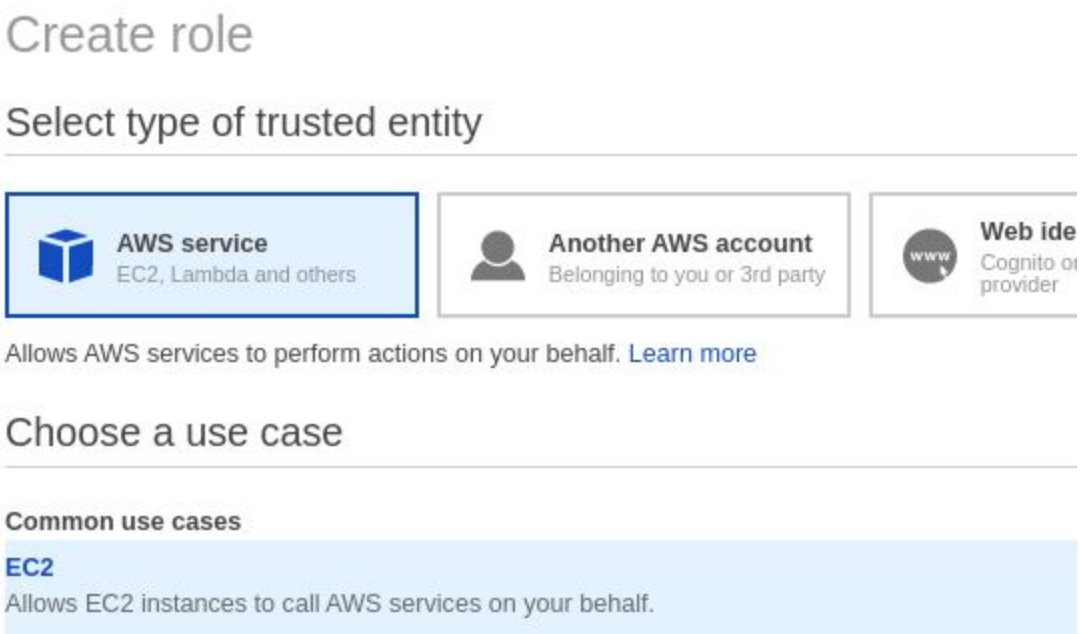
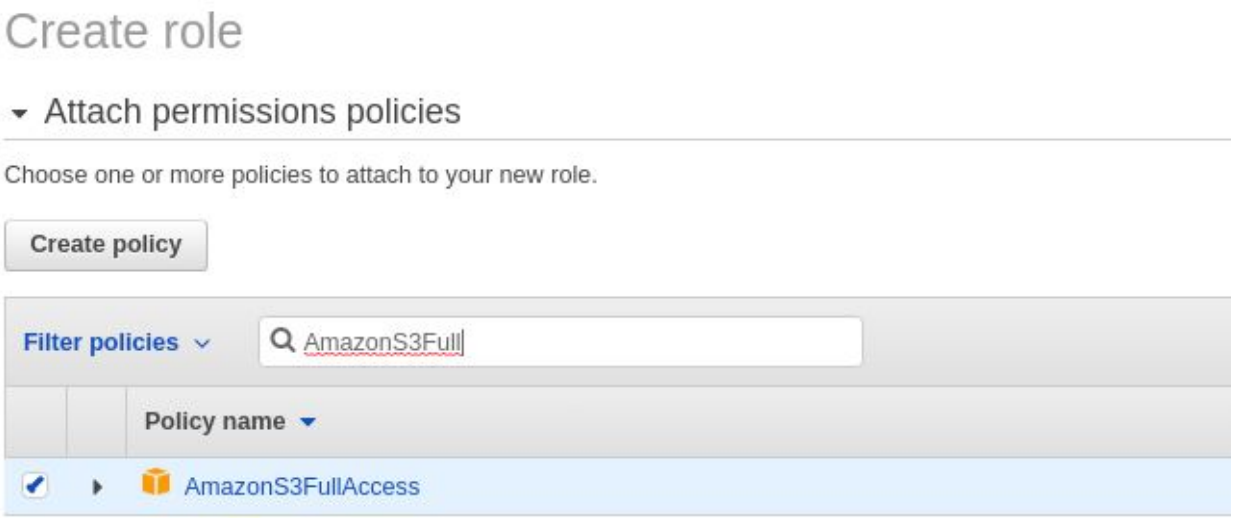
ASSESSMENT - 13

IAM

TO THE NEW™

1. Create a Role with full access to S3





Create role

1 2

Review

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

Role name* Role1-for-s3FullAccess

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 AmazonS3FullAccess

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

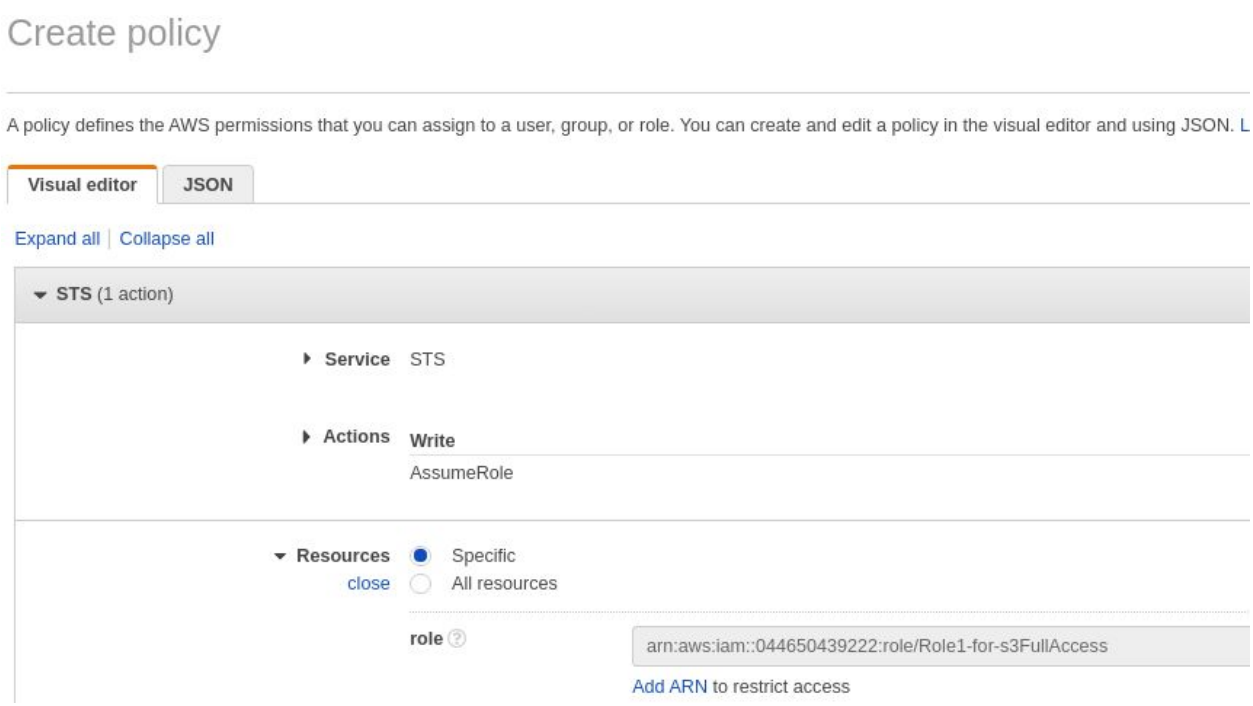
arn:aws:iam::044650439222:role/Role1-for-s3FullAccess

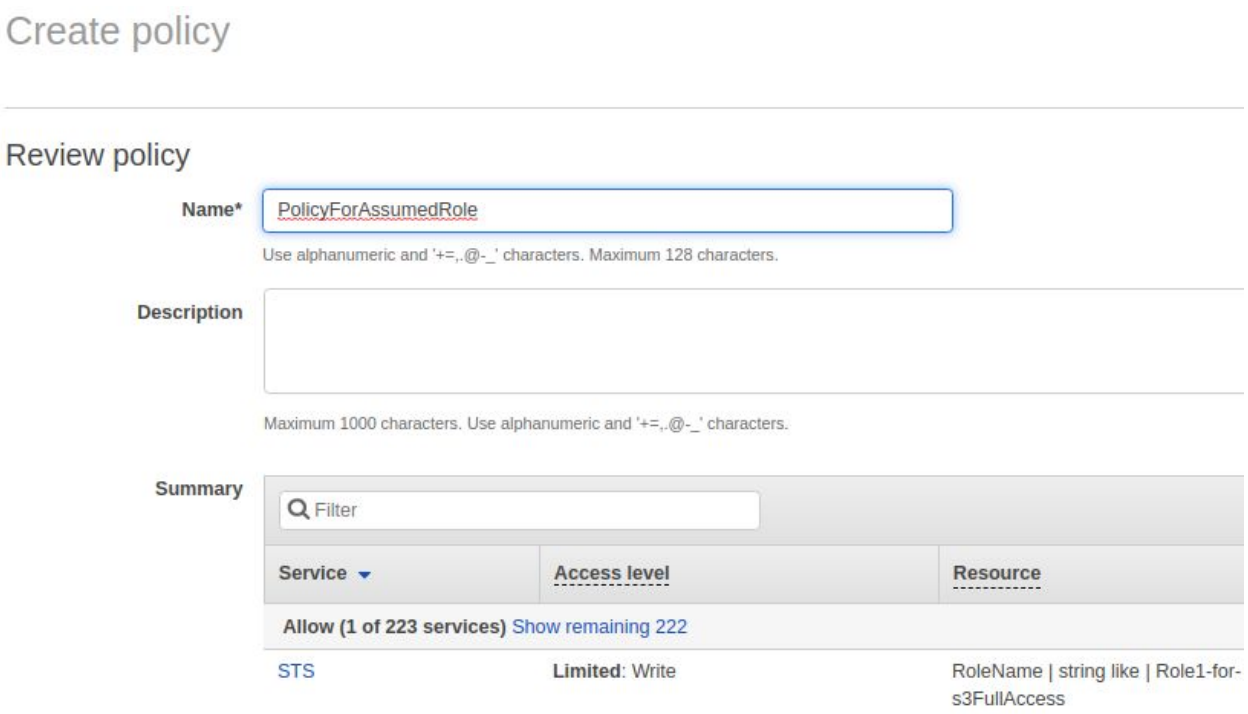
Account * 044650439222 Any

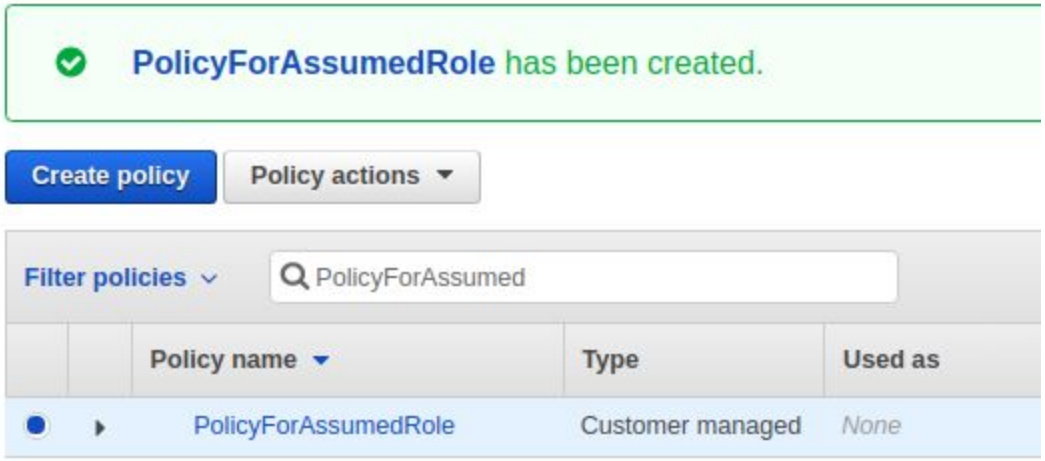
Role name with path * Role1-for-s3FullAccess Any

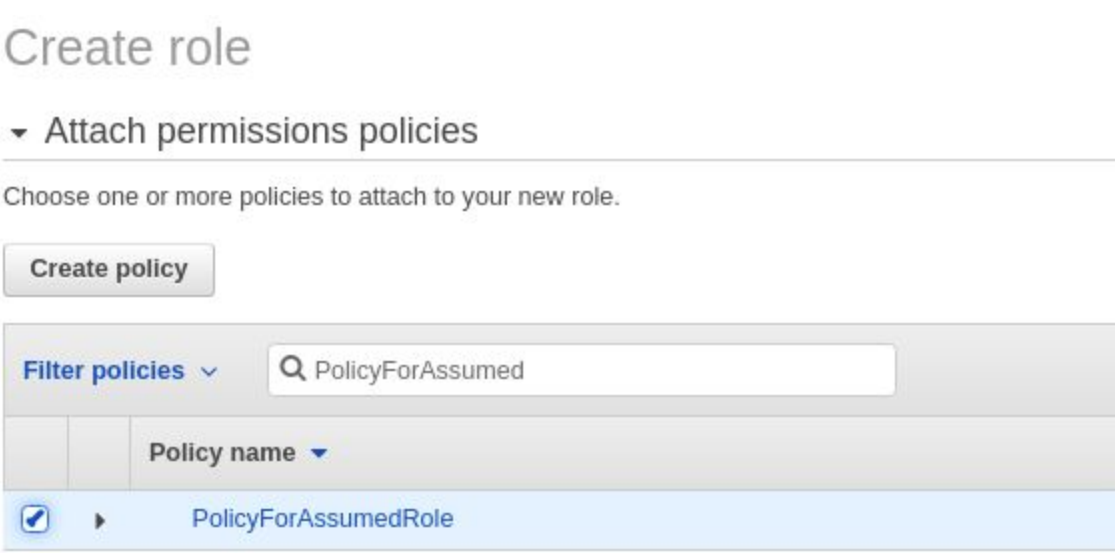
Cancel Add

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






PolicyForAssumedRole has been created.
Create policy
Policy actions
Filter policies
PolicyForAssumed
Policy name
Type
Used as
PolicyForAssumedRole
Customer managed
None


Create role
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
PolicyForAssumed
Policy name
PolicyForAssumedRole

Create role

1 2

Review

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

Role name* Role2-for-assumed-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 PolicyForAssumedRole

Create role | Delete role

Role

	Role name	Trusted entities
☐	AWSServiceRoleForAutoScaling	**AWS service:** autoscaling (
☐	AWSServiceRoleForElasticLoadBalancing	**AWS service:** elasticloadba
☐	AWSServiceRoleForSupport	**AWS service:** support (Serv
☐	AWSServiceRoleForTrustedAdvisor	**AWS service:** trustedadvisc
☐	example-role	**Account:** 044650439222
☑	Role1-for-s3FullAccess	**AWS service:** ec2
☑	Role2-for-assumed-role	**AWS service:** ec2

Roles > Role1-for-s3FullAccess

Summary

Role ARN	arn:aws:iam::044650439222:role/Role1-for-s3FullAccess
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::044650439222:instance-profile/Role1-for-s3FullAccess
Path	/
Creation time	2020-03-02 22:18 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions | **Trust relationships** | **Tags (1)** | **Access Advisor** | **Revoke sessions**

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy docume

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The identity provider(s) ec2.amazonaws.com

Conditions

The following conditions de

There are no conditions ass

Edit Trust Relationship

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

Policy Document

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": {
7          "AWS": "arn:aws:iam::044650439222:role/Role2-for-assumed-role",
8          "Service": "ec2.amazonaws.com",
9        },
10       "Action": "sts:AssumeRole"
11     }
12   ]
13 }
```

Roles > Role1-for-s3FullAccess

Summary

Role ARN	arn:aws:iam::044650439222:role/F
Role description	Allows EC2 instances to call AWS
Instance Profile ARNs	arn:aws:iam::044650439222:instar
Path	/
Creation time	2020-03-02 22:18 UTC+0530
Last activity	Not accessed in the tracking perio
Maximum CLI/API session duration	1 hour Edit

Permissions | **Trust relationships** | **Tags (1)** | **Access Advisor**

You can view the trusted entities that can assume the role and the access condit

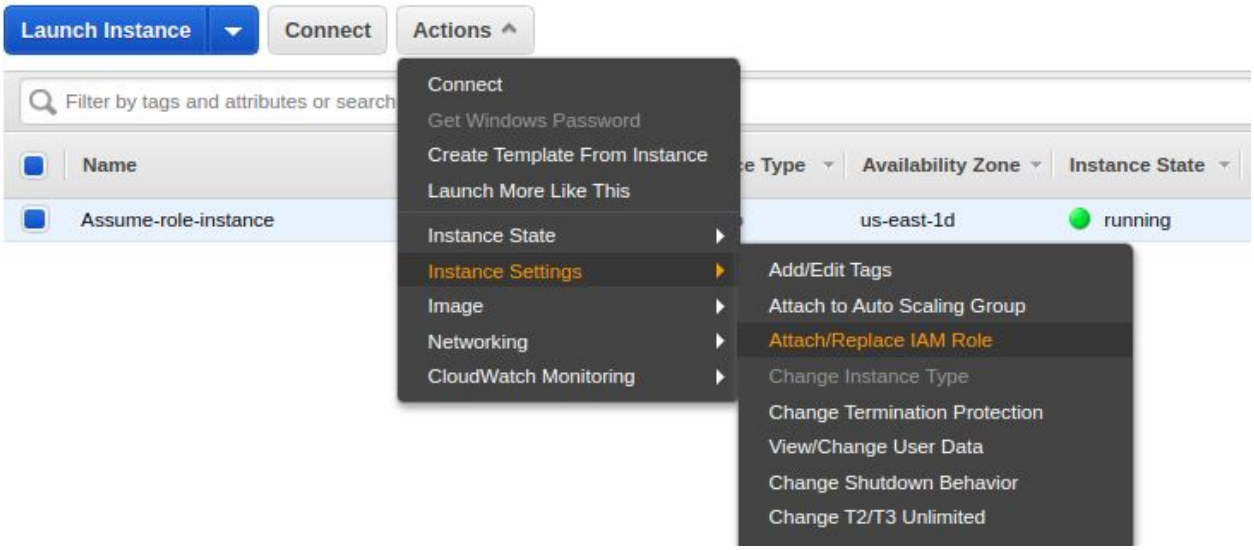
Edit trust relationship

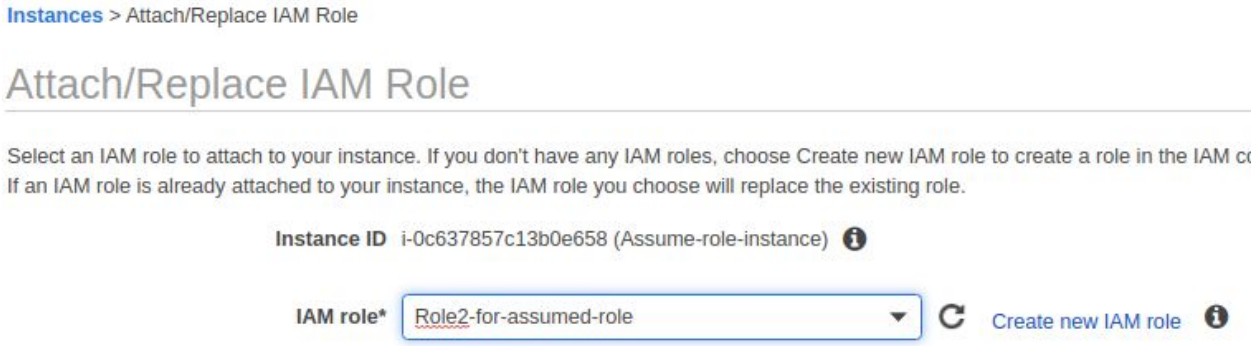
Trusted entities

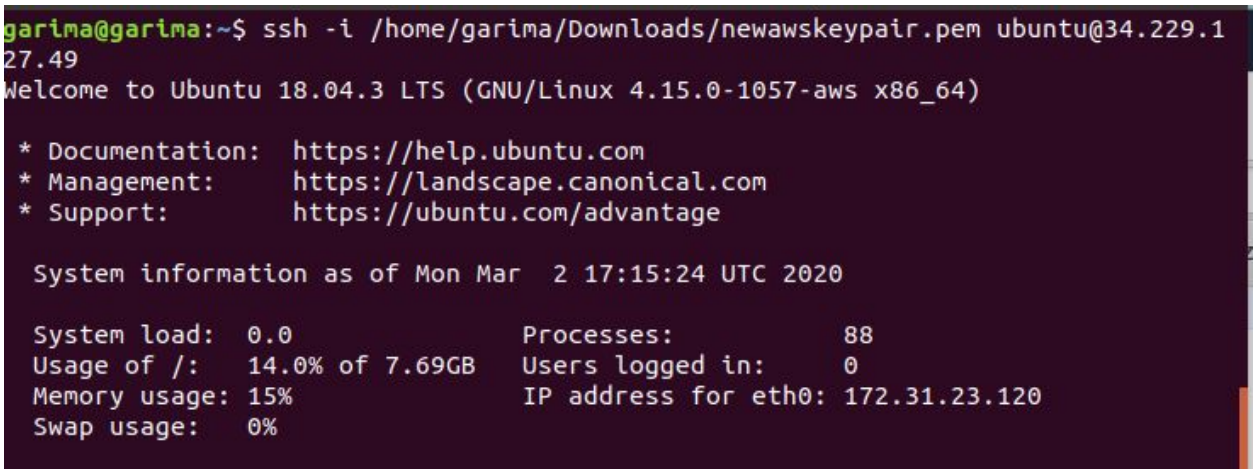
The following trusted entities can assume this role.

Trusted entities
The identity provider(s) ec2.amazonaws.com
arn:aws:iam::044650439222:role/Role1-for-s3FullAccess

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







```
ubuntu@ip-172-31-23-120:~$ aws sts get-caller-identity
{
    "UserId": "AROAQUZK7UI3NK3C6UGPV:i-0c637857c13b0e658",
    "Account": "044650439222",
    "Arn": "arn:aws:sts::044650439222:assumed-role/Role2-for-assumed-role/i-0c63
7857c13b0e658"
}
ubuntu@ip-172-31-23-120:~$
```

```
ubuntu@ip-172-31-23-120:~$ aws sts assume-role --role-arn arn:aws:iam::044650439
222:role/Role1-for-s3FullAccess --role-session-name garima
{
    "Credentials": {
        "SessionToken": "FwoGZXIvYXdzEGsaDACaKRV1uijfoOWtQyKqAaaxdD4qPBpzB6U4lyv
WgumyFJhPphlzHn6+WCGaFQyLsKsV1h6Z80kB8LyP/fgOgD5TDB4bftVxwQDsfpt5iPmS6Z/u4PQkJNS
BMKOYX55ZO0LTdRjZUqbwnql+AyUw+ERng708cBSUb0pfgvlAFykbiQqjBJdiu/DFe5JcOvkOjvEHemV
Xk1BoISAekaGl6YaHA/X8HEOUOVaKGSO6UecM/pNfSFx9vhxJKOqL9fIFMi1hWIY/5ATMKOAYZkKZsJv
7Hu4lpqTebfMU/l+Z7IoBvjxZMDE6gVfutB4Fqm0=",
        "AccessKeyId": "ASIAQUZK7UI3JQTGEJNY",
        "SecretAccessKey": "4HDDPotEU4XS2DseTmV8R6EpK9uvQzcEd0Ub72lk",
        "Expiration": "2020-03-02T18:44:10Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAQUZK7UI3HFOXNYD66:garima",
        "Arn": "arn:aws:sts::044650439222:assumed-role/Role1-for-s3FullAccess/ga
rima"
    }
}
```

```
ubuntu@ip-172-31-23-120:~$ export AWS_ACCESS_KEY_ID=ASIAQUZK7UI3JQTGEJNY
ubuntu@ip-172-31-23-120:~$ export AWS_SECRET_ACCESS_KEY=4HDDPotEU4XS2DseTmV8R6Ep
K9uvQzcEd0Ub72lk
ubuntu@ip-172-31-23-120:~$ export AWS_SESSION_TOKEN=FwoGZXIvYXdzEGsaDACaKRV1uijf
oOWtQyKqAaaxdD4qPBpzB6U4lyvWgumyFJhPphlzHn6+WCGaFQyLsKsV1h6Z80kB8LyP/fgOgD5TDB4b
ftVxwQDsfpt5iPmS6Z/u4PQkJNSBMKOYX55ZO0LTdRjZUqbwnql+AyUw+ERng708cBSUb0pfgvlAFykb
iQqjBJdiu/DFe5JcOvkOjvEHemVXk1BoISAekaGl6YaHA/X8HEOUOVaKGSO6UecM/pNfSFx9vhxJKOqL
9fIFMi1hWIY/5ATMKOAYZkKZsJv7Hu4lpqTebfMU/l+Z7IoBvjxZMDE6gVfutB4Fqm0=
ubuntu@ip-172-31-23-120:~$
```

```
ubuntu@ip-172-31-23-120:~$ aws s3 ls
2019-05-08 15:48:33 garima-essence
2020-02-26 18:14:51 garima-site
2020-03-02 07:16:16 non-public-bucket-garima
ubuntu@ip-172-31-23-120:~$
```

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)

Create policy

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 u

Visual editor | **JSON**

Expand all | Collapse all

S3 (75 actions) 4 warnings

Service S3

Actions

List

HeadBucket
ListAllMyBuckets
ListBucket

Read

DescribeJob	GetBucketPolicyStatus
GetAccelerateConfiguration	GetBucketPublicAccessBlock
GetAccessPoint	GetBucketRequestPayment
GetAccessPointPolicy	GetBucketTagging
GetAccessPointPolicyStatus	GetBucketVersioning
GetAccountPublicAccessBlock	GetBucketWebsite
GetAnalyticsConfiguration	GetEncryptionConfiguration
GetBucketAcl	GetInventoryConfiguration
GetBucketCORS	GetLifecycleConfiguration

Add ARN(s)

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

Specify ARN for bucket List ARNs manually

arn:aws:s3:::non-public-bucket-garima

Bucket name * non-public-bucket-garima Any

Cancel Add

▾ **Resources** close

- (●) Specific
- ( ) All resources

accesspoint	Any resource of type = accesspoint	[x] Any
bucket	arn:aws:s3:::non-public-bucket-garima EDIT Add ARN to restrict access	[ ] Any
job	Any resource of type = job	[x] Any
object	Any resource of type = object	[x] Any

Create policy

Review policy

Name* Data-Admin-Policy

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

Description

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

Summary

Filter

Service	Access level	Resource	Request co
Allow (1 of 223 services) Show remaining 222			
S3	**Full**: List, Read, Write	Multiple	None

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: Data-Admin

Example: Developers or ProjectAlpha
Maximum 128 characters

Attach Policy

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

Filter: Policy Type ▾ Data-

		Policy Name ⇕
☑		Data-Admin-Policy

Add user

Set user details

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

User name* Alice

Add another user

Select AWS access type

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

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

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

Console password* ○ Autogenerated password
● Custom password

•••••

Add user

Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions

Add user to group

Create group | Refresh

Search

	Group	Attached policies
☑	Data-Admin	Data-Admin-Policy

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://044650439222.signin.aws.amazon.com/console

Download .csv

		User	Email login instructions
▸	✓	Alice	Send email

Resource Groups

Alice @ 0446-5043-9222

Prevent S3 objects from being deleted for a predefined retention period with S3 Object Lock. Learn more »

S3 buckets

Search for buckets

All access types

Create bucket | Edit public access settings | Empty | Delete

3 Buckets

Bucket name	Access	Region
garima-essence	Error	US East (N. Virginia)
garima-site	Error	US East (N. Virginia)
non-public-bucket-garima	Bucket and objects not public	US East (N. Virginia)

Resource Groups

Alice @ 0446-5043-9222

EC2

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Running instances	-	Elastic IPs	-
Dedicated Hosts	-	Snapshots	-

Account

Supported

Default VP

Console ex

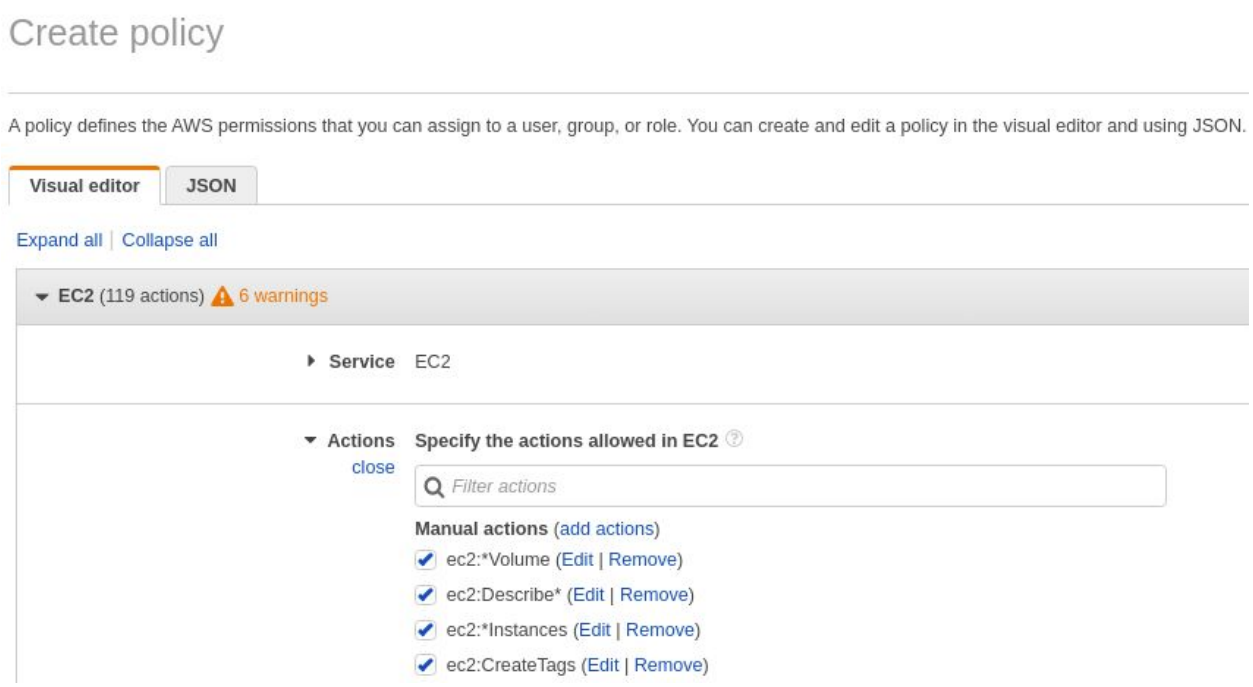
Settings

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



Add ARN(s)

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

Specify ARN for security-group List ARNs manually

arn:aws:ec2:us-east-1:044650439222:security-group/sg-044a56397d1fc7d7d

Region *	us-east-1	Any
Account *	044650439222	Any
Security group id *	sg-044a56397d1fc7d7d	Any

Cancel Add

Add ARN(s)

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

Specify ARN for vpc List ARNs manually

arn:aws:ec2:us-east-1:044650439222:vpc/vpc-7f05ba05

Region *	us-east-1	Any
Account *	044650439222	Any
Vpc id *	vpc-7f05ba05	Any

Cancel Add

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-1:044650439222:subnet/subnet-074b245b

Region *	us-east-1	Any
Account *	044650439222	Any
Subnet id *	subnet-074b245b	Any

Cancel Add

security-group	arn:aws:ec2:us-east-1:044650439222:security-group/sg-044a56397d1fc7d7d EDIT Add ARN to restrict access
snapshot	You have not specified resource with type **snapshot** Add ARN to restrict access
spot-instance-req...	You have not specified resource with type **spot-instance-request** Add ARN to restrict access
subnet	arn:aws:ec2:us-east-1:044650439222:subnet/subnet-074b245b EDIT Add ARN to restrict access
vpc	arn:aws:ec2:us-east-1:044650439222:vpc/vpc-7f05ba05 EDIT Add ARN to restrict access

Add ARN(s)

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

Specify ARN for volume List ARNs manually

arn:aws:ec2:us-east-1:044650439222:volume/vol-0c7ff4ebeb86baa9b

Region *	us-east-1	Any
Account *	044650439222	Any
Volume id *	vol-0c7ff4ebeb86baa9b	Any

Cancel Add

volume

arn:aws:ec2:us-east-1:044650439222:volume/vol-0c7ff4ebeb86baa9b EDIT

Add ARN to restrict access

Review policy

Name* Dev-only-subnet

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

Description

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

Summary

Filter

Service	Access level	Resource
Allow (1 of 223 services) Show remaining 222		
EC2	**Limited**: List, Read, Write, Tagging	Multiple

Dev-only-subnet has been created.

Create policy | Policy actions

Filter policies | Dev-only-subnet

Policy name	Type	Used as
Dev-only-subnet	Customer managed	*None*

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: garima-dev

Example: Developers or ProjectAlpha
Maximum 128 characters

Attach Policy

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

Filter: Policy Type ▾ Dev-only

		Policy Name ⇕
☑		Dev-only-subnet

IAM > Groups > **Data-Admin**

Summary

Group ARN:	arn:aws:iam::044650439222:group/Data-Admin
Users (in this group):	1
Path:	/
Creation Time:	2020-03-02 23:41 UTC+0530

Users | **Permissions** | **Access Advisor**

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
Data-Admin-Policy	Show Policy | Detach Policy | Simulate Policy

Add user

1 2 3

Set user details

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

User name* Bob

Add another user

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

1

Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job

Add user to group

Create group **Refresh**

Search

	Group	Attached policies
☐	Data-Admin	Data-Admin-Policy
☑	garima-dev	Dev-only-subnet

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

```
garima@garima:~$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "Alice",
            "UserId": "AIDAQUZK7UI3AHCVMV7VO",
            "Arn": "arn:aws:iam::044650439222:user/Alice",
            "CreateDate": "2020-03-02T18:17:25Z",
            "PasswordLastUsed": "2020-03-02T18:20:09Z"
        },
        {
            "Path": "/",
            "UserName": "garimaCC7thsem",
            "UserId": "AIDAQUZK7UI3N6OUUOJQP",
            "Arn": "arn:aws:iam::044650439222:user/garimaCC7thsem",
            "CreateDate": "2019-11-11T03:39:58Z",
            "PasswordLastUsed": "2019-11-11T03:46:58Z"
        },
        {
            "Path": "/",
            "UserName": "Juhi",
            "UserId": "AIDAQUZK7UI3PZW4JMWZ6",
            "Arn": "arn:aws:iam::044650439222:user/Juhi",
```

```
garima@garima:~$ sudo apt-get install jq
[sudo] password for garima:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installec
  libjq1 libonig4
The following NEW packages will be installed:
  jq libjq1 libonig4
0 upgraded, 3 newly installed, 0 to remove and 34 r
Need to get 276 kB of archives.
```

```
garima@garima: ~
File  Edit  View  Search  Terminal  Help
garima@garima:~$ aws iam list-users | jq '.Users[] | select(.PasswordLastUsed=nu
ll) | .UserName'
"Alice"
"garimaCC7thsem"
"Juhi"
"testuser1"
"testuser2"
garima@garima:~$
```

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

```
garima@garima:~$ aws ec2 describe-instances --filters "Name=tag:backup,Values=tr
ue"
{
    "Reservations": []
}
garima@garima:~$
```

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.

Launch Instance | Connect | Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State
my-instance	i-0c637857c13b0e658	t2.micro	us-east-1d	running

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 Open provider

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.

Create role

Attach permissions policies

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

Create policy

Filter policies Amazons3

		Policy name
☑	▸	AmazonS3FullAccess

Create role

1

Review

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

Role name* S3-Roll-For-EC2-ques8

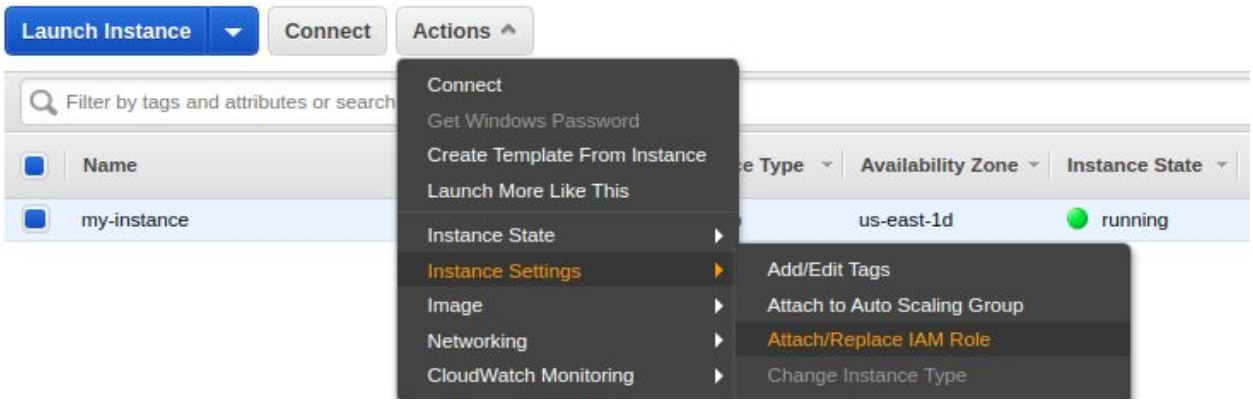
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

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 AmazonS3FullAccess



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 IA
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-0c637857c13b0e658 (my-instance)

IAM role* S3-Roll-For-EC2-ques8 Create new IAM role

```
ubuntu@ip-172-31-23-120: ~
File  Edit  View  Search  Terminal  Help
ubuntu@ip-172-31-23-120:~$ aws s3 ls
2019-05-08 15:48:33 garima-essence
2020-02-26 18:14:51 garima-site
2020-03-02 07:16:16 non-public-bucket-garima
ubuntu@ip-172-31-23-120:~$
```

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.

Launch Instance | Connect | Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State
my-instance	i-0c637857c13b0e658	t2.micro	us-east-1d	running
garima-prod	i-0e86f88a7923b8571	t2.micro	us-east-1b	running
garima-dev	i-0f92cca4e6722723c	t2.micro	us-east-1a	running

Add user

1

Set user details

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

User name* garima-dev-user

garima-prod-user

Add another user

Select AWS access type

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

Access type*

- [x] **Programmatic access**
  Enables an **access key ID** and **secret access key** for the AWS API, CLI, SI
  other development tools.
- [x] **AWS Management Console access**
  Enables a **password** that allows users to sign-in to the AWS Management C

Console password*

- ( ) Autogenerated password
- (•) Custom password

password

- [x] Show password

Add user

1

Success

You successfully created the users shown below. You can view and download user security credentials. You c
instructions for signing in to the AWS Management Console. This is the last time these credentials will be ava
you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://044650439222.signin.aws.amazon.com/

Download .csv

	User	Access key ID	Secret access key
	garima-dev-user	AKIAQUZK7UI3MNU42PFH	********* Show
	garima-prod-user	AKIAQUZK7UI3ETCVVAHB	********* Show

Create policy

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 usi

Visual editor | JSON

```
{
    "Version": "2012-10-17",
    "Statement": [ {
        "Sid": "StartStopIfTags",
        "Effect": "Allow", "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec:DescribeTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Project": "garima-dev",
                    "aws:PrincipalTag/Department": "garima-dev-user"
                    }
                }

    }    ]

}
```

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy

Visual editor | JSON

```
    "Version": "2012-10-17",
    "Statement": [ {
        "Sid": "StartStopIfTags",
        "Effect": "Allow", "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec:DescribeTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Project": "garima-prod",
                    "aws:PrincipalTag/Department": "garima-prod-user"
                    }
                }

    }    ]

}
```

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.

Create policy

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 usi

Visual editor | JSON

Expand all | Collapse all

IAM (13 actions)

Service IAM

Actions

List

ListAccessKeys
ListMFADevices
ListVirtualMFADevices

Read

GetAccessKeyLastUsed
GetAccountPasswordPolicy

Write

ChangePassword
CreateVirtualMFADevice
DeactivateMFADevice
DeleteVirtualMFADevice
EnableMFADevice
PassRole
UpdateAccountPasswordPolicy

Permissions management

DeleteAccountPasswordPolicy

Resources close

- ○ Specific
- ◉ All resources

Create policy

Review policy

Name* NewPolicy

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

Description

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

Summary

Filter

Service	Access level	Resource
Allow (1 of 223 services) Show remaining 222		
IAM	**Limited**: List, Read, Write, Permissions management	All resources