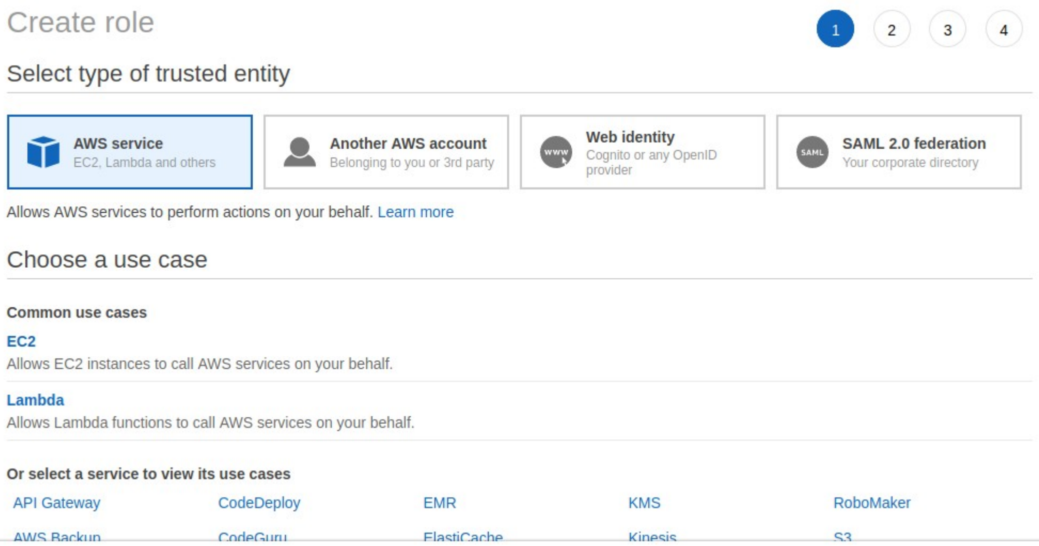
IAM Session

1. Create a Role with full access to S3



Create role

Select type of trusted entity

AWS service EC2, Lambda and others

Another AWS account Belonging to you or 3rd party

Web identity Cognito or any OpenID provider

SAML 2.0 federation Your corporate directory

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

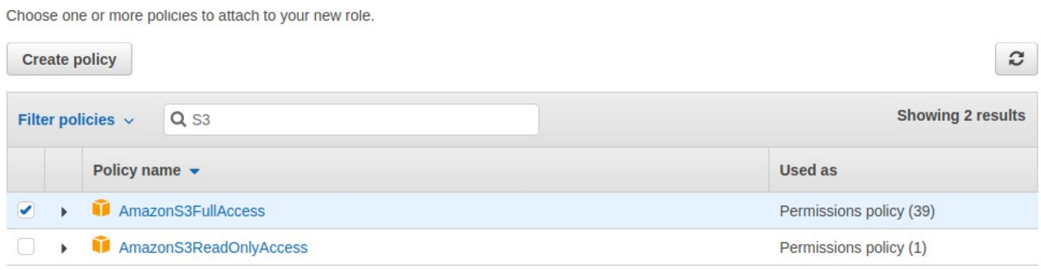
Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

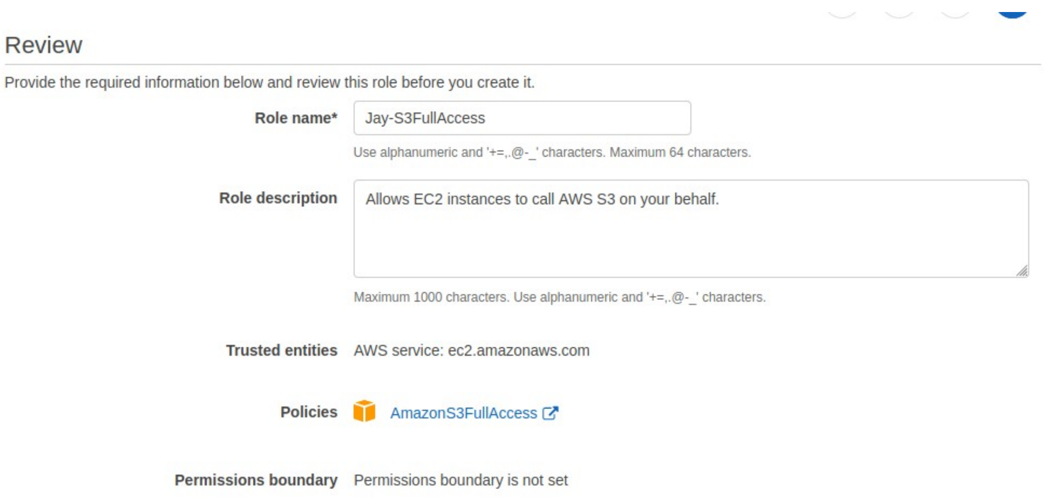
API Gateway CodeDeploy EMR KMS RoboMaker
AWS Backup CodeGuru ElastiCache Kinesis S3



Choose one or more policies to attach to your new role.

Filter policies ⌄ S3 **Showing 2 results**

		Policy name ▾	Used as
☑	▸	AmazonS3FullAccess	Permissions policy (39)
□	▸	AmazonS3ReadOnlyAccess	Permissions policy (1)



Review

Provide the required information below and review this role before you create it.

Role name* Jay-S3FullAccess
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

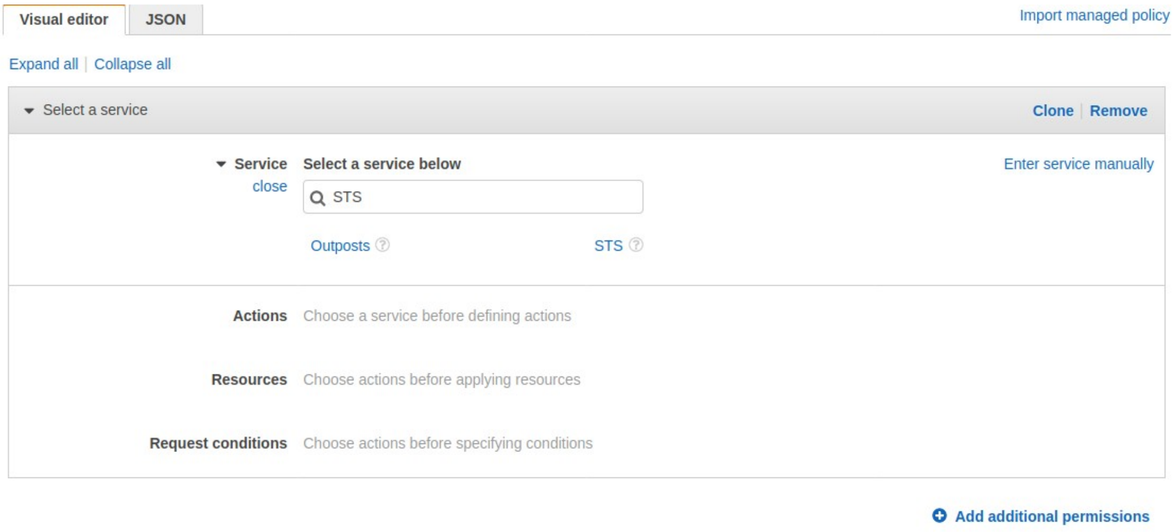
Role description Allows EC2 instances to call AWS S3 on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess

Permissions boundary Permissions boundary is not set

2. Create another which has the policy to assume the previous Role



Visual editor | JSON | Import managed policy

Expand all | Collapse all

Select a service — Clone | Remove

Service — Select a service below — Enter service manually
close

STS

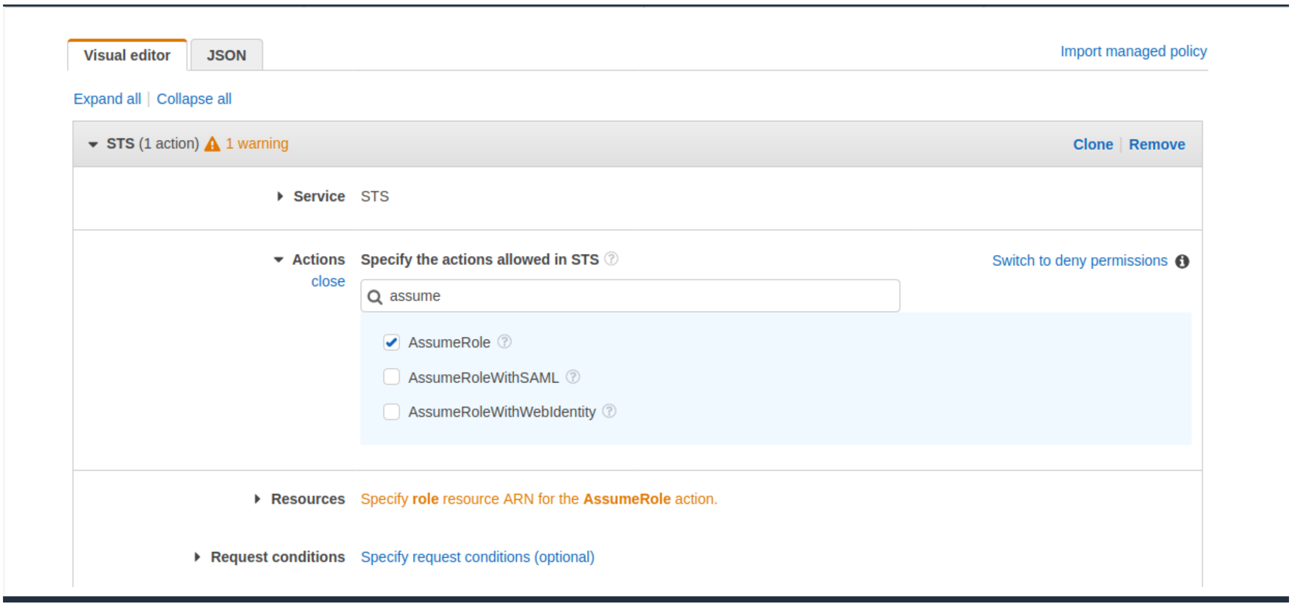
Outposts | STS

Actions — Choose a service before defining actions

Resources — Choose actions before applying resources

Request conditions — Choose actions before specifying conditions

Add additional permissions



Visual editor | JSON | Import managed policy

Expand all | Collapse all

STS (1 action) ⚠ 1 warning — Clone | Remove

Service — STS

Actions — Specify the actions allowed in STS — Switch to deny permissions
close

assume

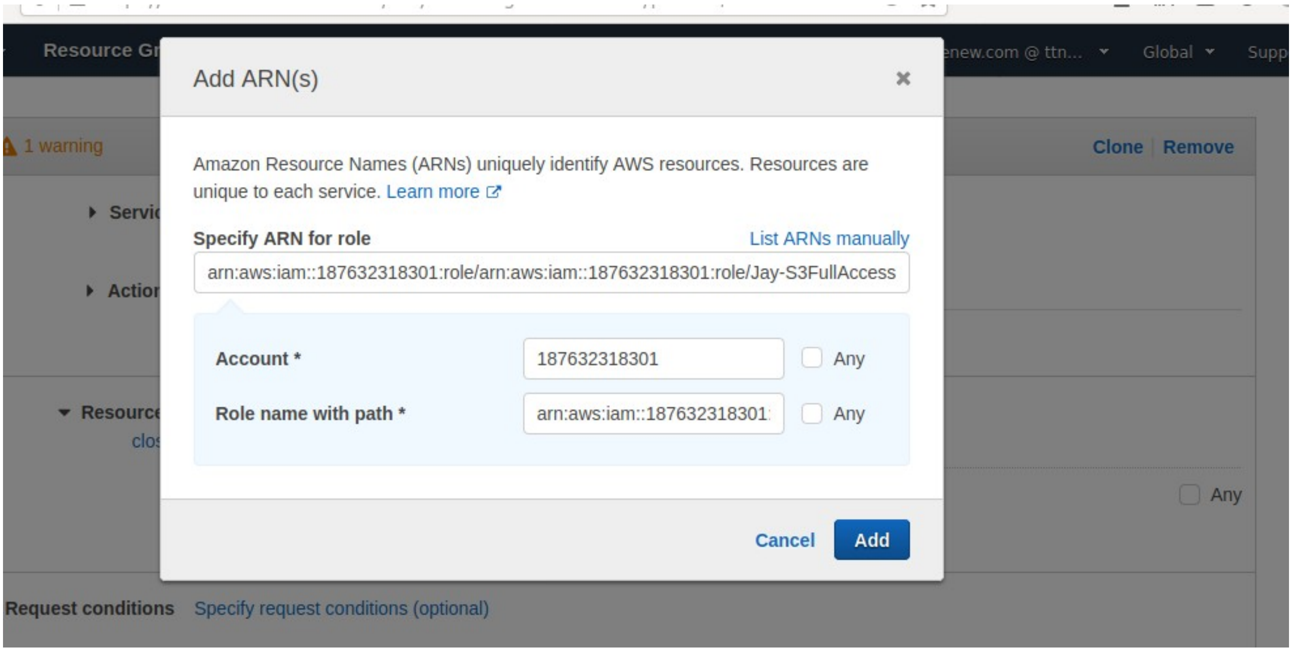
☑ AssumeRole

□ AssumeRoleWithSAML

□ AssumeRoleWithWebIdentity

Resources — Specify **role** resource ARN for the **AssumeRole** action.

Request conditions — Specify request conditions (optional)



Add ARN(s) ✖

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

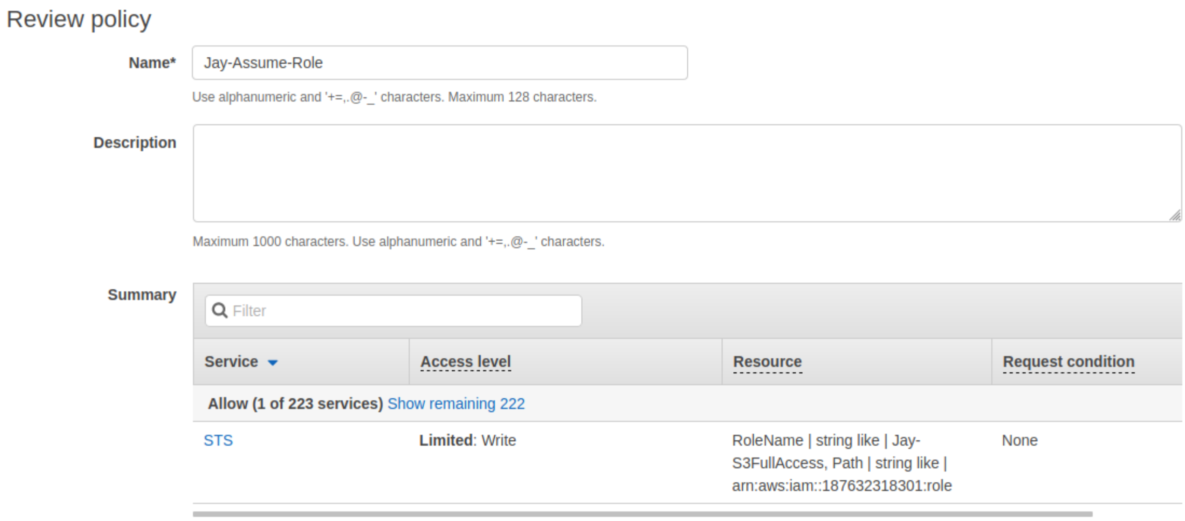
Specify ARN for role List ARNs manually

arn:aws:iam::187632318301:role/arn:aws:iam::187632318301:role/Jay-S3FullAccess

Account *	187632318301	□ Any
Role name with path *	arn:aws:iam::187632318301:	□ Any

Cancel | Add

Request conditions Specify request conditions (optional)



Review policy

Name* Jay-Assume-Role

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

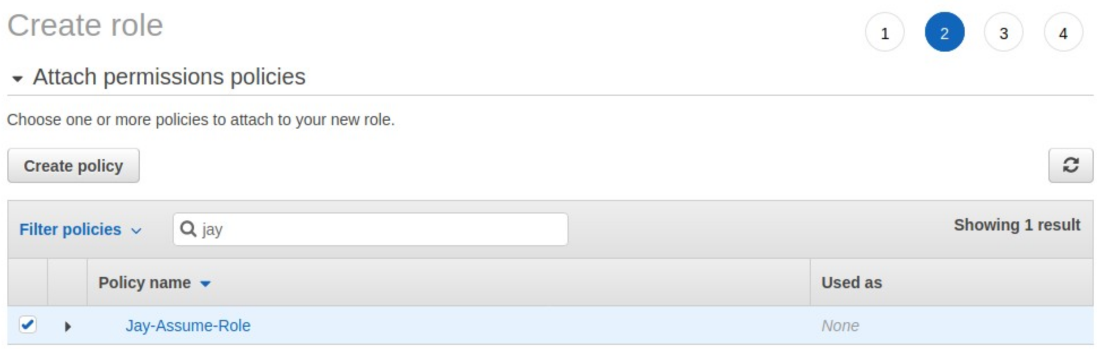
Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			
STS	**Limited**: Write	RoleName | string like | Jay-S3FullAccess, Path | string like | arn:aws:iam::187632318301:role	None



Create role

Attach permissions policies

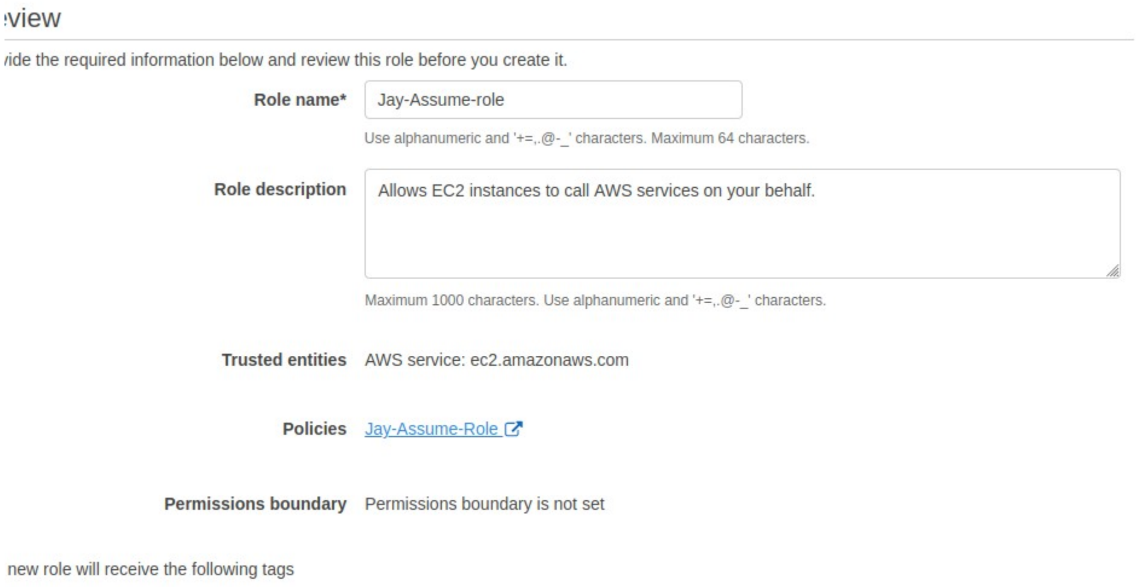
Choose one or more policies to attach to your new role.

Create policy

Filter policies ⌄ jay

Showing 1 result

		Policy name	Used as
☑	▸	Jay-Assume-Role	None



·view

/ide the required information below and review this role before you create it.

Role name* Jay-Assume-role

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.

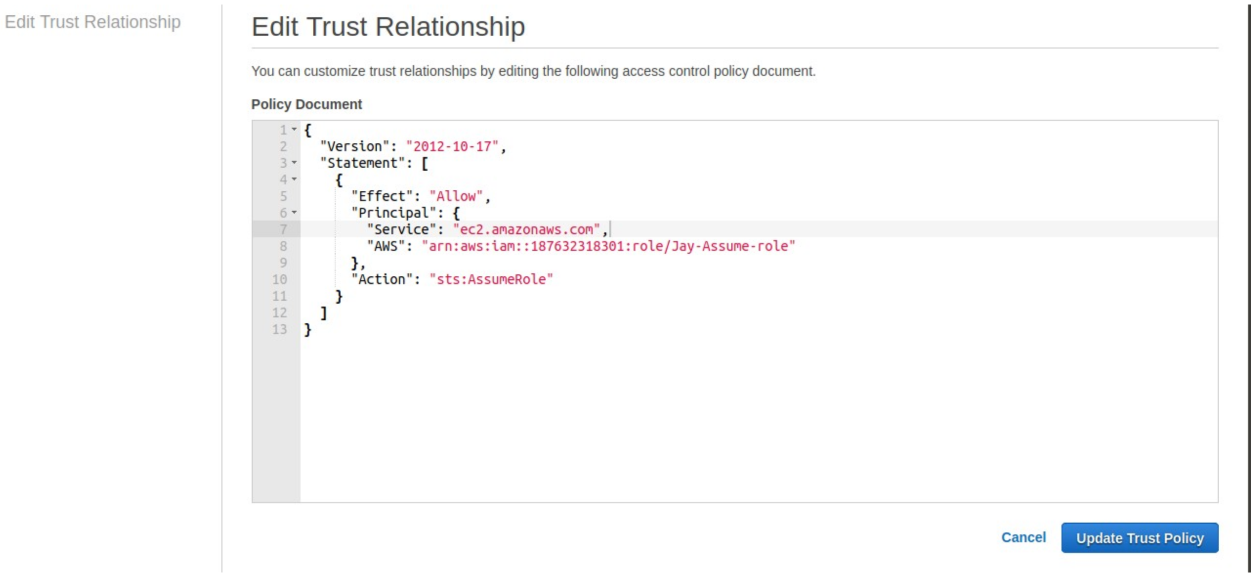
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies Jay-Assume-Role

Permissions boundary Permissions boundary is not set

new role will receive the following tags



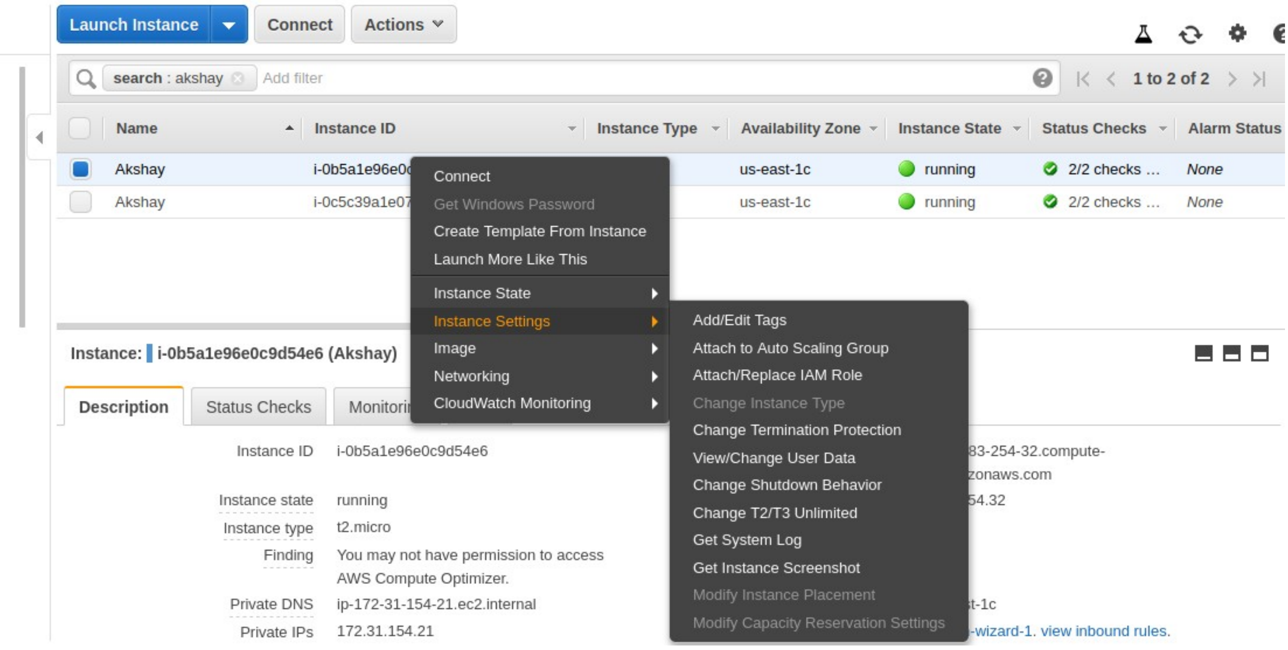
Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com",
        "AWS": "arn:aws:iam::187632318301:role/Jay-Assume-role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

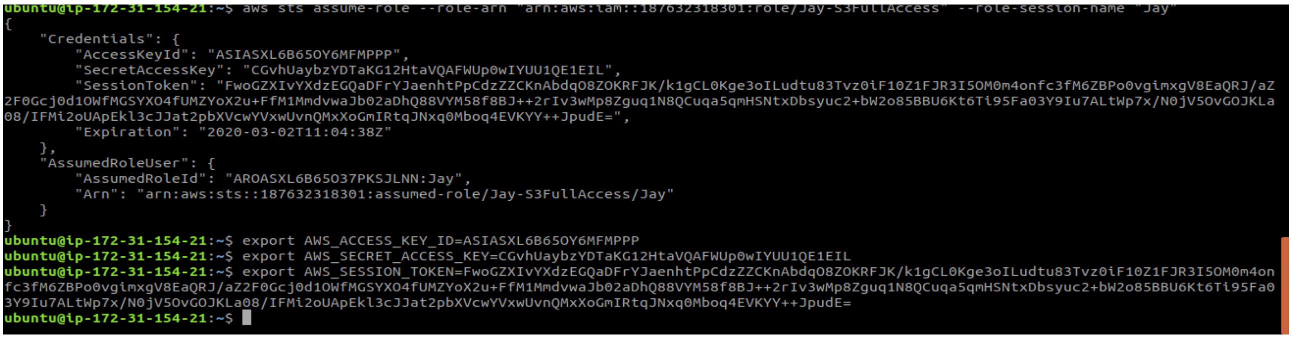
3. Attach this to an instance and get an sts token.



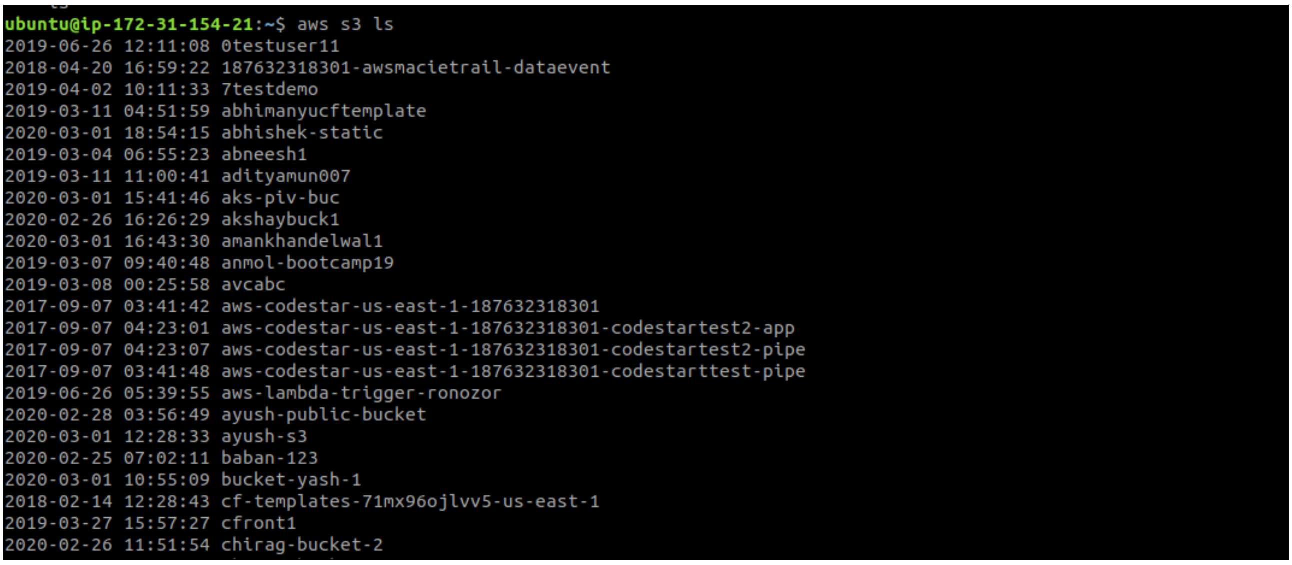
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Akshay	i-0b5a1e96e0c		us-east-1c	running	2/2 checks ...	None
Akshay	i-0c5c39a1e07		us-east-1c	running	2/2 checks ...	None

Instance: i-0b5a1e96e0c9d54e6 (Akshay)

Instance ID	i-0b5a1e96e0c9d54e6
Instance state	running
Instance type	t2.micro
Finding	You may not have permission to access AWS Compute Optimizer.
Private DNS	ip-172-31-154-21.ec2.internal
Private IPs	172.31.154.21



```
ubuntu@ip-172-31-154-21:~$ aws sts assume-role --role-arn "arn:aws:iam::187632318301:role/Jay-S3FullAccess" --role-session-name "Jay"
{
    "Credentials": {
        "AccessKeyId": "ASIASXL6B65OY6MFMPPP",
        "SecretAccessKey": "CGvhUaybzYDTaKG12HtaVQAFWUp0wIYUU1QE1EIL",
        "SessionToken": "FwoGZXIvYXdzEGQaDFrYJaenhtPpCdzZZCKnAbdqO8ZOKRFJK/k1gCL0Kge3oILudtu83Tvz0iF10Z1FJR3I5OM0m4onfc3fM6ZBPo0vgimxgV8EaQRJ/aZ
2F0Gcj0d1OWfMGSYXO4fUMZYoX2u+FfM1MmdvwaJb02aDhQ88VYM58f8BJ++2rIv3wMp8Zguq1N8QCuqa5qmHSNtxDbsyuc2+bW2o85BBU6Kt6Ti95Fa03Y9Iu7ALtWp7x/N0jV5OvGOJKLa
08/IFMi2oUApEkl3cJJat2pbXVcwYVxwUvnQMxXoGmIRtqJNxq0Mboq4EVKYY++JpudE=",
        "Expiration": "2020-03-02T11:04:38Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROASXL6B65O37PKSJLNN:Jay",
        "Arn": "arn:aws:sts::187632318301:assumed-role/Jay-S3FullAccess/Jay"
    }
}
ubuntu@ip-172-31-154-21:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B65OY6MFMPPP
ubuntu@ip-172-31-154-21:~$ export AWS_SECRET_ACCESS_KEY=CGvhUaybzYDTaKG12HtaVQAFWUp0wIYUU1QE1EIL
ubuntu@ip-172-31-154-21:~$ export AWS_SESSION_TOKEN=FwoGZXIvYXdzEGQaDFrYJaenhtPpCdzZZCKnAbdqO8ZOKRFJK/k1gCL0Kge3oILudtu83Tvz0iF10Z1FJR3I5OM0m4on
fc3fM6ZBPo0vgimxgV8EaQRJ/aZ2F0Gcj0d1OWfMGSYXO4fUMZYoX2u+FfM1MmdvwaJb02aDhQ88VYM58f8BJ++2rIv3wMp8Zguq1N8QCuqa5qmHSNtxDbsyuc2+bW2o85BBU6Kt6Ti95Fa0
3Y9Iu7ALtWp7x/N0jV5OvGOJKLa08/IFMi2oUApEkl3cJJat2pbXVcwYVxwUvnQMxXoGmIRtqJNxq0Mboq4EVKYY++JpudE=
ubuntu@ip-172-31-154-21:~$
```

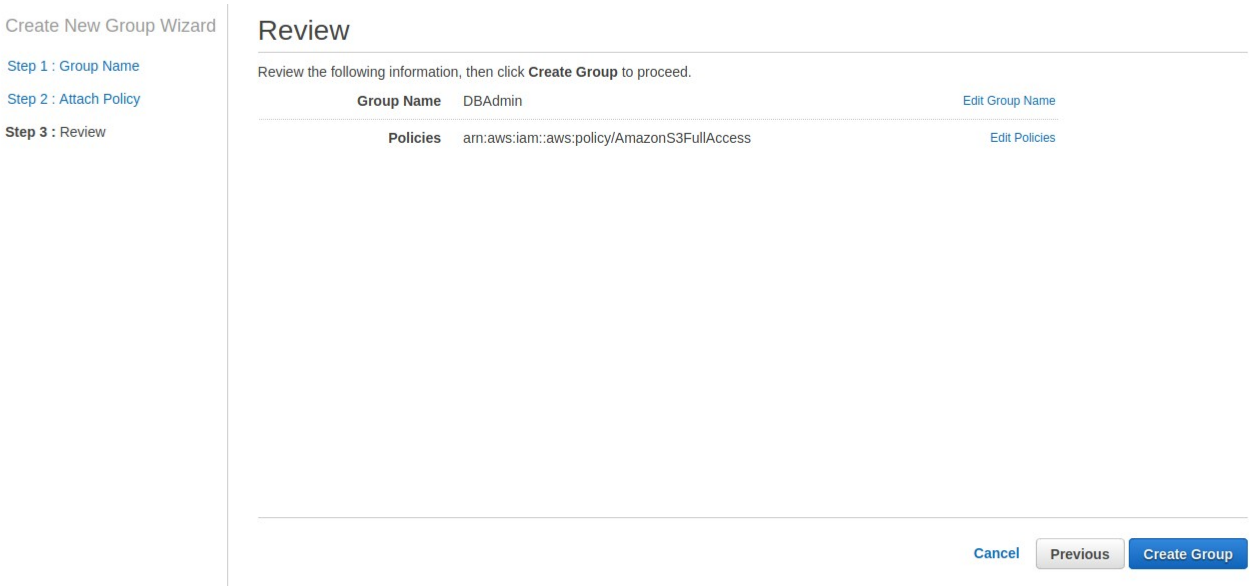


```
ubuntu@ip-172-31-154-21:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-03-01 18:54:15 abhishek-static
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-03-01 15:41:46 aks-piv-buc
2020-02-26 16:26:29 akshaybuck1
2020-03-01 16:43:30 amankhandelwal1
2019-03-07 09:40:48 anmol-bootcamp19
2019-03-08 00:25:58 avcabc
2017-09-07 03:41:42 aws-codestar-us-east-1-187632318301
2017-09-07 04:23:01 aws-codestar-us-east-1-187632318301-codestartest2-app
2017-09-07 04:23:07 aws-codestar-us-east-1-187632318301-codestartest2-pipe
2017-09-07 03:41:48 aws-codestar-us-east-1-187632318301-codestarttest-pipe
2019-06-26 05:39:55 aws-lambda-trigger-ronozor
2020-02-28 03:56:49 ayush-public-bucket
2020-03-01 12:28:33 ayush-s3
2020-02-25 07:02:11 baban-123
2020-03-01 10:55:09 bucket-yash-1
2018-02-14 12:28:43 cf-templates-71mx96ojlvv5-us-east-1
2019-03-27 15:57:27 cfront1
2020-02-26 11:51:54 chirag-bucket-2
```

4. Create a group for "Data Administrator" where the user 'Alice' be a member of this group. This group will prepare the data for the analysis. So Provide the following access to the group.

Service: Amazon S3;
Action:

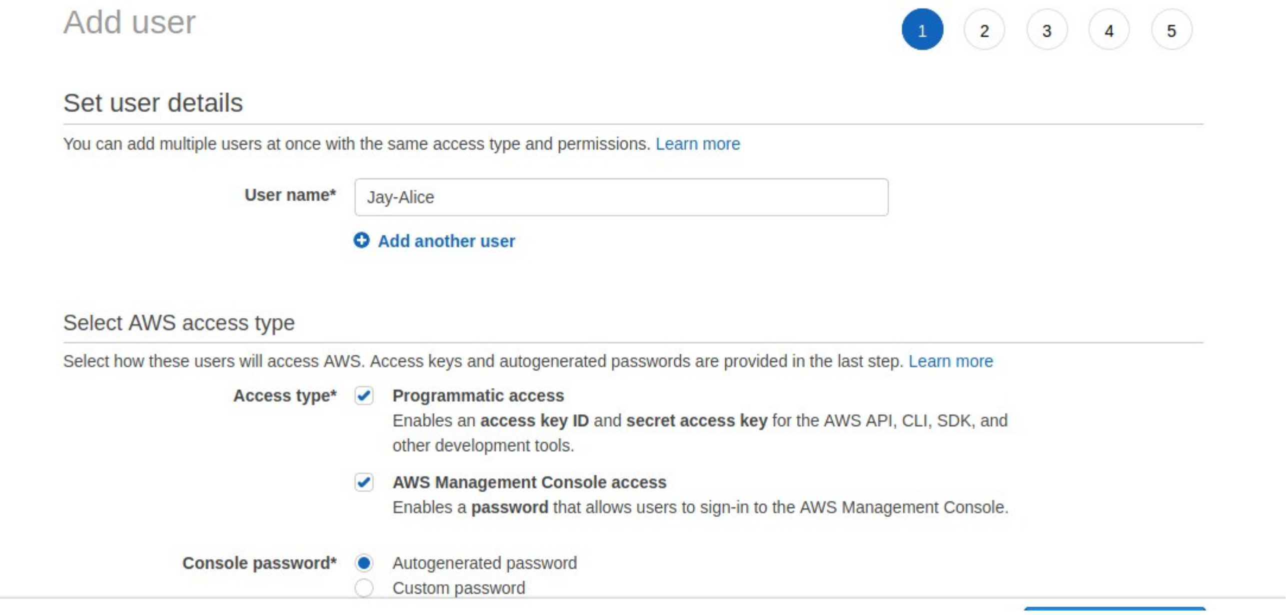
Get*,
List*,
Put*,
ARN: Input and output Buckets (no conditions)



Review

Review the following information, then click **Create Group** to proceed.

Group Name	DBAdmin	Edit Group Name
Policies	arn:aws:iam::aws:policy/AmazonS3FullAccess	Edit Policies



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Jay-Alice

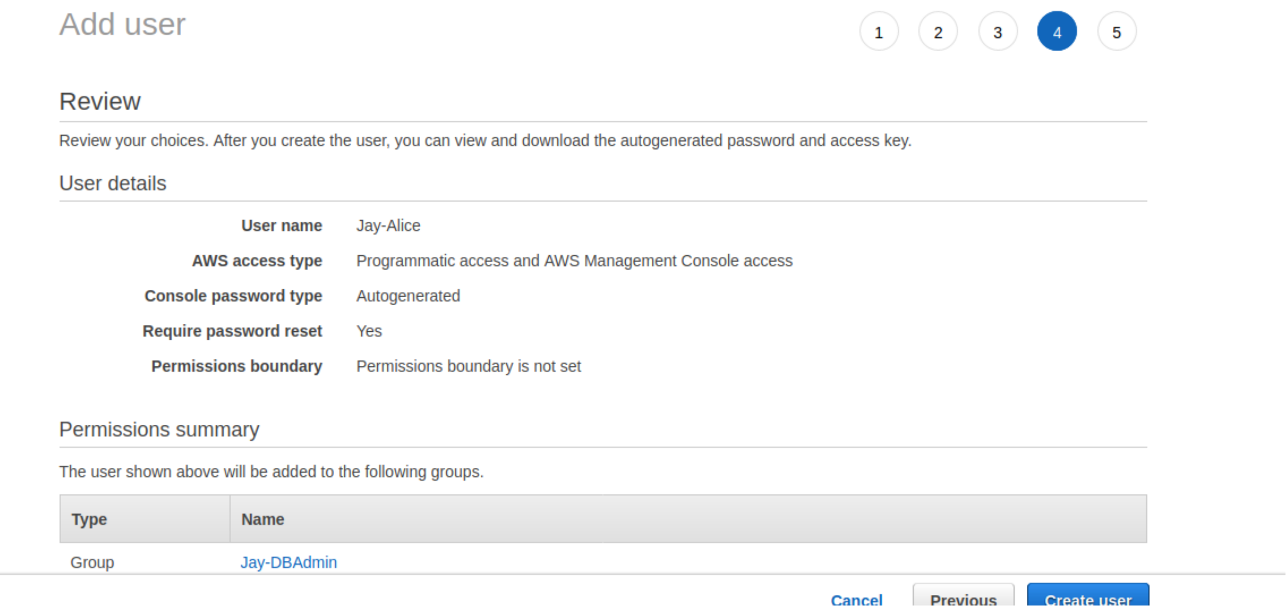
Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom password



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

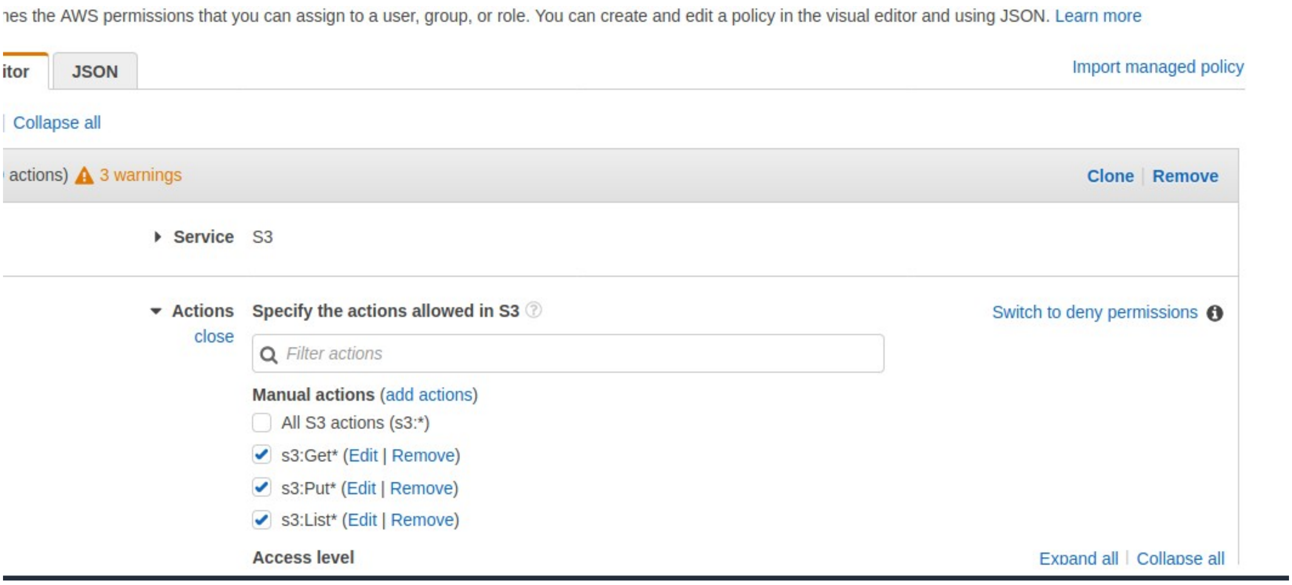
User details

User name	Jay-Alice
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	Jay-DBAdmin



ıes the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

actions) ⚠ 3 warnings

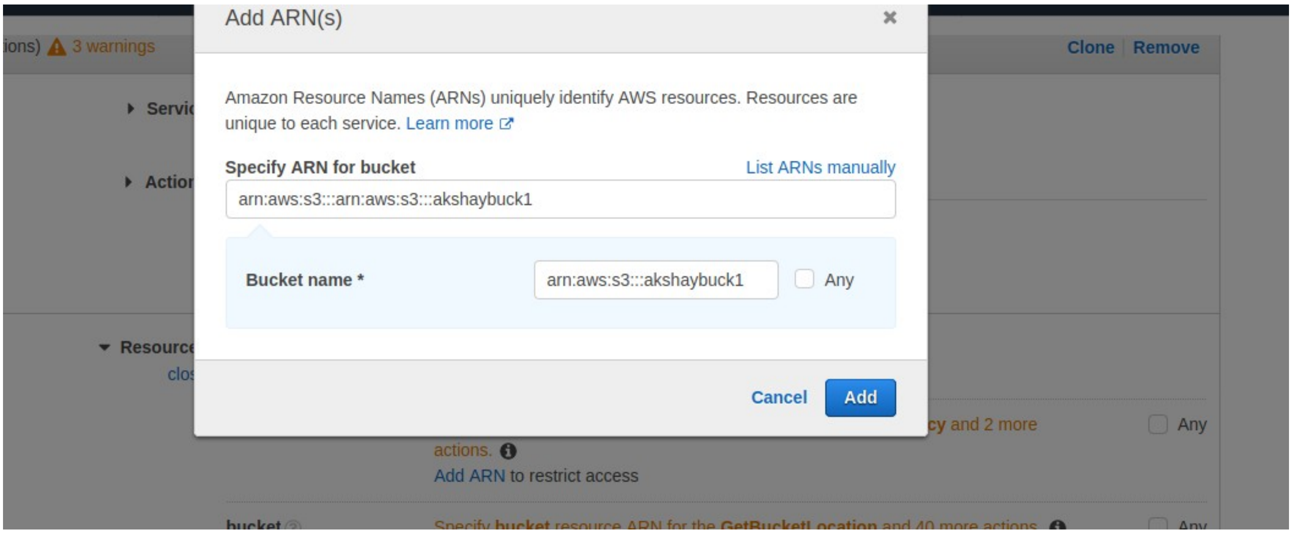
Service S3

Actions close — Specify the actions allowed in S3

Manual actions (add actions)

- □ All S3 actions (s3:*)
- ☑ s3:Get* (Edit | Remove)
- ☑ s3:Put* (Edit | Remove)
- ☑ s3:List* (Edit | Remove)

Access level



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for bucket

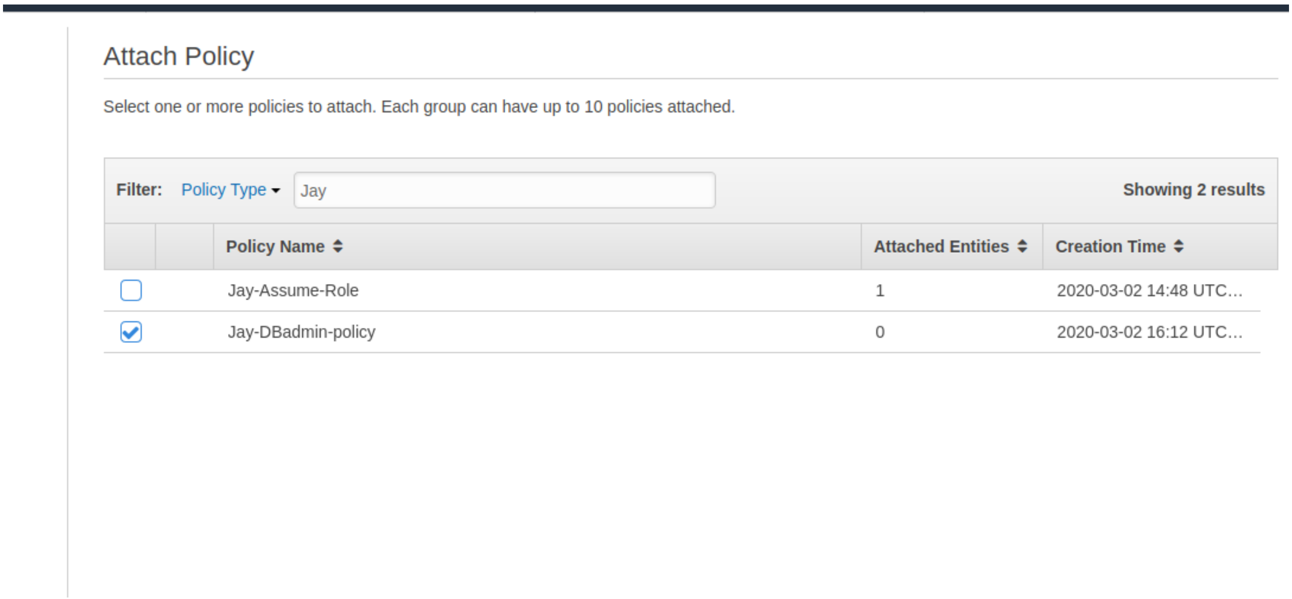
arn:aws:s3:::arn:aws:s3:::akshaybuck1

Bucket name * arn:aws:s3:::akshaybuck1 □ Any

cy and 2 more actions. □ Any

Add ARN to restrict access

bucket — Specify bucket resource ARN for the GetBucketLocation and 40 more actions. □ Any



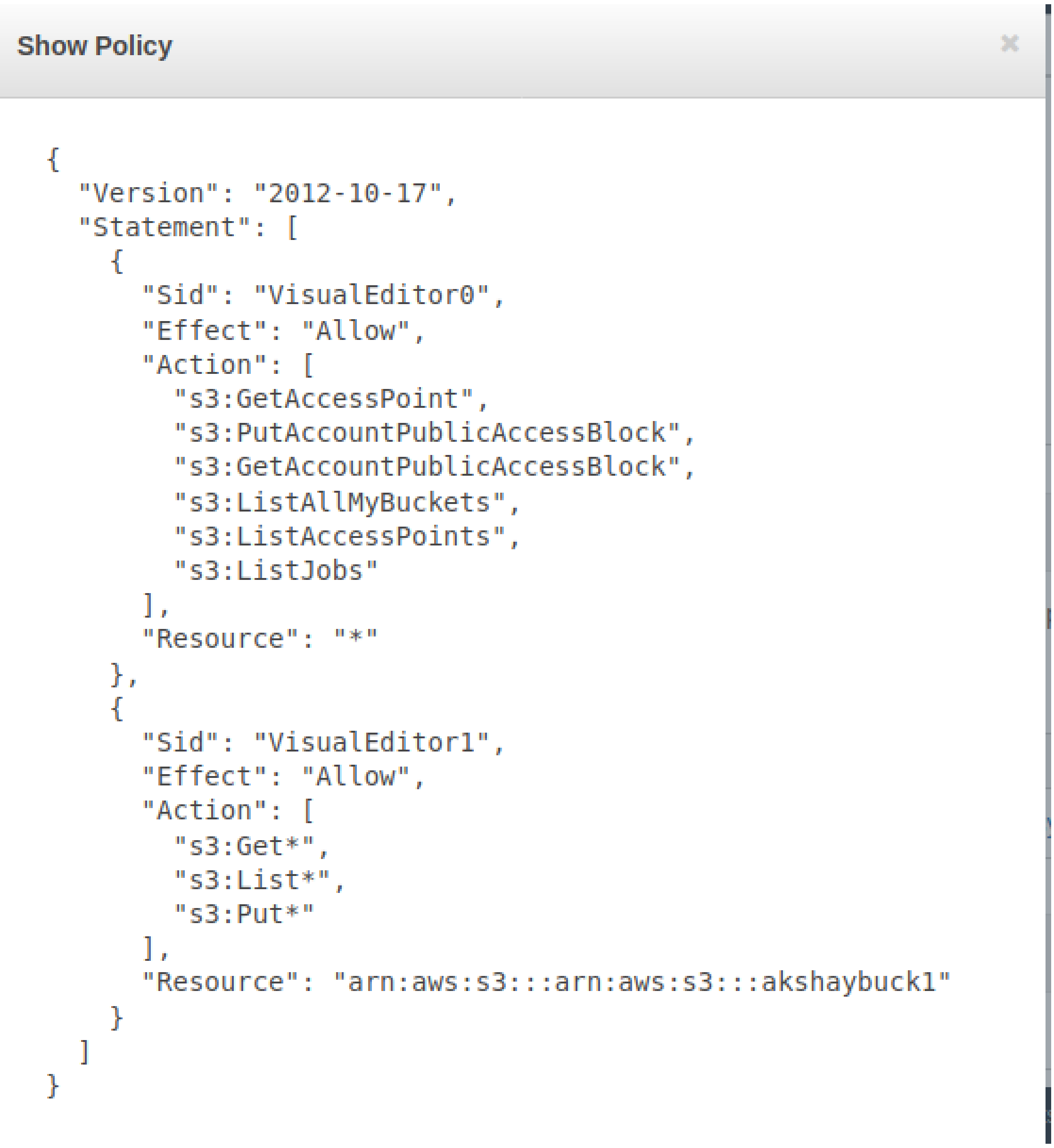
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ Jay

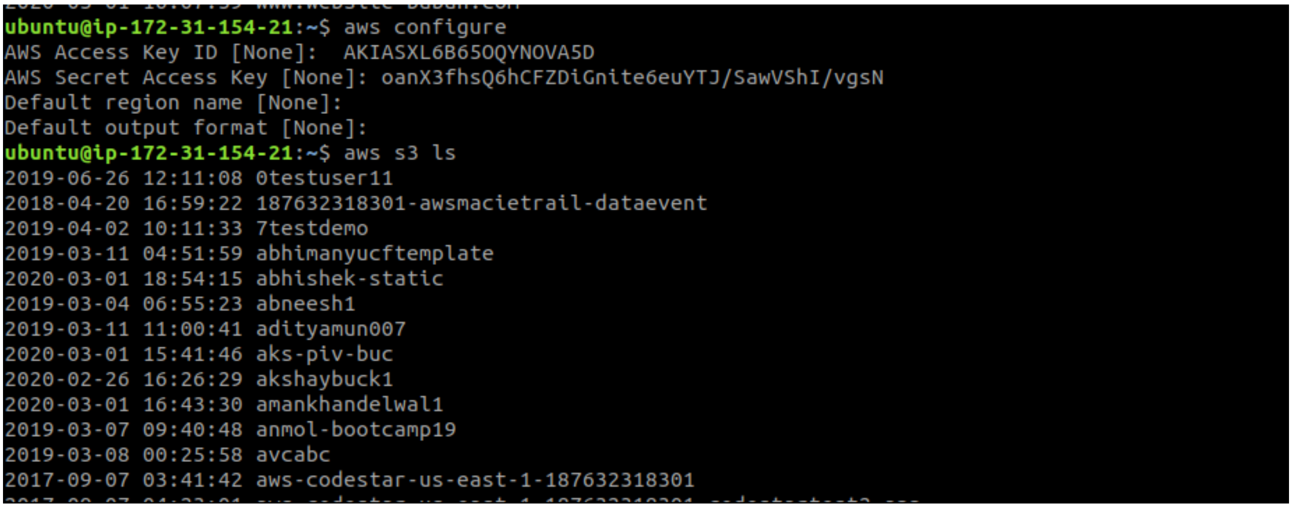
Showing 2 results

	Policy Name ⬍	Attached Entities ⬍	Creation Time ⬍
☐	Jay-Assume-Role	1	2020-03-02 14:48 UTC...
☑	Jay-DBadmin-policy	0	2020-03-02 16:12 UTC...



Show Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetAccessPoint",
        "s3:PutAccountPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:ListAccessPoints",
        "s3:ListJobs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Resource": "arn:aws:s3:::arn:aws:s3:::akshaybuck1"
    }
  ]
}
```

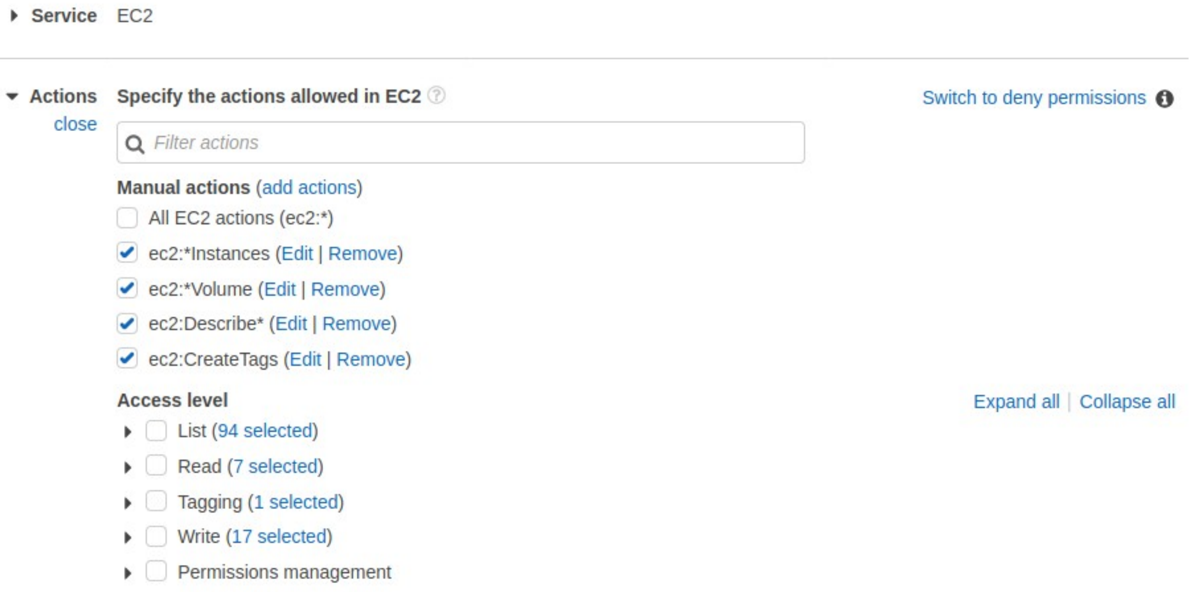


```
ubuntu@ip-172-31-154-21:~$ aws configure
AWS Access Key ID [None]:  AKIASXL6B65OQYNOVA5D
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
ubuntu@ip-172-31-154-21:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-03-01 18:54:15 abhishek-static
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-03-01 15:41:46 aks-piv-buc
2020-02-26 16:26:29 akshaybuck1
2020-03-01 16:43:30 amankhandelwal1
2019-03-07 09:40:48 anmol-bootcamp19
2019-03-08 00:25:58 avcabc
2017-09-07 03:41:42 aws-codestar-us-east-1-187632318301
```

5. Create a group for the "Developer group " where the user 'bob ' is a member of this group. This group with Test Newly Developed Features for which they require access to EC2 instances. Provide the following access to this group:

Service: Amazon EC2
Action: *Instances, *Volume, Describe*, CreateTags;
Condition: Dev Subnets only

Used above group and user for demonstration



Service EC2

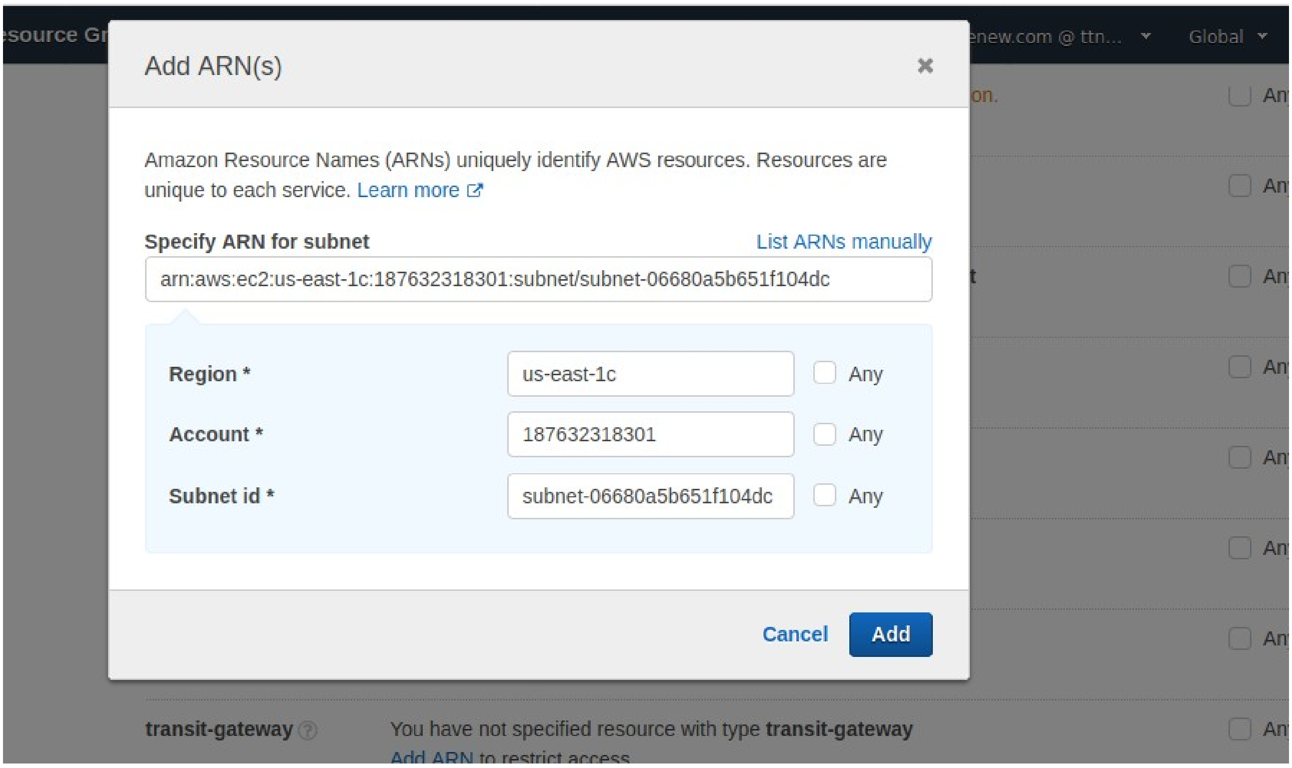
Actions Specify the actions allowed in EC2

Manual actions (add actions)

□ All EC2 actions (ec2:*)
☑ ec2:*Instances (Edit | Remove)
☑ ec2:*Volume (Edit | Remove)
☑ ec2:Describe* (Edit | Remove)
☑ ec2:CreateTags (Edit | Remove)

Access level

□ List (94 selected)
□ Read (7 selected)
□ Tagging (1 selected)
□ Write (17 selected)
□ Permissions management



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for subnet

List ARNs manually

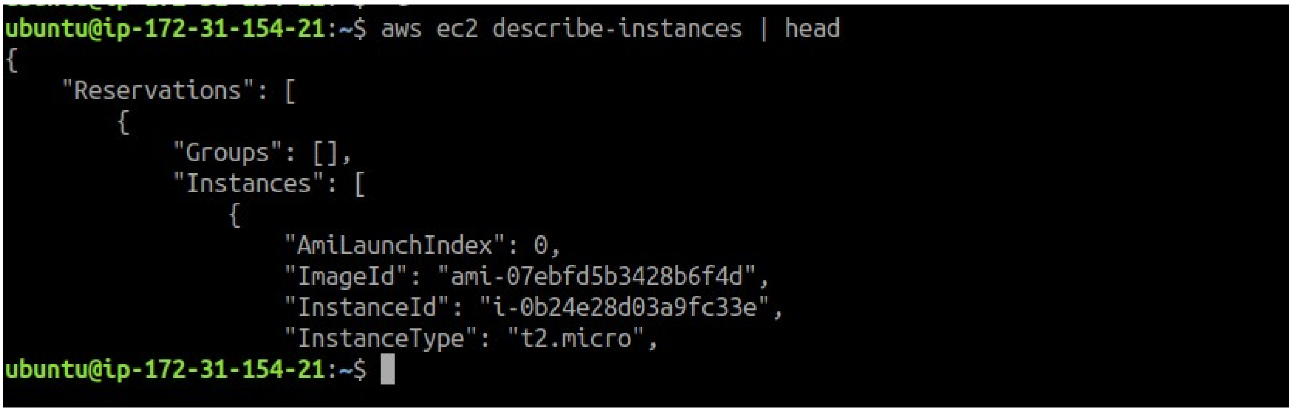
arn:aws:ec2:us-east-1c:187632318301:subnet/subnet-06680a5b651f104dc

Region *	us-east-1c	□ Any
Account *	187632318301	□ Any
Subnet id *	subnet-06680a5b651f104dc	□ Any

transit-gateway

You have not specified resource with type **transit-gateway**

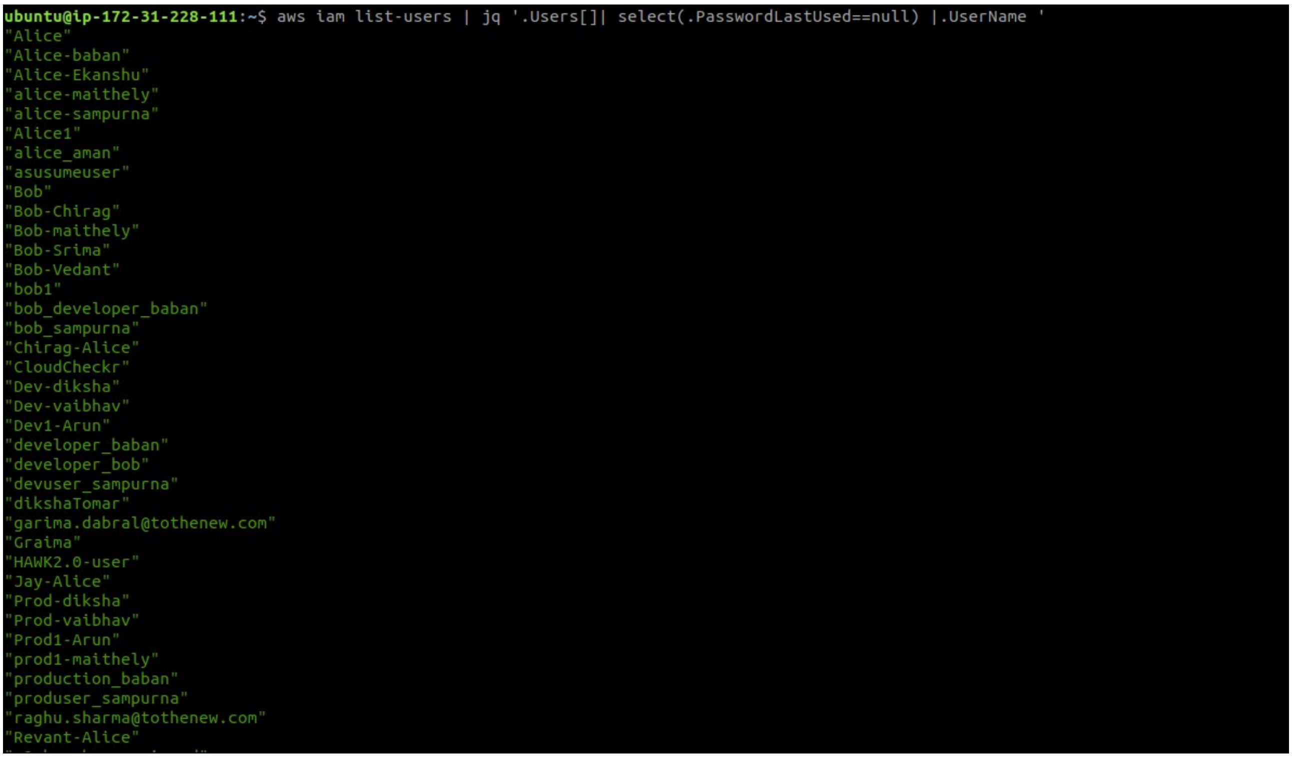
Add ARN to restrict access.



```
ubuntu@ip-172-31-154-21:~$ aws ec2 describe-instances | head
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-07ebfd5b3428b6f4d",
                    "InstanceId": "i-0b24e28d03a9fc33e",
                    "InstanceType": "t2.micro",
ubuntu@ip-172-31-154-21:~$ 
```

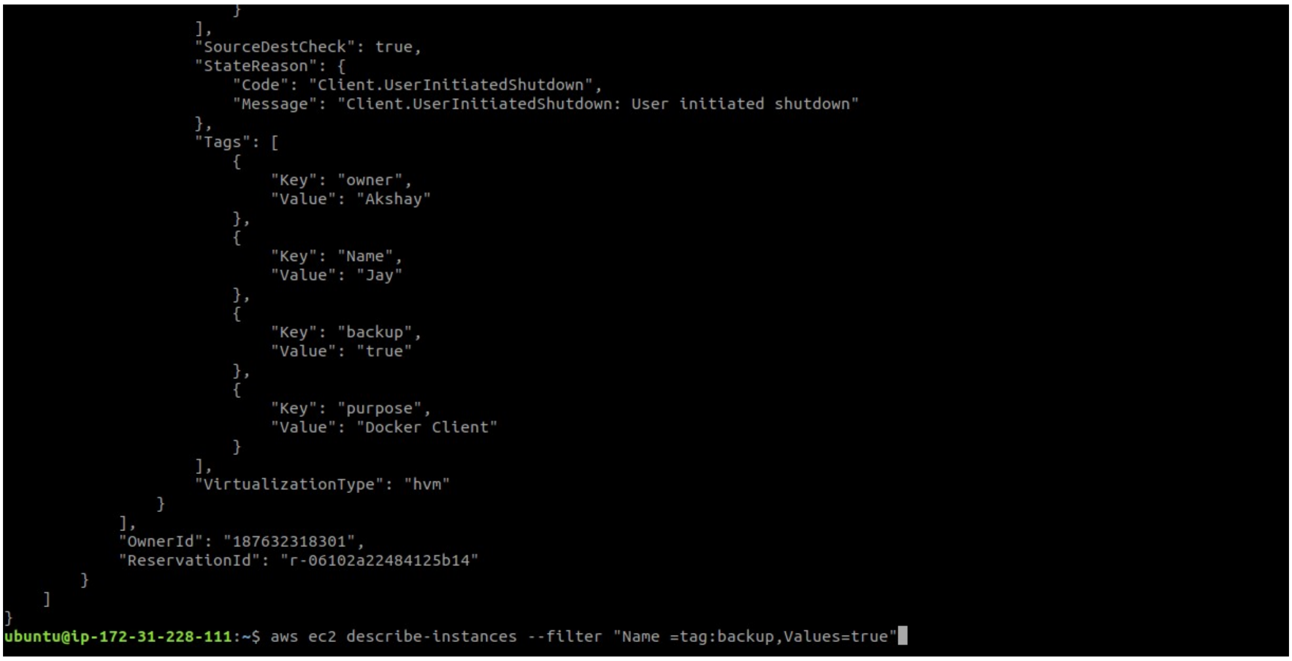
Output of # aws ec2 describe-instances.(veryfying)

6. Identify the unused IAM users/credentials using AWS CLI.



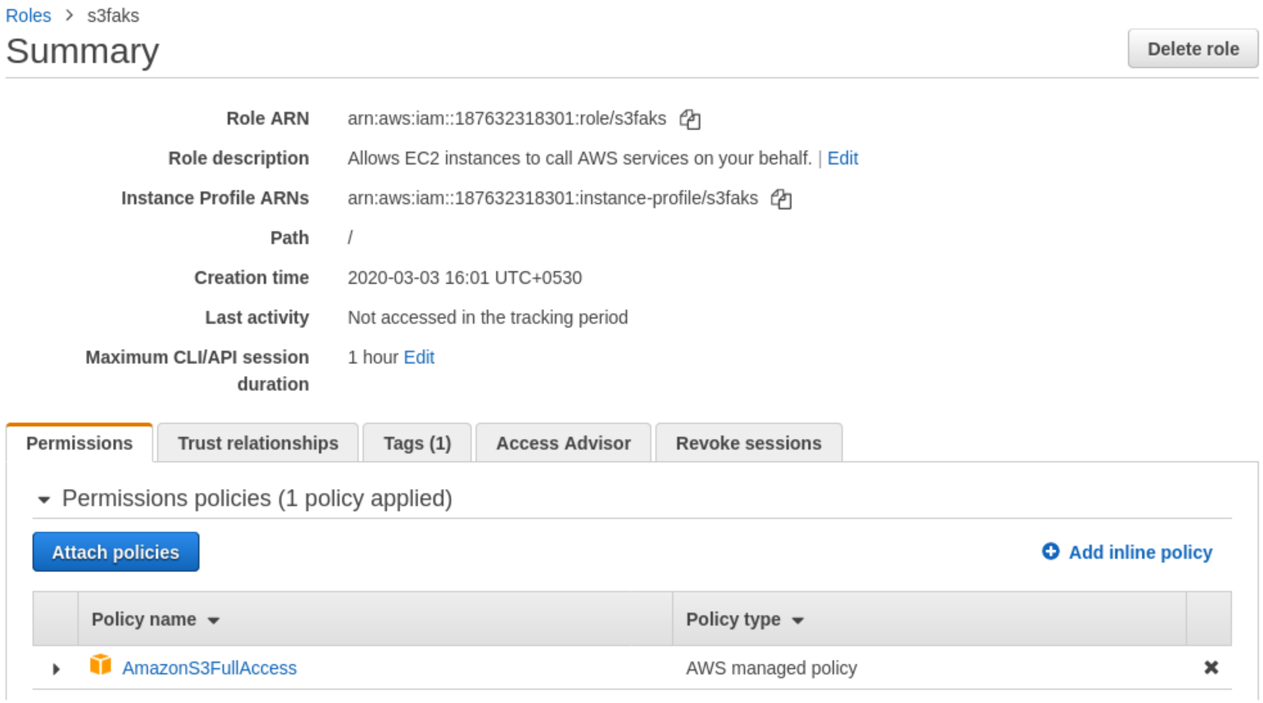
```
ubuntu@ip-172-31-228-111:~$ aws iam list-users | jq '.Users[]| select(.PasswordLastUsed==null) |.UserName '
"Alice"
"Alice-baban"
"Alice-Ekanshu"
"alice-maithely"
"alice-sampurna"
"Alice1"
"alice_aman"
"asusumeuser"
"Bob"
"Bob-Chirag"
"Bob-maithely"
"Bob-Srima"
"Bob-Vedant"
"bob1"
"bob_developer_baban"
"bob_sampurna"
"Chirag-Alice"
"CloudCheckr"
"Dev-diksha"
"Dev-vaibhav"
"Dev1-Arun"
"developer_baban"
"developer_bob"
"devuser_sampurna"
"dikshaTomar"
"garima.dabral@tothenew.com"
"Graima"
"HAWK2.0-user"
"Jay-Alice"
"Prod-diksha"
"Prod-vaibhav"
"Prod1-Arun"
"prod1-maithely"
"production_baban"
"produser_sampurna"
"raghu.sharma@tothenew.com"
"Revant-Alice"
```

7. Identify all the instances having the tag key-value "backup=true" using AWS CLI.



```
                    }
                ],
                "SourceDestCheck": true,
                "StateReason": {
                    "Code": "Client.UserInitiatedShutdown",
                    "Message": "Client.UserInitiatedShutdown: User initiated shutdown"
                },
                "Tags": [
                    {
                        "Key": "owner",
                        "Value": "Akshay"
                    },
                    {
                        "Key": "Name",
                        "Value": "Jay"
                    },
                    {
                        "Key": "backup",
                        "Value": "true"
                    },
                    {
                        "Key": "purpose",
                        "Value": "Docker Client"
                    }
                ],
                "VirtualizationType": "hvm"
            }
        ],
        "OwnerId": "187632318301",
        "ReservationId": "r-06102a22484125b14"
    }
    ]
}
ubuntu@ip-172-31-228-111:~$ aws ec2 describe-instances --filter "Name =tag:backup,Values=true"
```

8.An EC2 Instance hosts a Java-based application that accesses an s3 bucket. This EC2 Instance is currently serving production users. Create the role and assign the role to EC2 instance.



Roles > s3faks

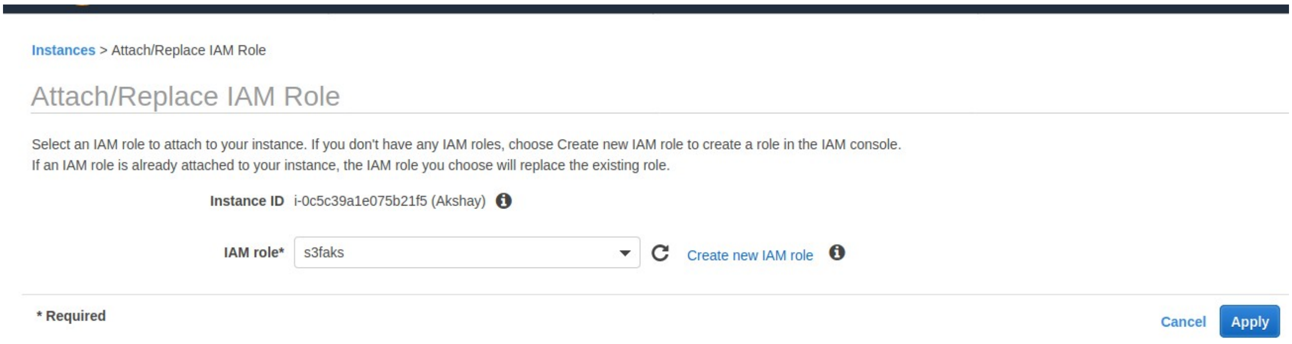
Summary

Delete role

Role ARN	arn:aws:iam::187632318301:role/s3faks
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/s3faks
Path	/
Creation time	2020-03-03 16:01 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions policies (1 policy applied)

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy



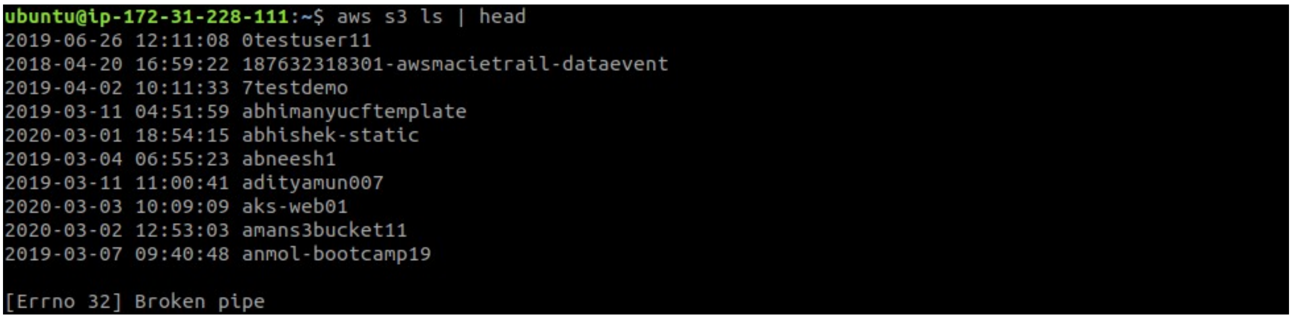
Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console.
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-0c5c39a1e075b21f5 (Akshay)

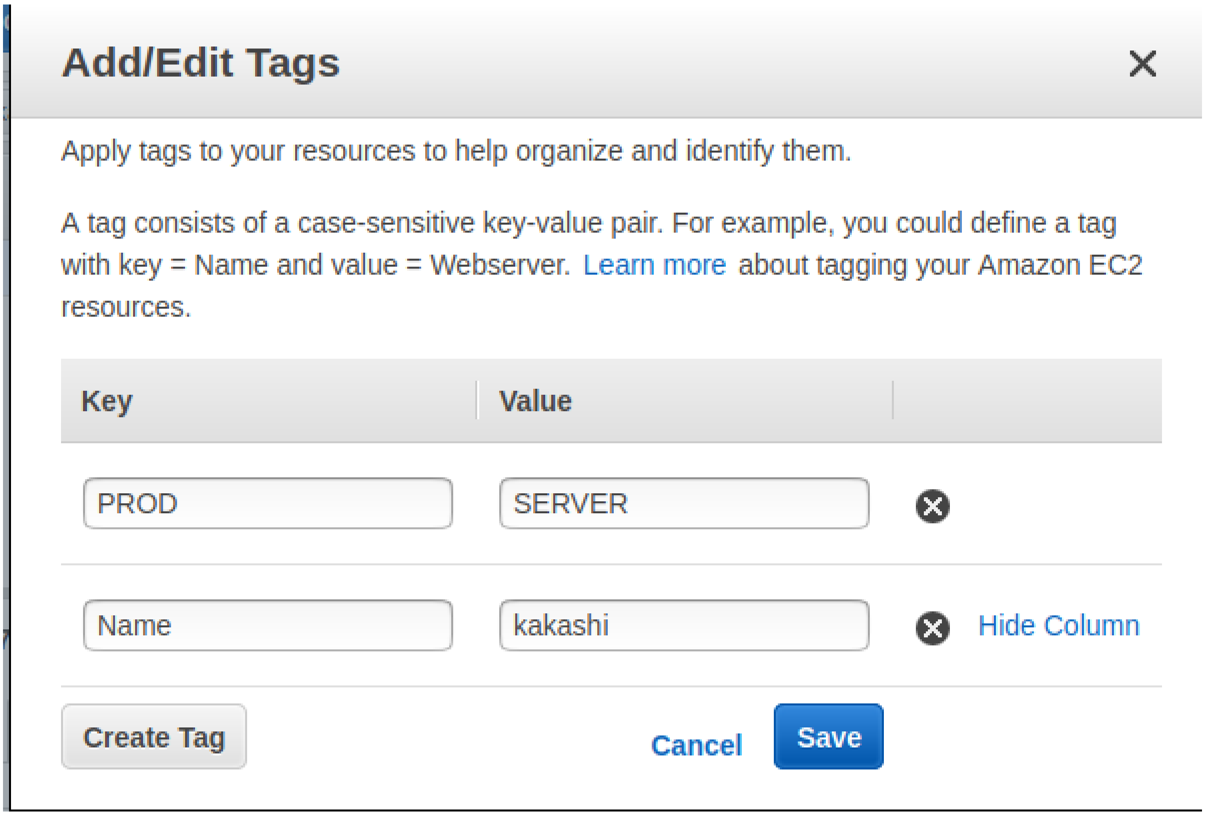
IAM role* s3faks



```
ubuntu@ip-172-31-228-111:~$ aws s3 ls | head
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-03-01 18:54:15 abhishek-static
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-03-03 10:09:09 aks-web01
2020-03-02 12:53:03 amans3bucket11
2019-03-07 09:40:48 anmol-bootcamp19

[Errno 32] Broken pipe
```

9.You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Define the tags on the test and production servers and add a condition to the IAMPolicy which allows access to specific tags.

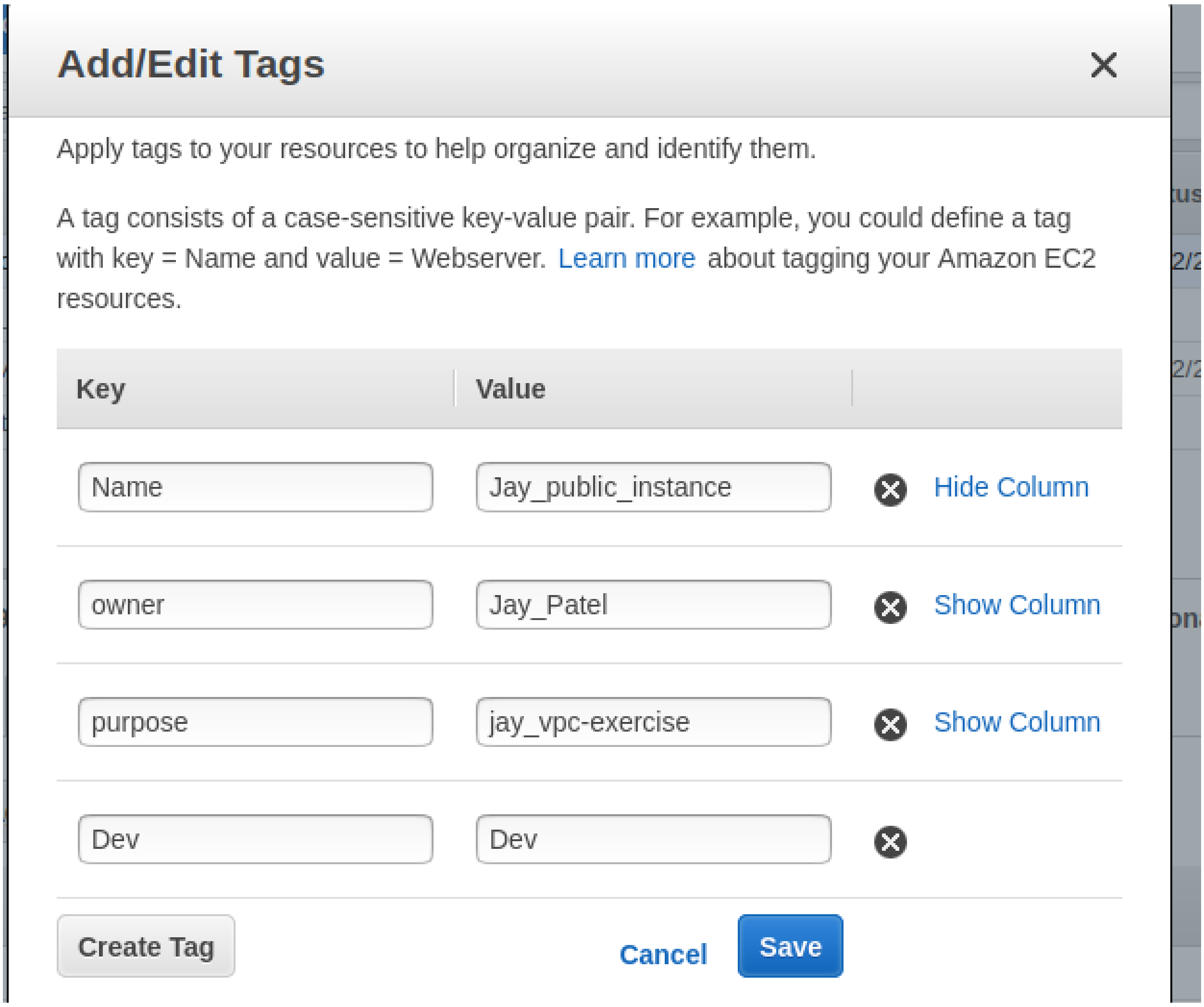


Add/Edit Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key	Value
PROD	SERVER
Name	kakashi

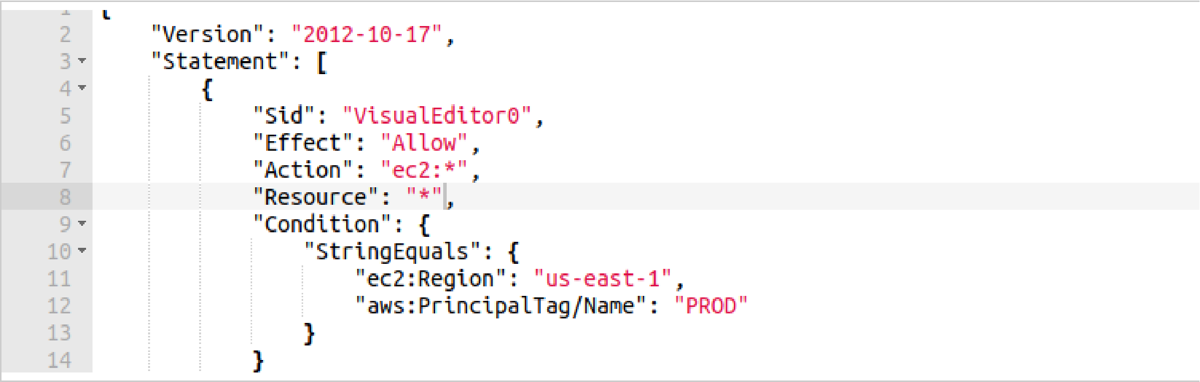


Add/Edit Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

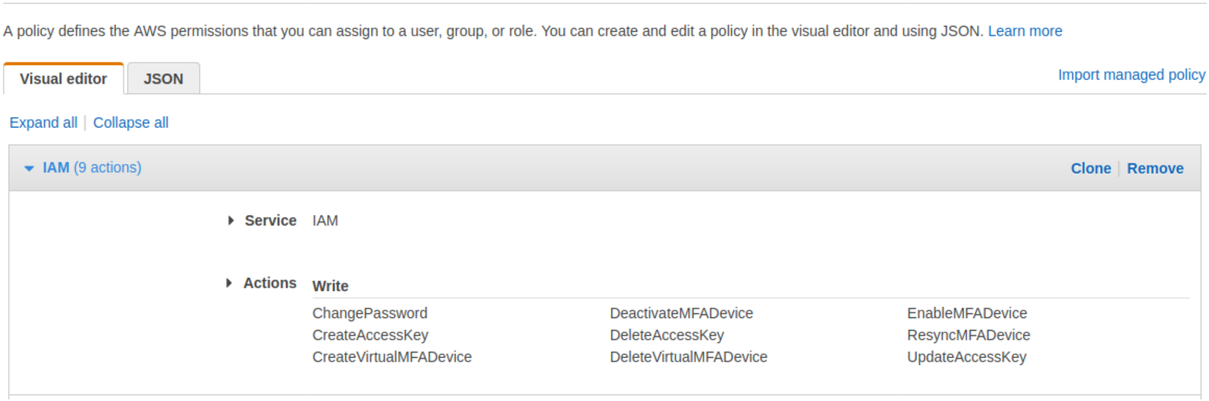
Key	Value	
Name	Jay_public_instance	⊗ Hide Column
owner	Jay_Patel	⊗ Show Column
purpose	jay_vpc-exercise	⊗ Show Column
Dev	Dev	⊗



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1",
                    "aws:PrincipalTag/Name": "PROD"
                }
            }
```

policy with only PROD tag can access.

10.Create a policy for allowing users to set or rotate their credentials, such as their console password, their programmatic access keys, and their MFA devices.

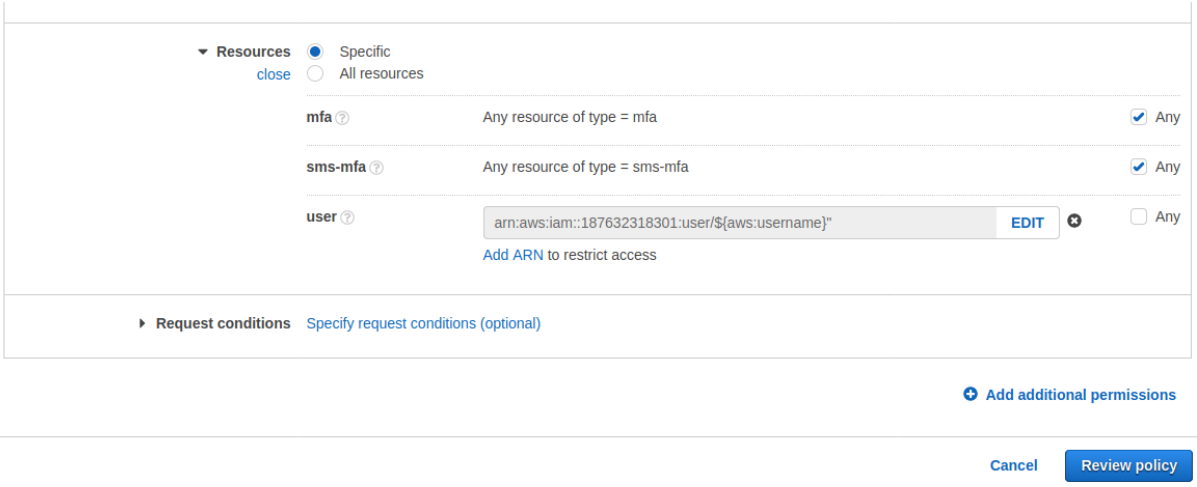


A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Service: IAM

Actions: Write

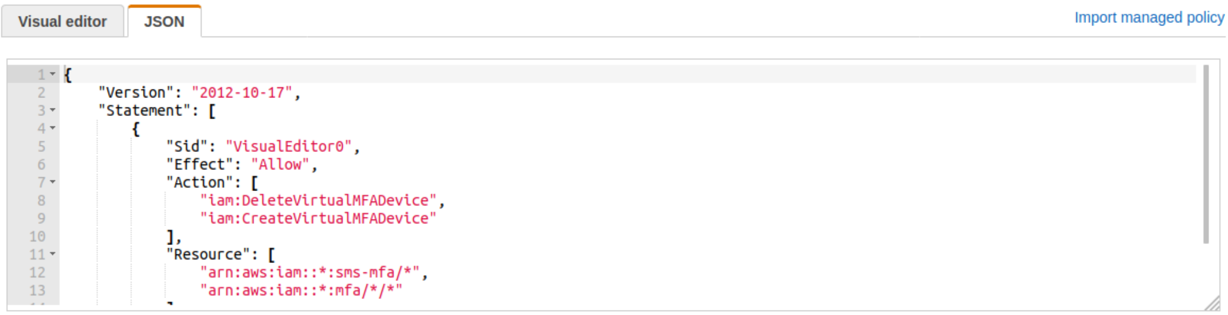
ChangePassword	DeactivateMFADevice	EnableMFADevice
CreateAccessKey	DeleteAccessKey	ResyncMFADevice
CreateVirtualMFADevice	DeleteVirtualMFADevice	UpdateAccessKey



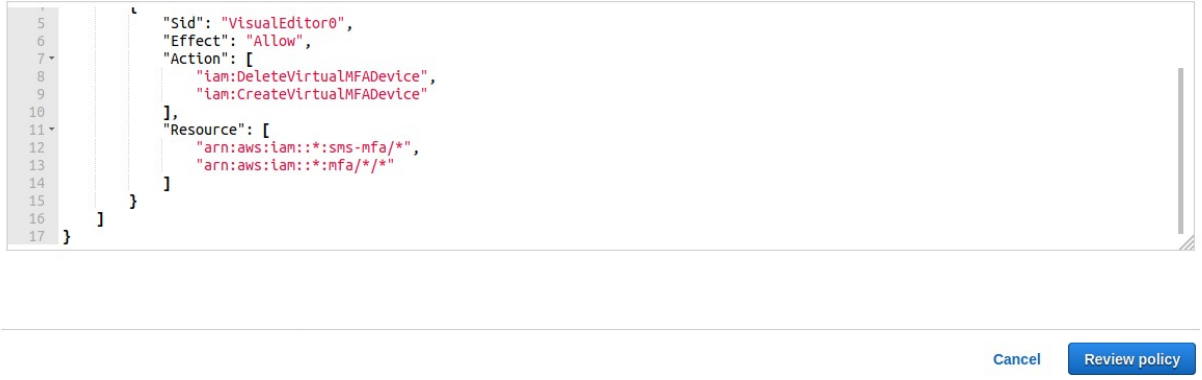
Resources: ● Specific ○ All resources

mfa	Any resource of type = mfa	☑ Any
sms-mfa	Any resource of type = sms-mfa	☑ Any
user	arn:aws:iam::187632318301:user/${aws:username}" EDIT Add ARN to restrict access	□ Any

Request conditions: Specify request conditions (optional)



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteVirtualMFADevice",
                "iam:CreateVirtualMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:sms-mfa/*",
                "arn:aws:iam::*:mfa/*/*"
```



```
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteVirtualMFADevice",
                "iam:CreateVirtualMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:sms-mfa/*",
                "arn:aws:iam::*:mfa/*/*"
            ]
        }
    ]
}
```