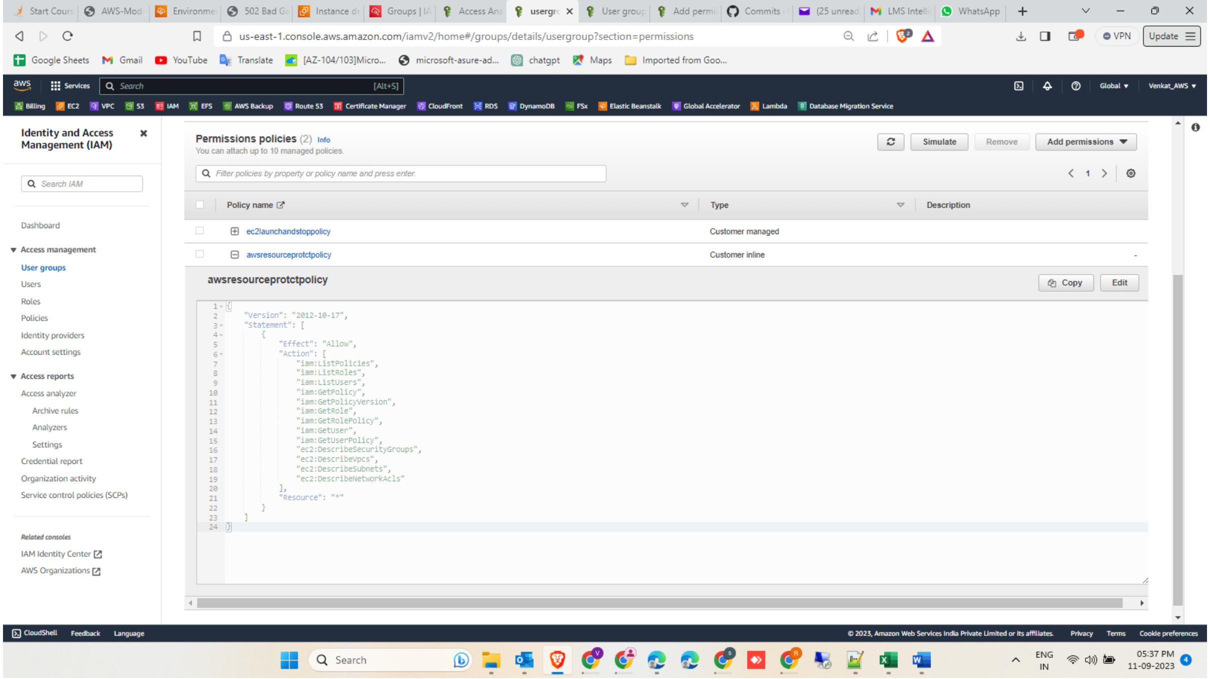
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance",
                "rds:CreateDBSnapshot"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

4. Security protects policy permission created for group.


us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/usergroup?section=permissions
Identity and Access Management (IAM)
Simulate
Remove
Add permissions
Copy
Edit

Permissions policies (2) Info

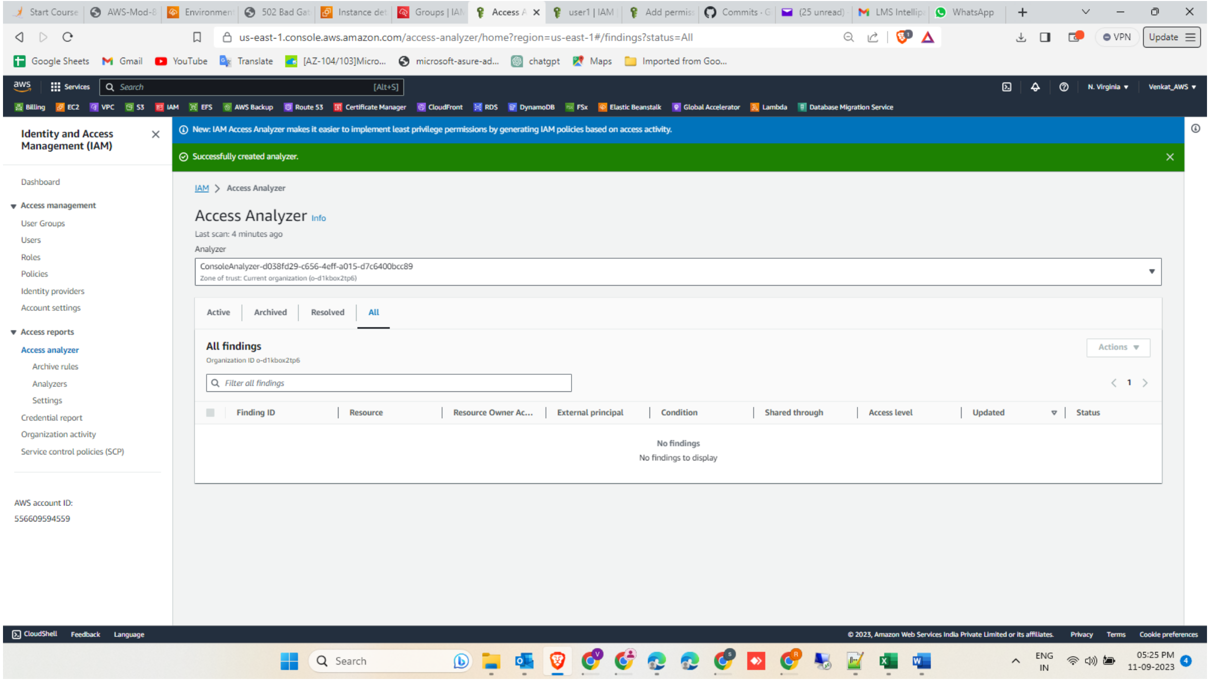
You can attach up to 10 managed policies.

Policy name	Type	Description
ec2launchandstoppolicy	Customer managed	
awsresourceprotctpolicy	Customer inline	-

awsresourceprotctpolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListPolicies",
                "iam:ListRoles",
                "iam:ListUsers",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:GetUserPolicy",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkAcls"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Created an IAM Access Analyzer, and I did not find any potential risk.



us-east-1.console.aws.amazon.com/access-analyzer/home?region=us-east-1#/findings?status=All

New: IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity.

Successfully created analyzer.

IAM > Access Analyzer

Access Analyzer Info

Last scan: 4 minutes ago

Analyzer: ConsoleAnalyzer-d038fd29-c656-4eff-a015-d7c6400bcc89

Zone of trust: Current organization (o-d1kbox2tp6)

Active | Archived | Resolved | All

All findings

Organization ID o-d1kbox2tp6

Finding ID	Resource	Resource Owner Ac...	External principal	Condition	Shared through	Access level	Updated	Status

No findings

No findings to display

AWS account ID: 556609594559