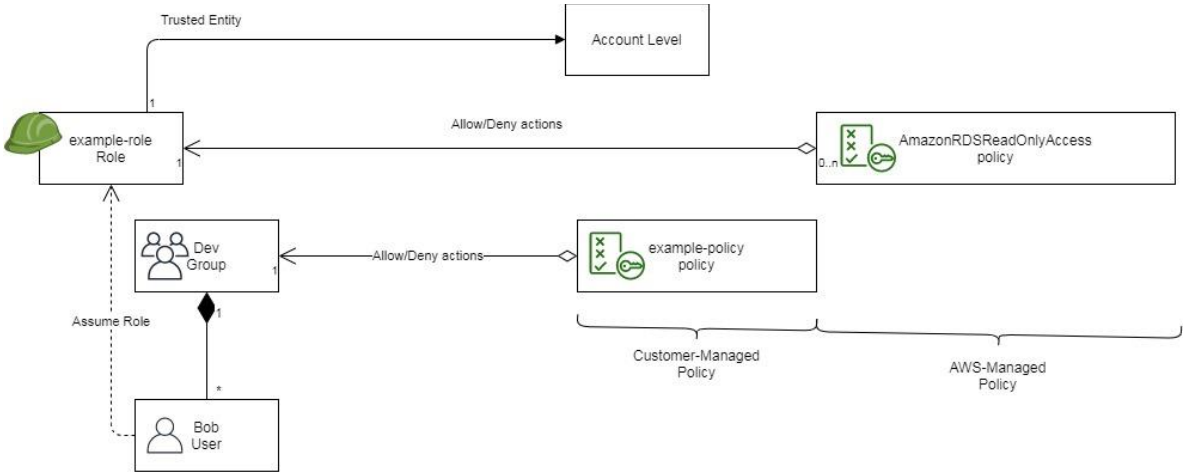
Contents

Purpose

General idea of this lab is to have a change of role to a specific user, with different assigned permissions (policies) for this reason you have a forbidden message.



Steps:

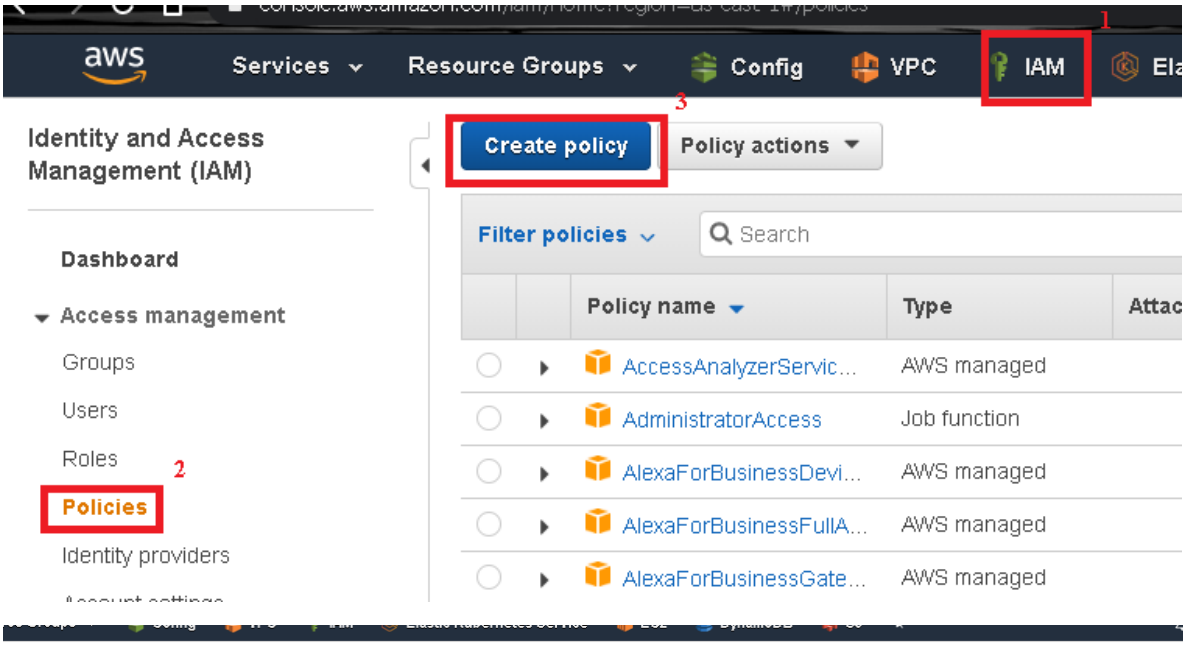
1. Create Customer-Managed Policy
2. Create a Dev group and attach it the previous policy.
3. Create a user Bob on a group.
4. Create a role and attach AWS-Managed Policy.
5. Modify the Trusted Entity of the role.
6. Test the user with group and role permissions.

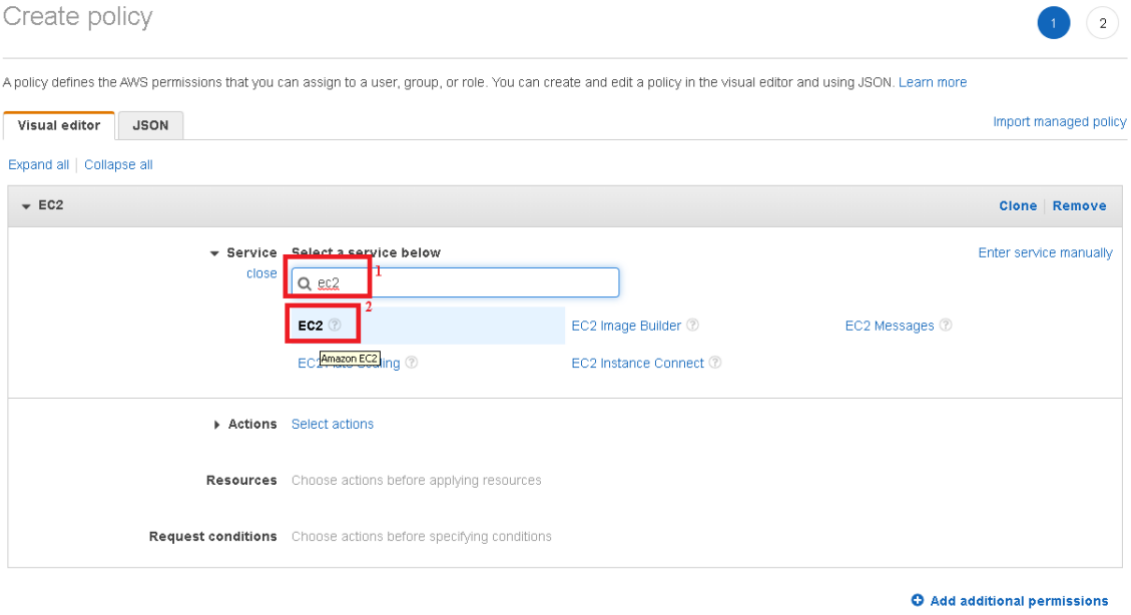
Prerequisites

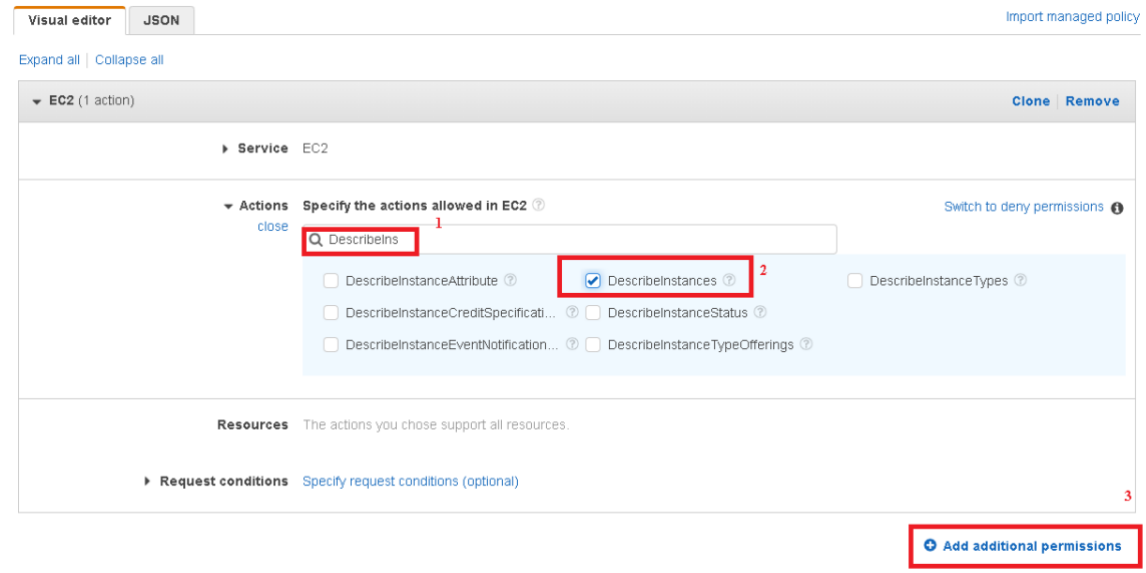
Labs1c1 have to be done and the context for Administrative user have to activated on Command Line Session.

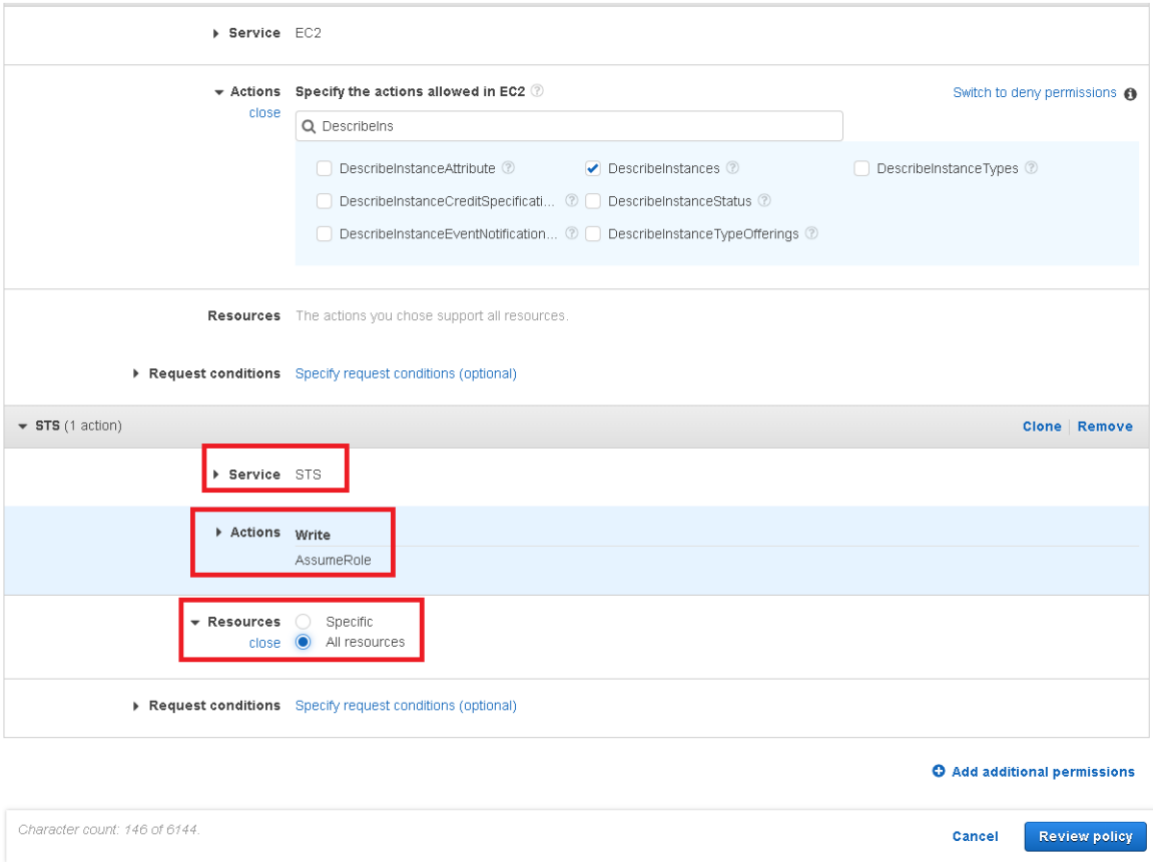
Lab 2 using Web Management Console

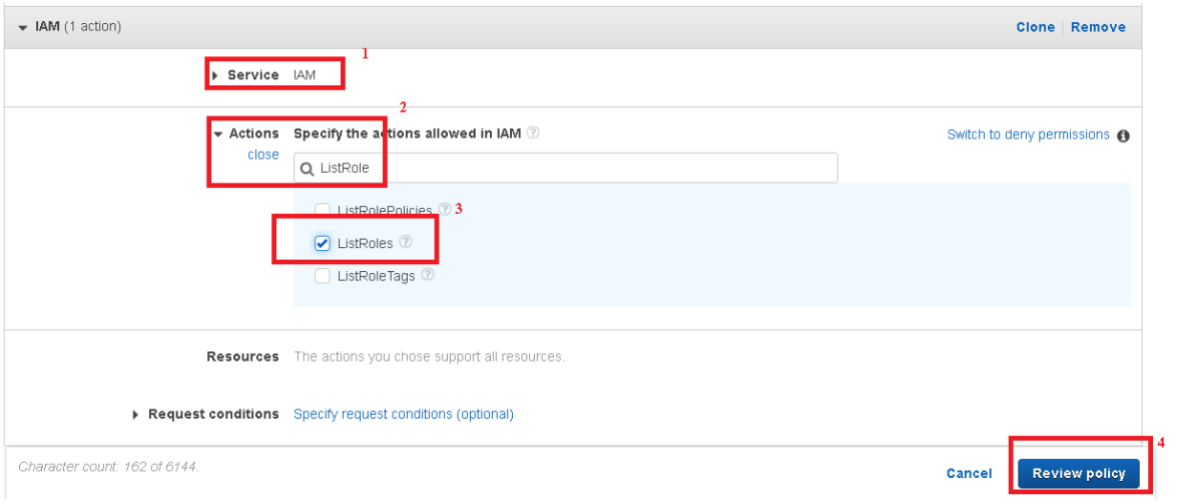
Create a policy

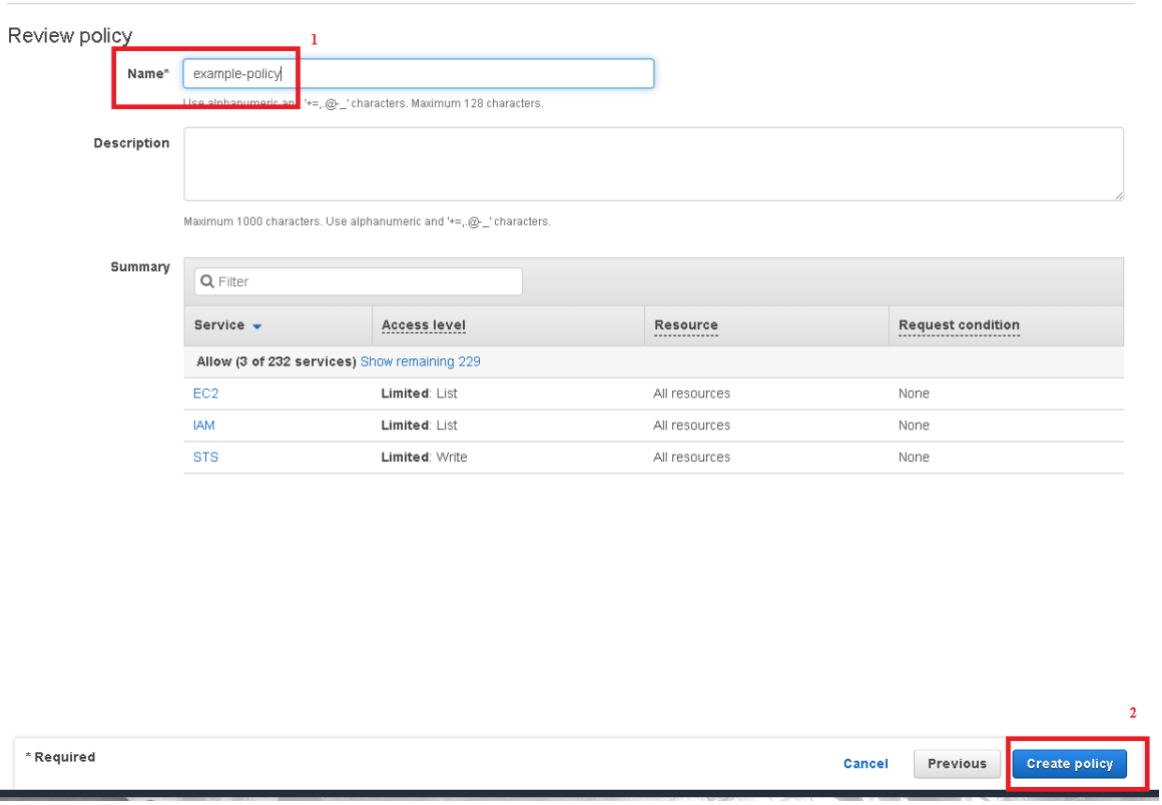




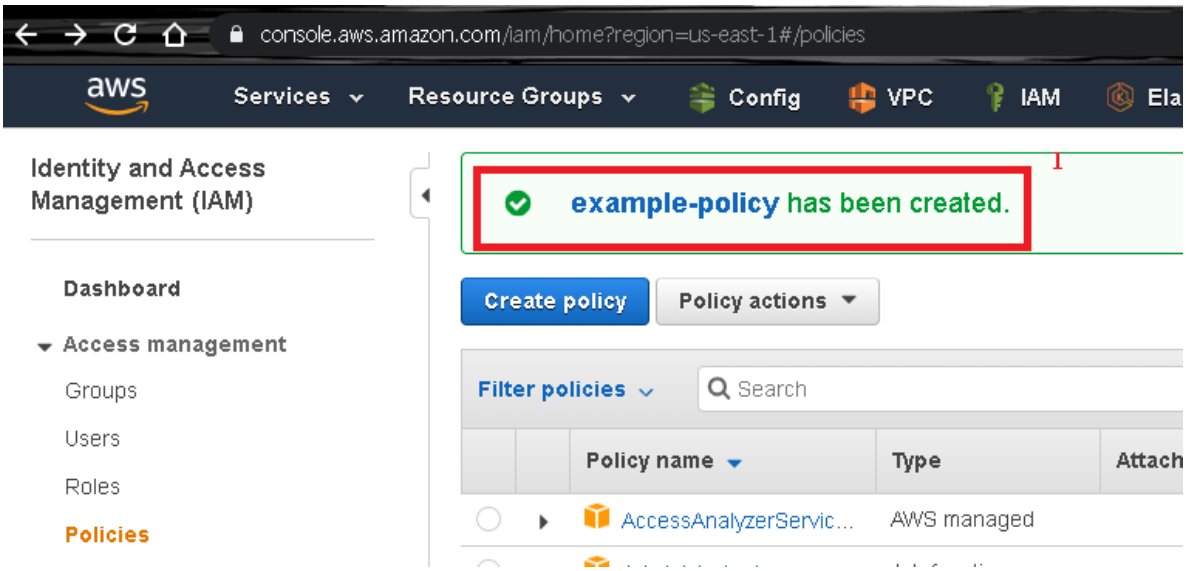

Visual editor
JSON
Import managed policy
Expand all | Collapse all
EC2 (1 action)
Clone | Remove
Service EC2
Actions Specify the actions allowed in EC2
close
Switch to deny permissions
DescribeIns
1
DescribeInstanceAttribute
DescribeInstances
2
DescribeInstanceTypes
DescribeInstanceCreditSpecificati...
DescribeInstanceStatus
DescribeInstanceEventNotification...
DescribeInstanceTypeOfferings
Resources The actions you chose support all resources.
Request conditions Specify request conditions (optional)
3
Add additional permissions

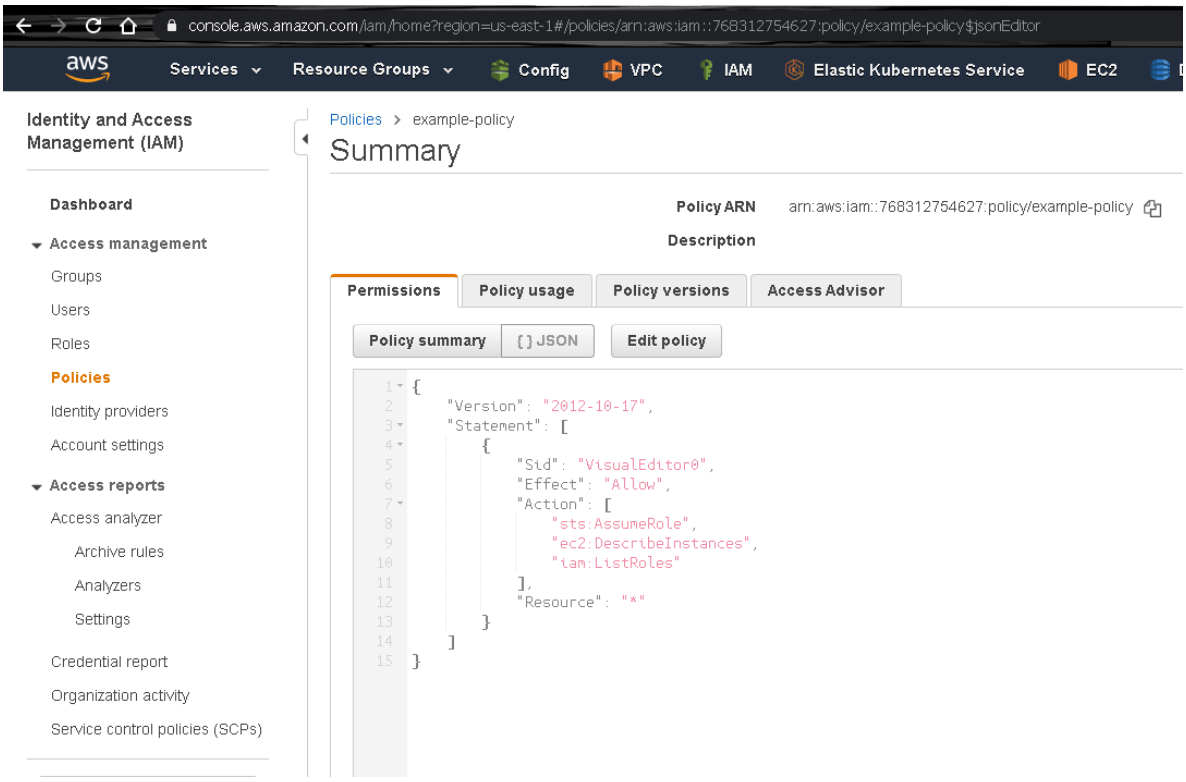

Service EC2
Actions Specify the actions allowed in EC2
close
Switch to deny permissions
DescribeIns
DescribeInstanceAttribute
DescribeInstances
DescribeInstanceTypes
DescribeInstanceCreditSpecificati...
DescribeInstanceStatus
DescribeInstanceEventNotification...
DescribeInstanceTypeOfferings
Resources The actions you chose support all resources.
Request conditions Specify request conditions (optional)
STS (1 action)
Clone | Remove
Service STS
Actions Write
AssumeRole
Resources
close
Specific
All resources
Request conditions Specify request conditions (optional)
Add additional permissions
Character count: 146 of 6144.
Cancel
Review policy


IAM (1 action)
Clone
Remove
1
Service IAM
2
Actions
close
Specify the actions allowed in IAM
Switch to deny permissions
ListRole
ListRolePolicies
3
ListRoles
ListRoleTags
Resources
The actions you chose support all resources.
Request conditions
Specify request conditions (optional)
Character count: 162 of 6144.
Cancel
Review policy
4

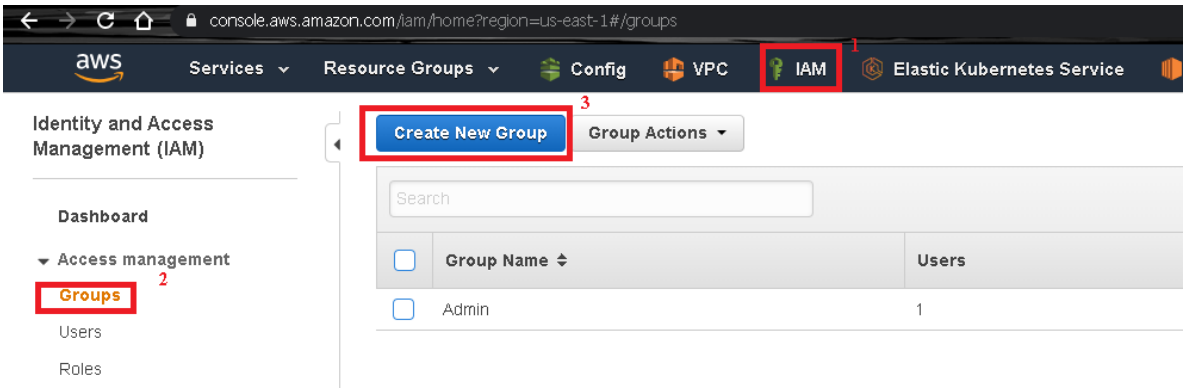

Review policy
1
Name*
example-policy
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter
Service
Access level
Resource
Request condition
Allow (3 of 232 services) Show remaining 229
EC2
Limited: List
All resources
None
IAM
Limited: List
All resources
None
STS
Limited: Write
All resources
None

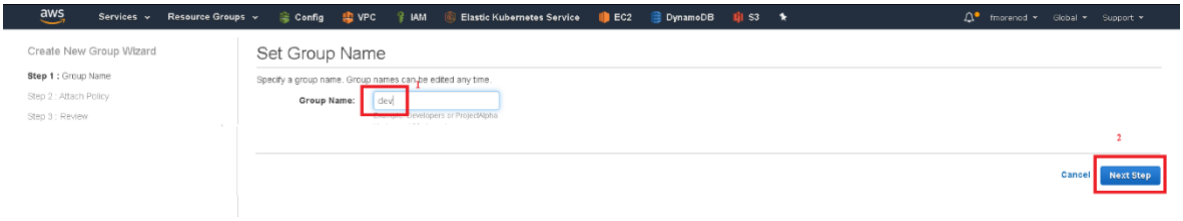
2
* Required
Cancel
Previous
Create policy

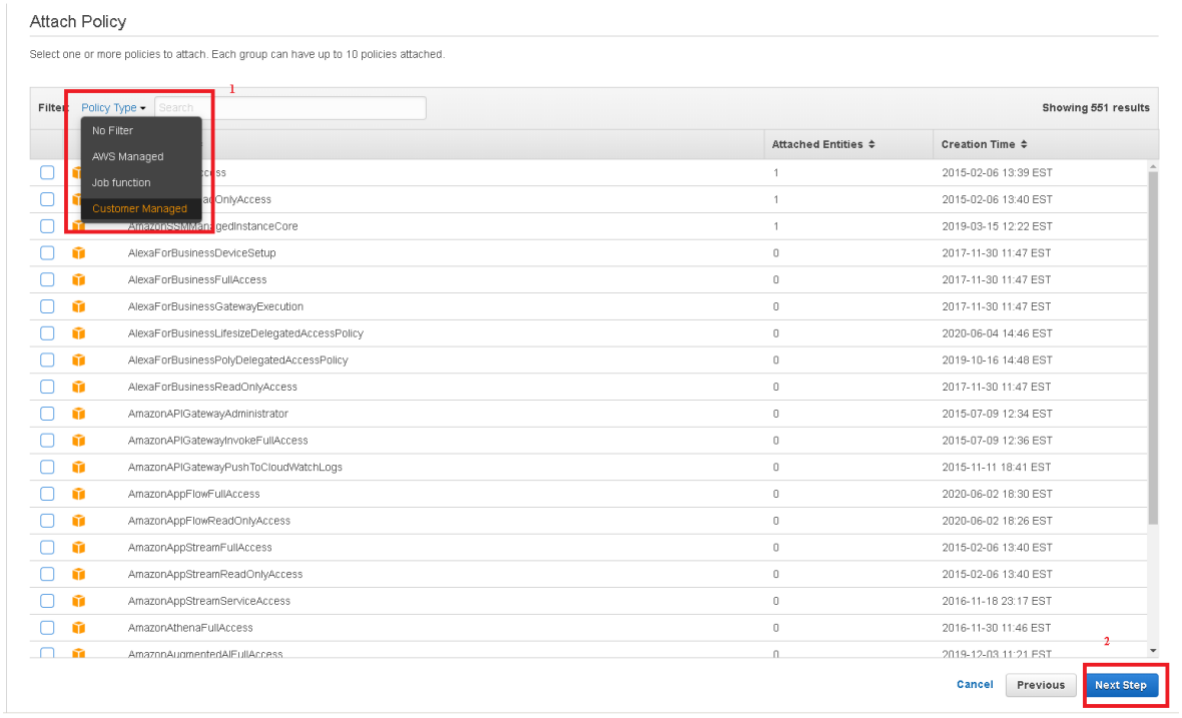


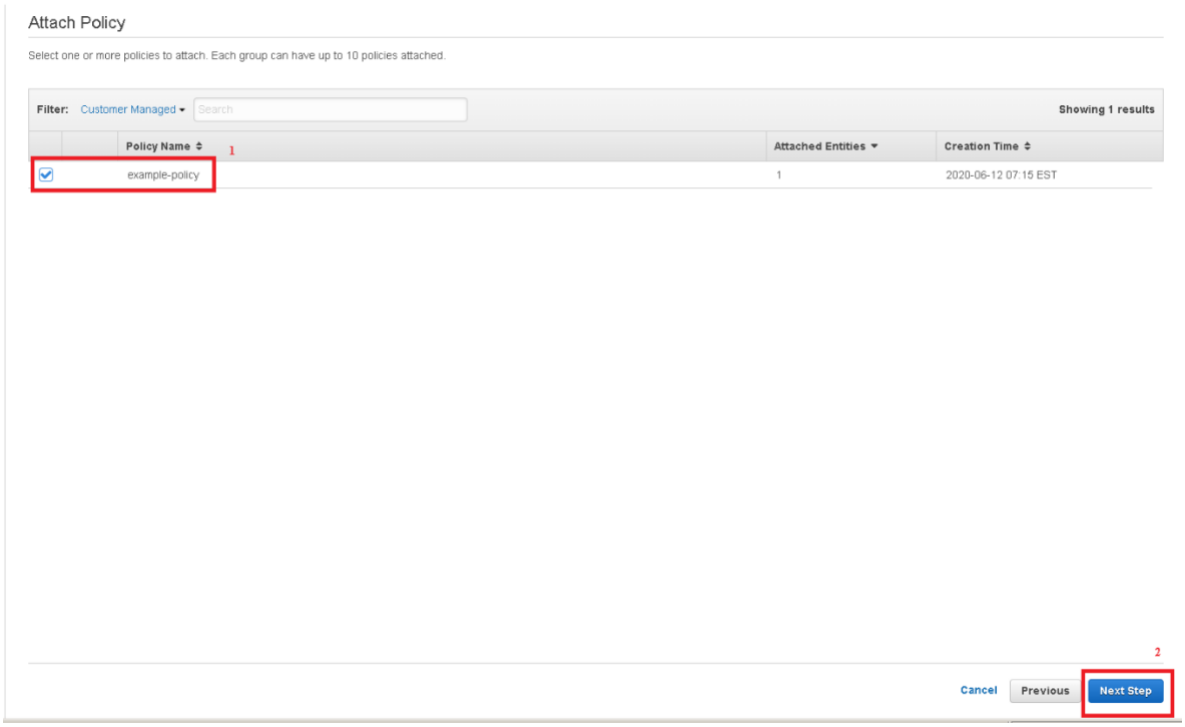


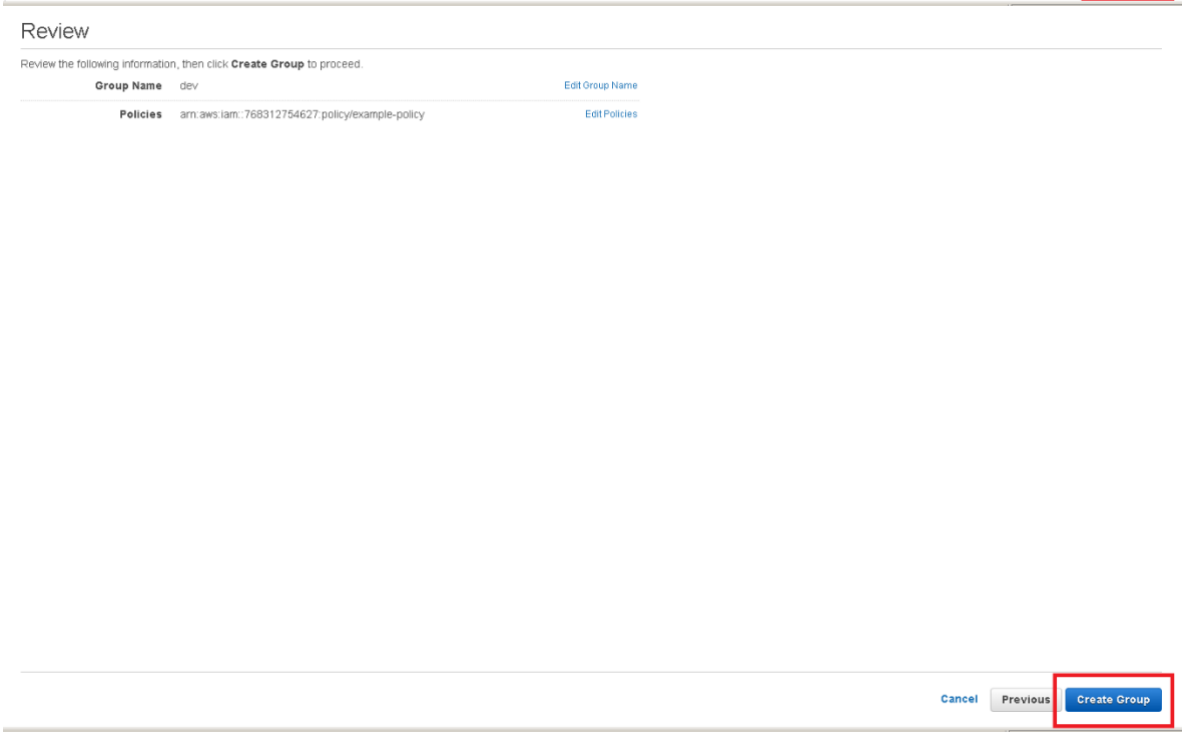
Create group and attached a policy


console.aws.amazon.com/iam/home?region=us-east-1#/groups
aws
Services
Resource Groups
Config
VPC
IAM
Elastic Kubernetes Service
1
Identity and Access Management (IAM)
Dashboard
Access management
Groups
2
Users
Roles
Create New Group
3
Group Actions
Search
Group Name
Users
Admin
1

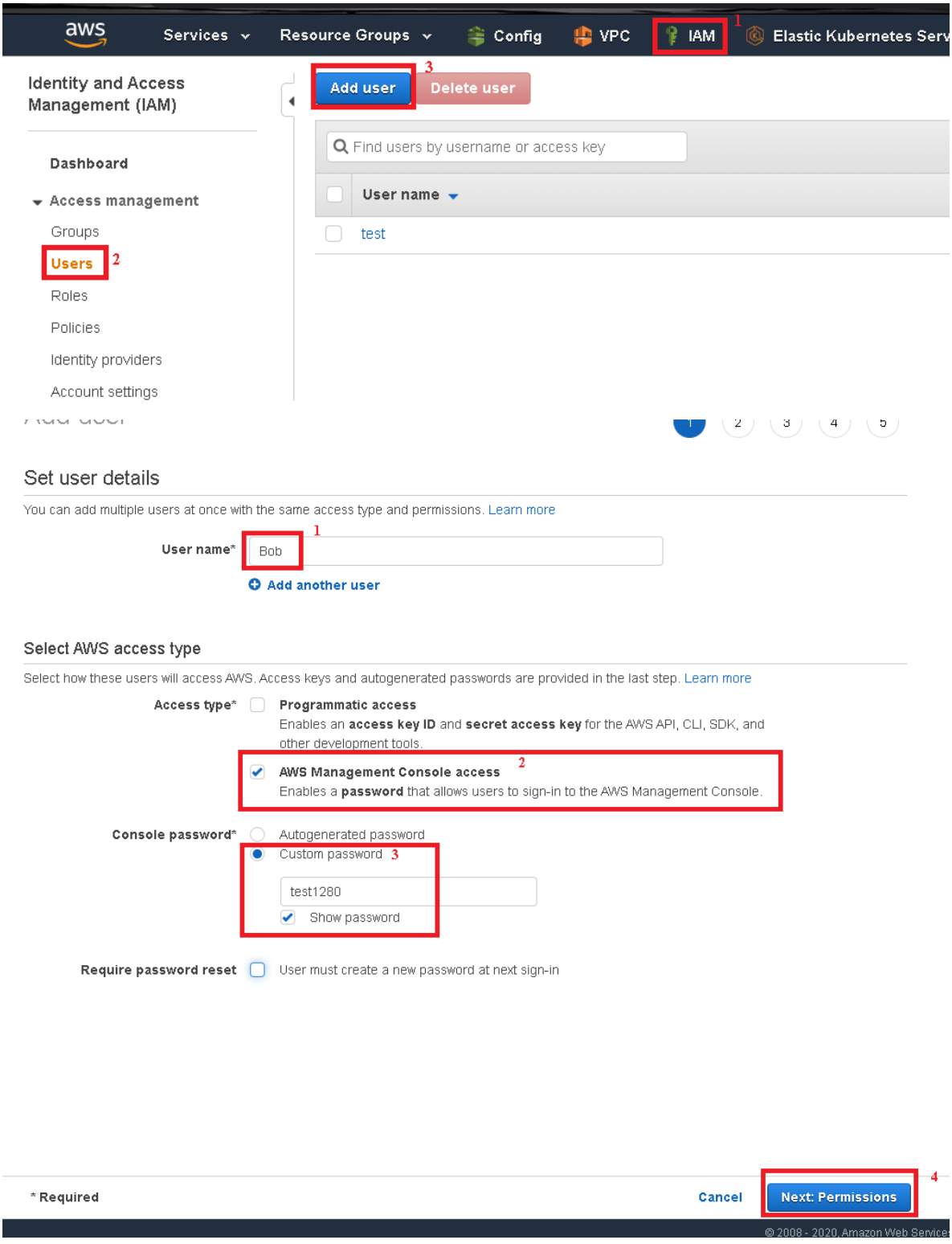

Create New Group Wizard
Step 1 : Group Name
Step 2 : Attach Policy
Step 3 : Review
Set Group Name
Specify a group name. Group names can be edited any time.
Group Name:
dev
1
2
Cancel
Next Step

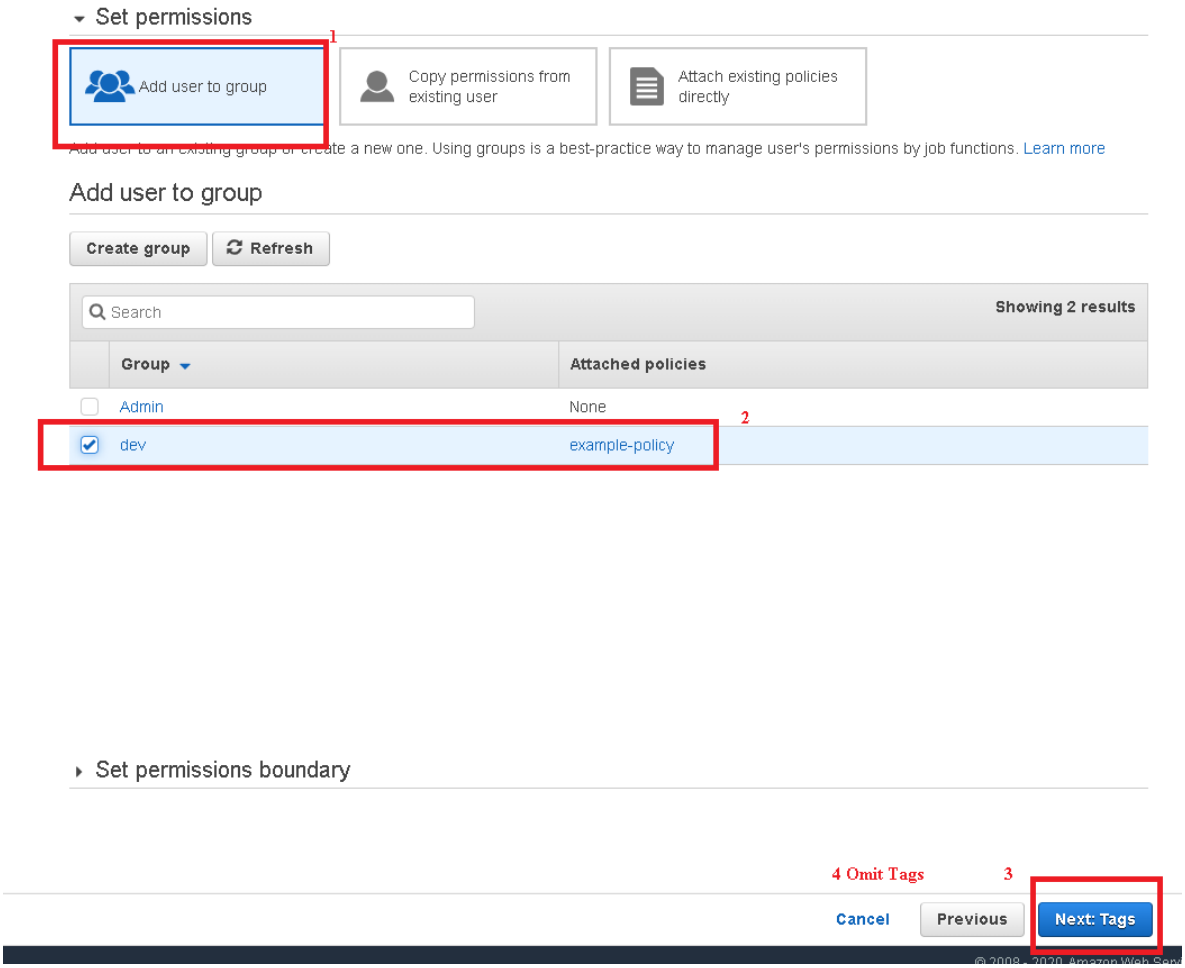

Attach Policy
Select one or more policies to attach. Each group can have up to 10 policies attached.
Filter:
Policy Type
Search
1
No Filter
AWS Managed
Job function
Customer Managed
Showing 551 results
Attached Entities
Creation Time
AlexaForBusinessDeviceSetup 0 2017-11-30 11:47 EST
AlexaForBusinessFullAccess 0 2017-11-30 11:47 EST
AlexaForBusinessGatewayExecution 0 2017-11-30 11:47 EST
AlexaForBusinessLifesizeDelegatedAccessPolicy 0 2020-06-04 14:46 EST
AlexaForBusinessPolyDelegatedAccessPolicy 0 2019-10-16 14:48 EST
AlexaForBusinessReadOnlyAccess 0 2017-11-30 11:47 EST
AmazonAPIGatewayAdministrator 0 2015-07-09 12:34 EST
AmazonAPIGatewayInvokeFullAccess 0 2015-07-09 12:36 EST
AmazonAPIGatewayPushToCloudWatchLogs 0 2015-11-11 18:41 EST
AmazonAppFlowFullAccess 0 2020-06-02 18:30 EST
AmazonAppFlowReadOnlyAccess 0 2020-06-02 18:26 EST
AmazonAppStreamFullAccess 0 2015-02-06 13:40 EST
AmazonAppStreamReadOnlyAccess 0 2015-02-06 13:40 EST
AmazonAppStreamServiceAccess 0 2016-11-18 23:17 EST
AmazonAthenaFullAccess 0 2016-11-30 11:46 EST
2
Cancel
Previous
Next Step


Attach Policy
Select one or more policies to attach. Each group can have up to 10 policies attached.
Filter: Customer Managed
Search
Showing 1 results
Policy Name
Attached Entities
Creation Time
example-policy
1
2020-06-12 07:15 EST
1
2
Cancel
Previous
Next Step


Review
Review the following information, then click Create Group to proceed.
Group Name
dev
Edit Group Name
Policies
arn:aws:iam::768312754627:policy/example-policy
Edit Policies
Cancel
Previous
Create Group

Create user and attached to the group




Set permissions
1
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 functions. Learn more
Add user to group
Create group
Refresh
Search
Showing 2 results
Group
Attached policies
Admin
None
dev
example-policy
2
Set permissions boundary
4 Omit Tags
3
Cancel
Previous
Next: Tags

Review

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

User details

User name	Bob
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Group	dev

Tags

No tags were added.

1

Cancel Previous **Create user**

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.

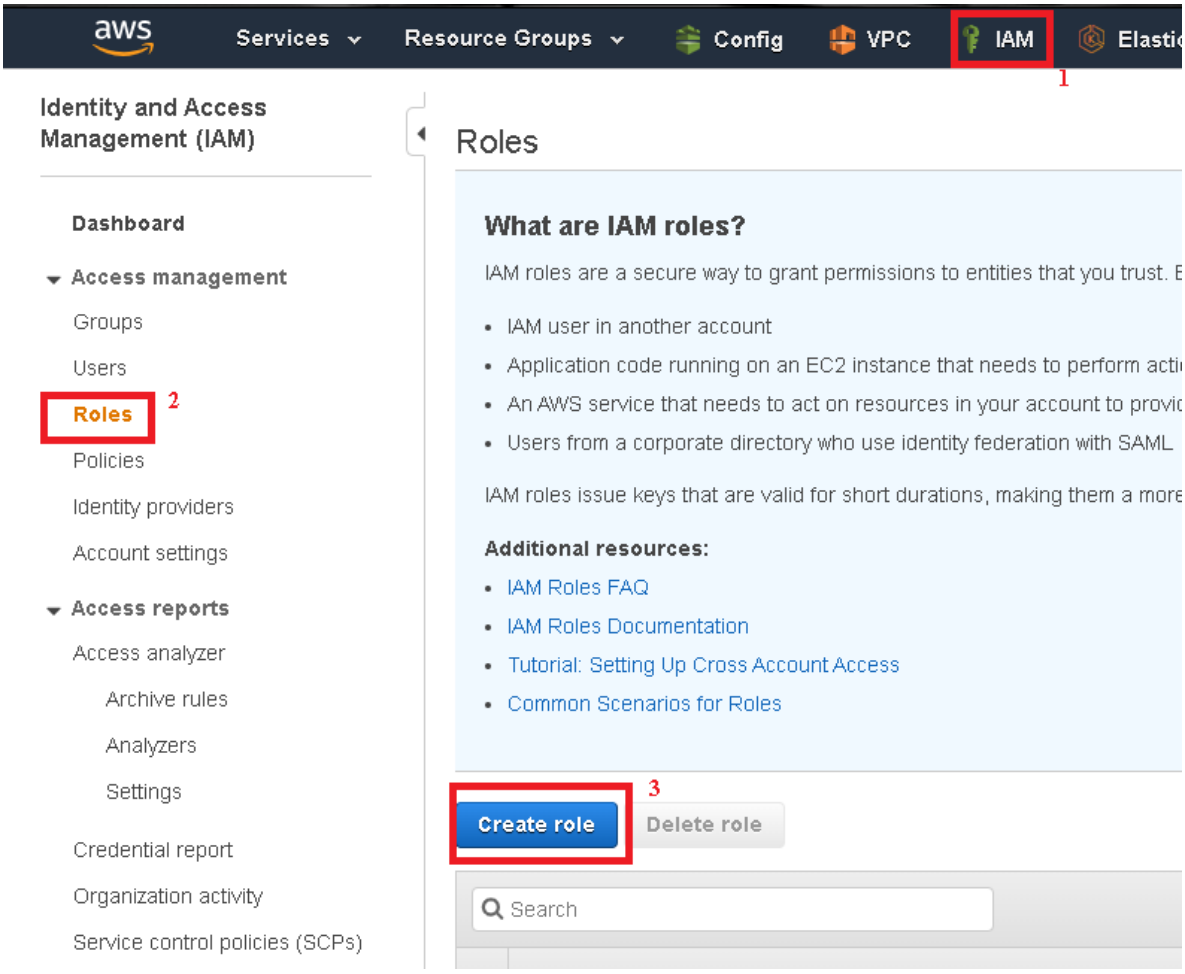
Users with AWS Management Console access can sign-in at: https://fmoreno-test.signin.aws.amazon.com/console

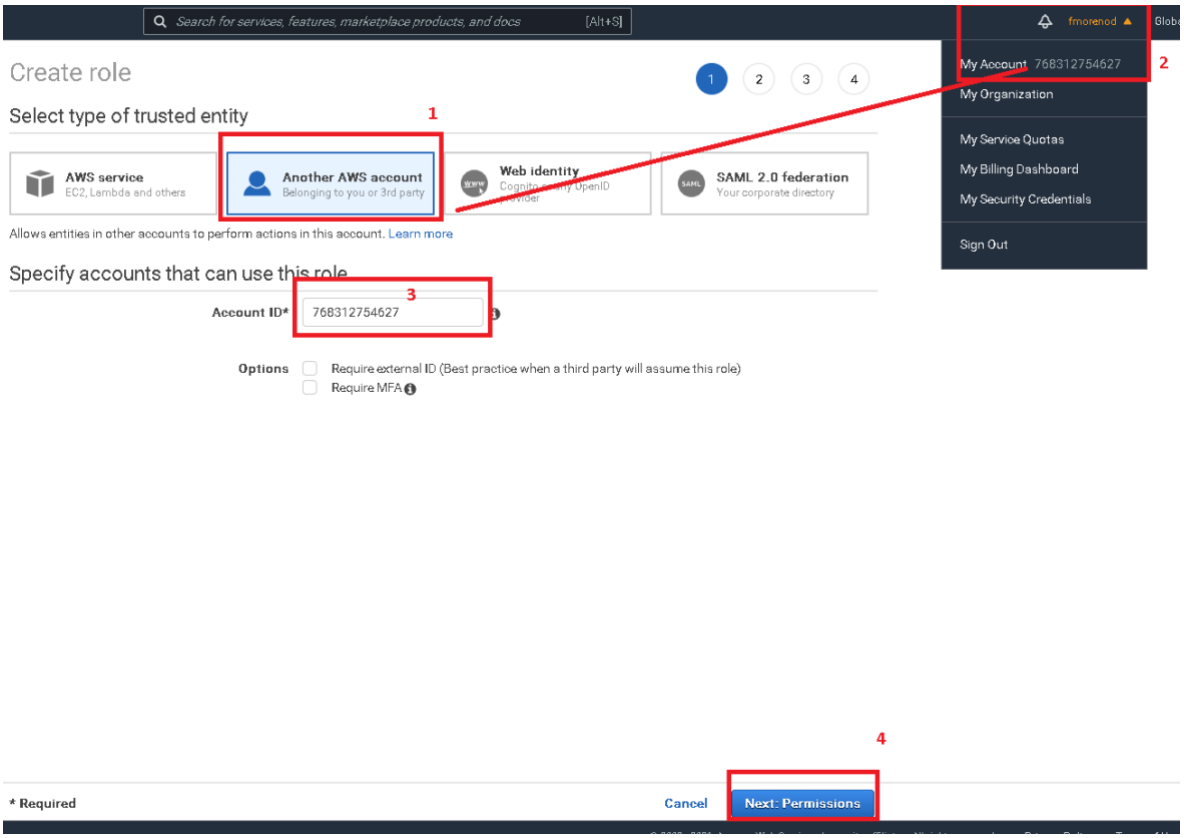
Download .csv

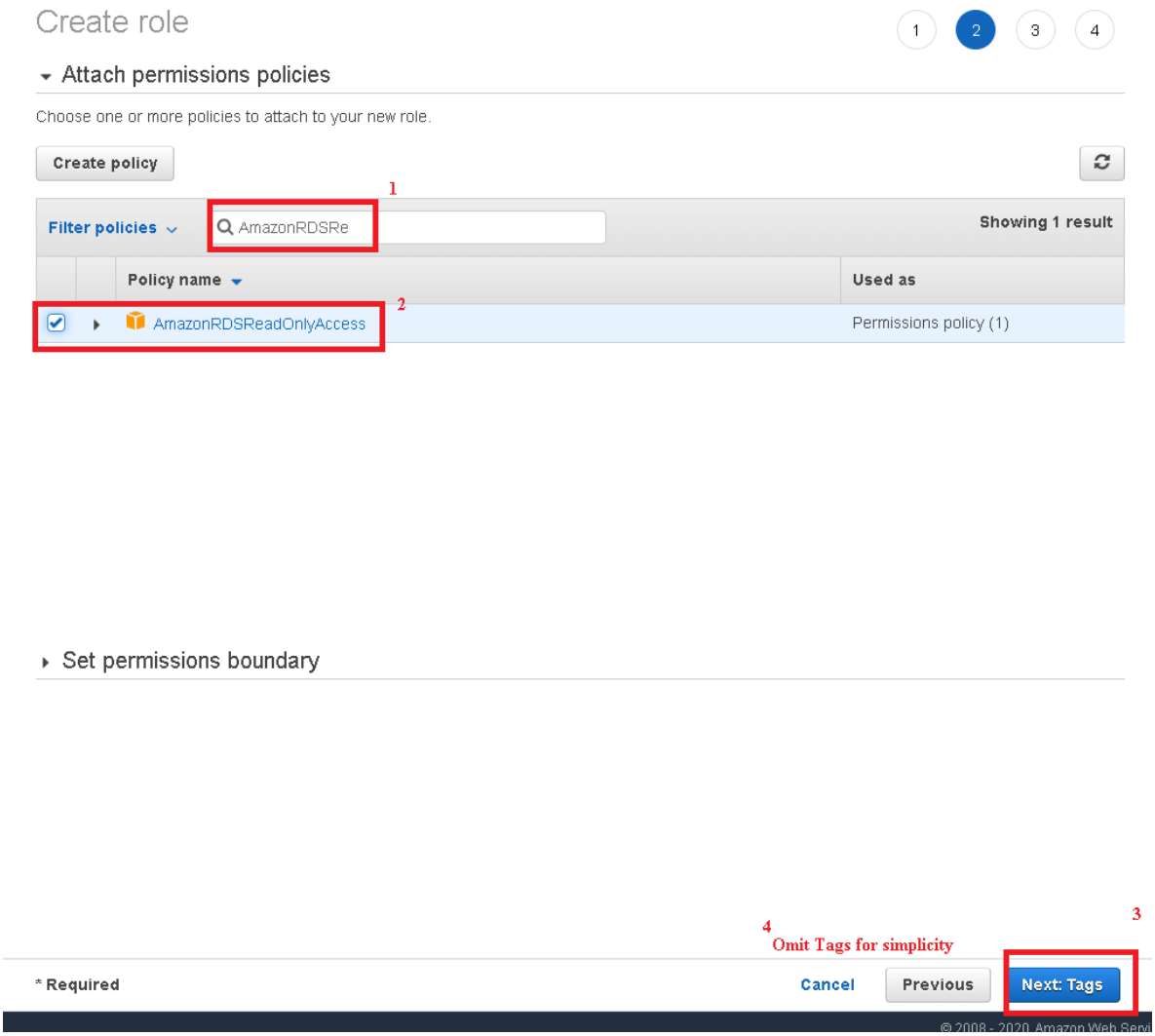
	User	Email login instructions
▸	Bob	Send email

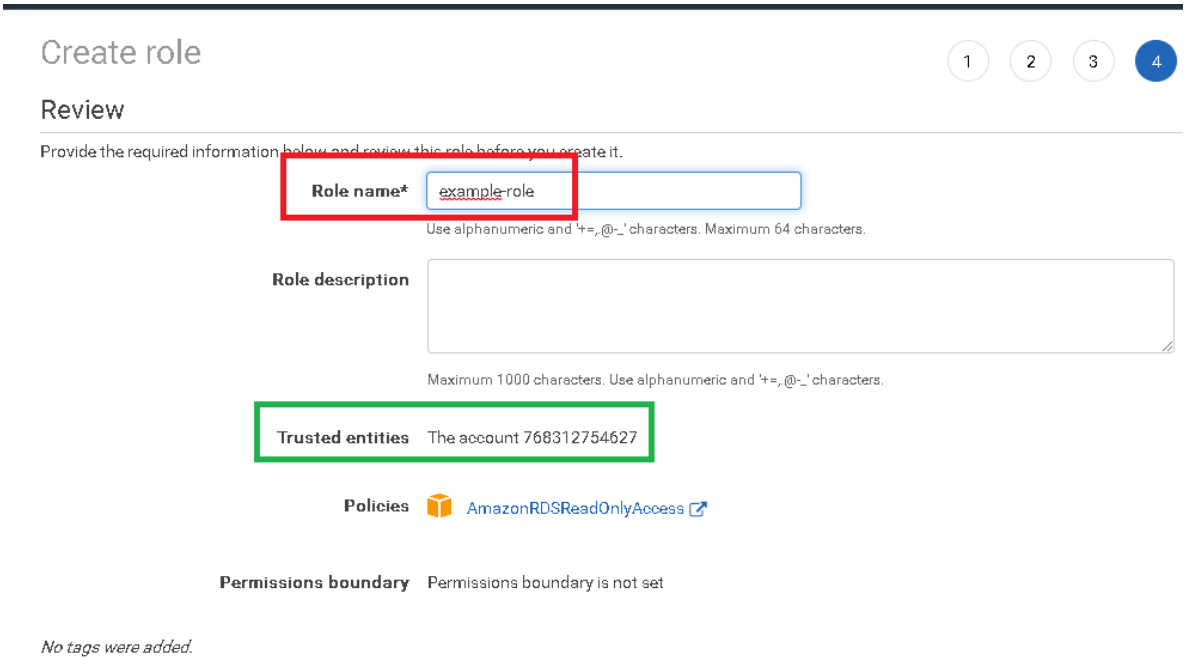
Close

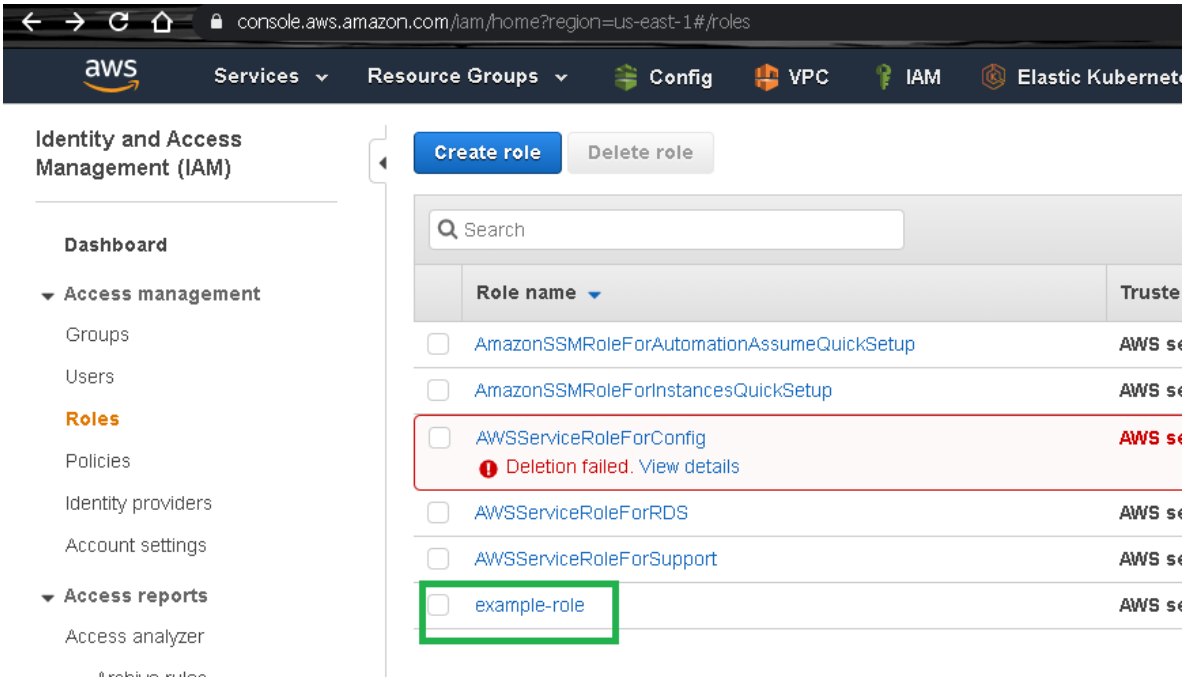
Create a role and apply an aws-managed policy




Search for services, features, marketplace products, and docs [Alt+S]
fmorenod
My Account 768312754627
My Organization
My Service Quotas
My Billing Dashboard
My Security Credentials
Sign Out
2
Create role
1 2 3 4
Select type of trusted entity
1
AWS service
EC2, Lambda and others
Another AWS account
Belonging to you or 3rd party
Web identity
SAML 2.0 federation
Your corporate directory
Allows entities in other accounts to perform actions in this account. Learn more
Specify accounts that can use this role
3
Account ID*
768312754627
Options
Require external ID (Best practice when a third party will assume this role)
Require MFA
4
* Required
Cancel
Next: Permissions

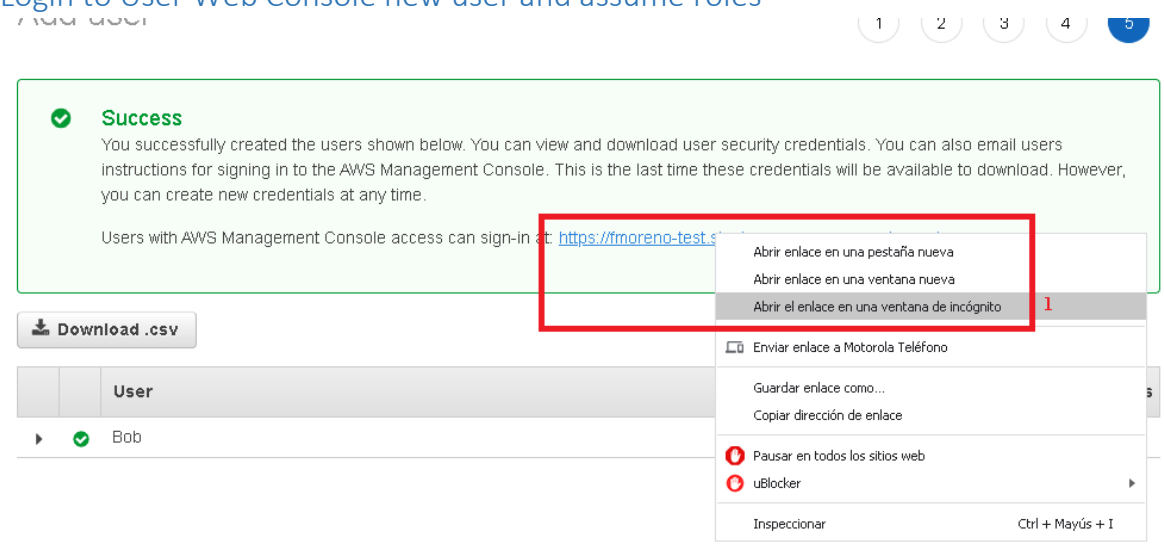

Create role
1
2
3
4
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
1
Filter policies
AmazonRDSRe
Showing 1 result
Policy name
Used as
2
AmazonRDSReadOnlyAccess
Permissions policy (1)
Set permissions boundary
4
Omit Tags for simplicity
3
* Required
Cancel
Previous
Next: Tags

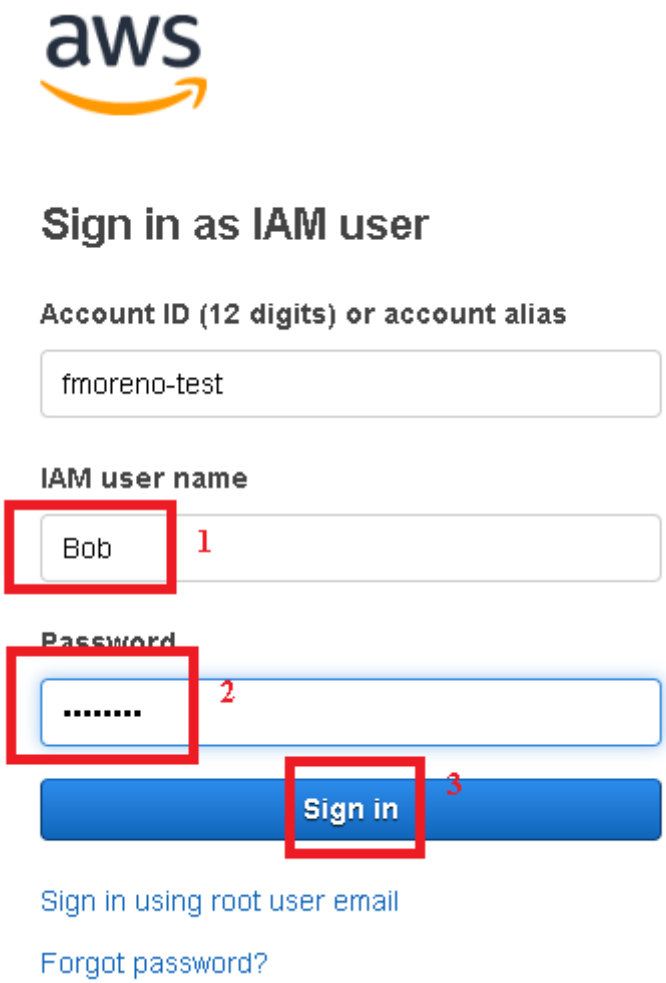




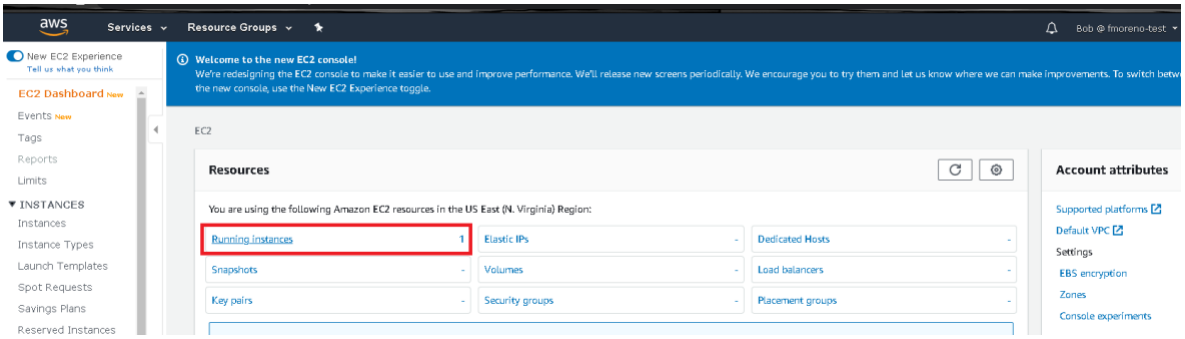
Click on example-role

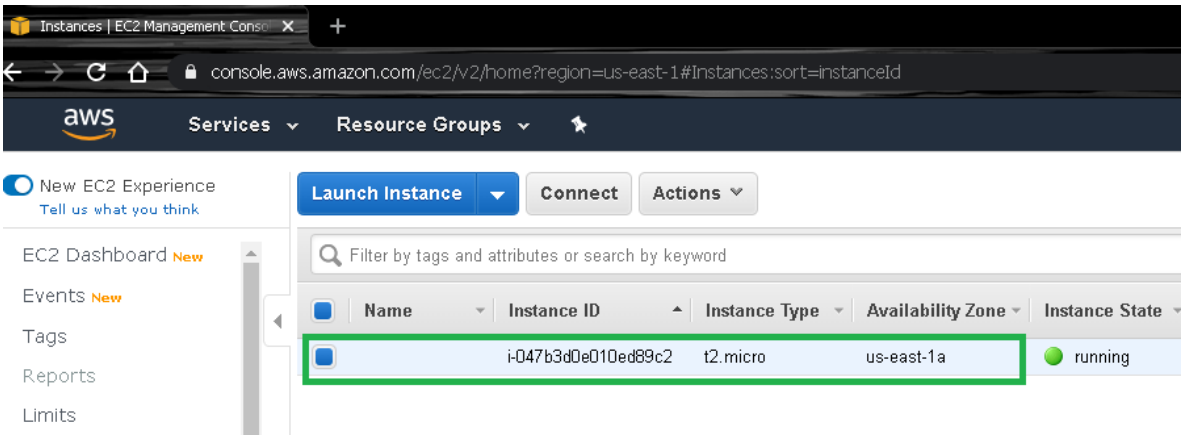
Login to User Web Console new user and assume roles

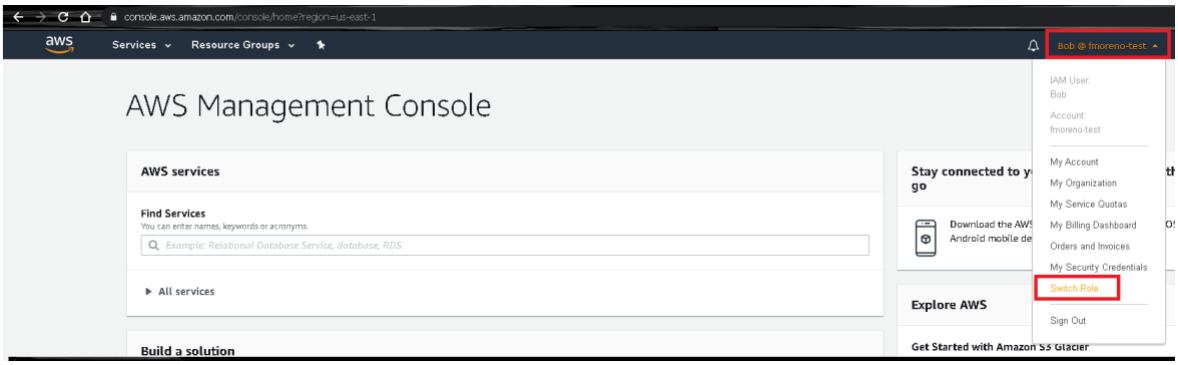


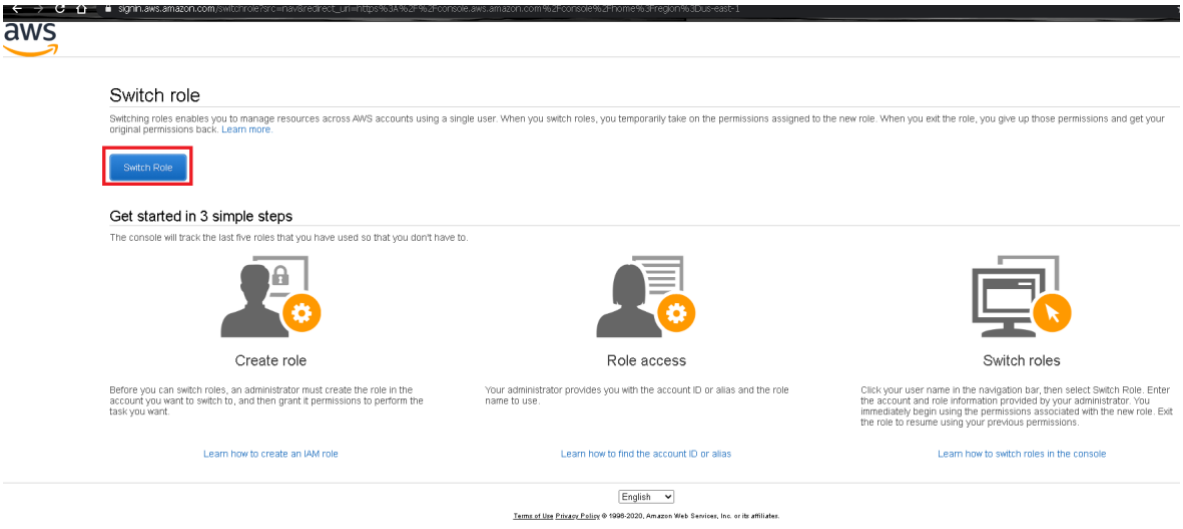


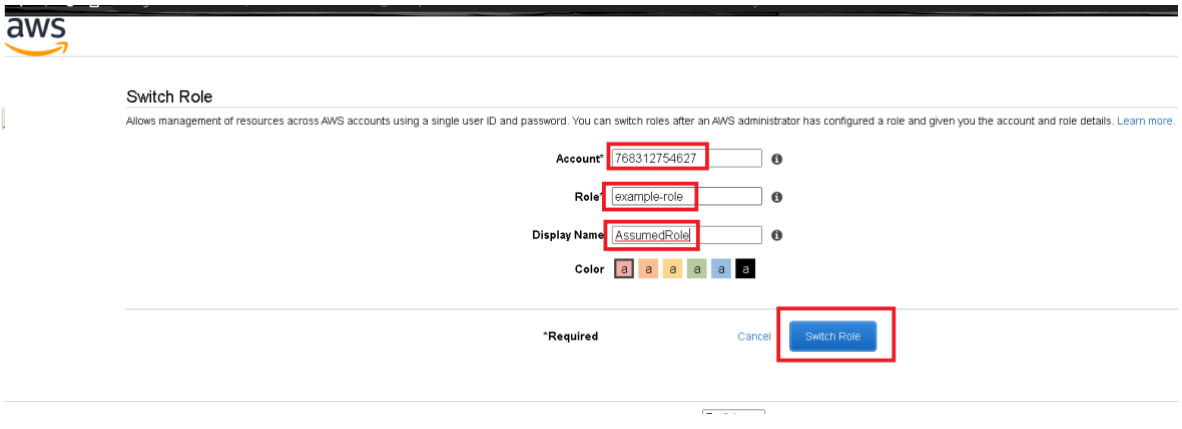
After entered to Web Management Console, go to EC2 Services and then:

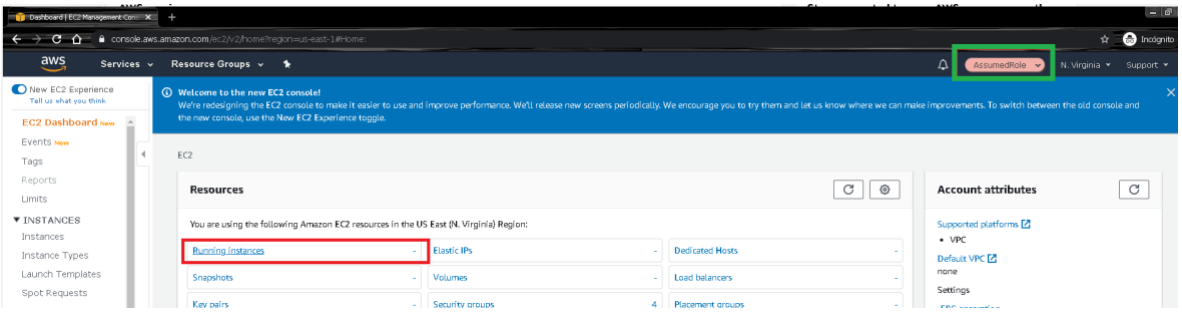


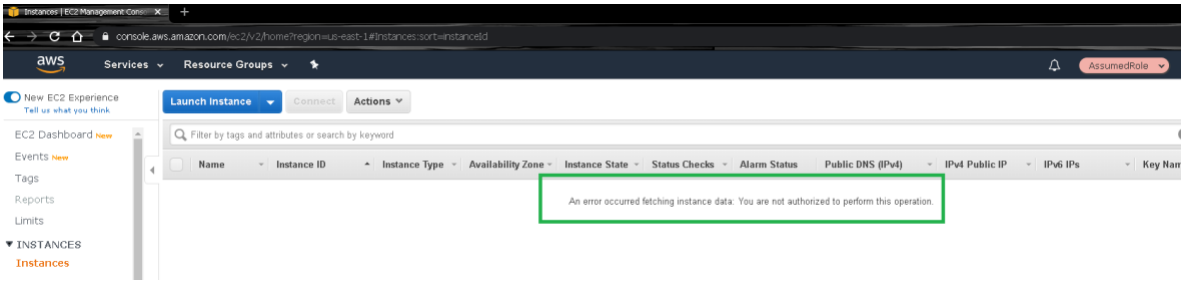

Instances | EC2 Management Conso
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:sort=instanceId
Services
Resource Groups
New EC2 Experience
Tell us what you think
EC2 Dashboard New
Events New
Tags
Reports
Limits
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
Name
Instance ID
Instance Type
Availability Zone
Instance State
i-047b3d0e010ed89c2
t2.micro
us-east-1a
running

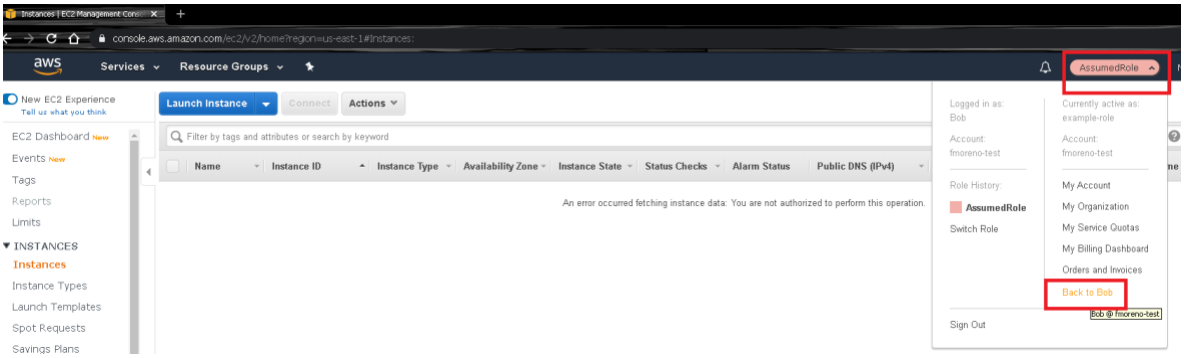

AWS Management Console
AWS services
Find Services
Build a solution
Explore AWS
Bob @ fmoreno-test
My Account
My Organization
My Service Quotas
My Billing Dashboard
Orders and Invoices
My Security Credentials
Switch Role
Sign Out


Switch role
Switch Role
Get started in 3 simple steps
Create role
Role access
Switch roles
Learn how to create an IAM role
Learn how to find the account ID or alias
Learn how to switch roles in the console


Switch Role
Allows management of resources across AWS accounts using a single user ID and password. You can switch roles after an AWS administrator has configured a role and given you the account and role details. Learn more.
Account* 768312754627
Role* example-role
Display Name AssumedRole
Color
*Required
Cancel
Switch Role


AssumedRole
Welcome to the new EC2 console!
Resources
Account attributes
Running Instances
Elastic IPs
Dedicated Hosts
Snapshots
Volumes
Load balancers

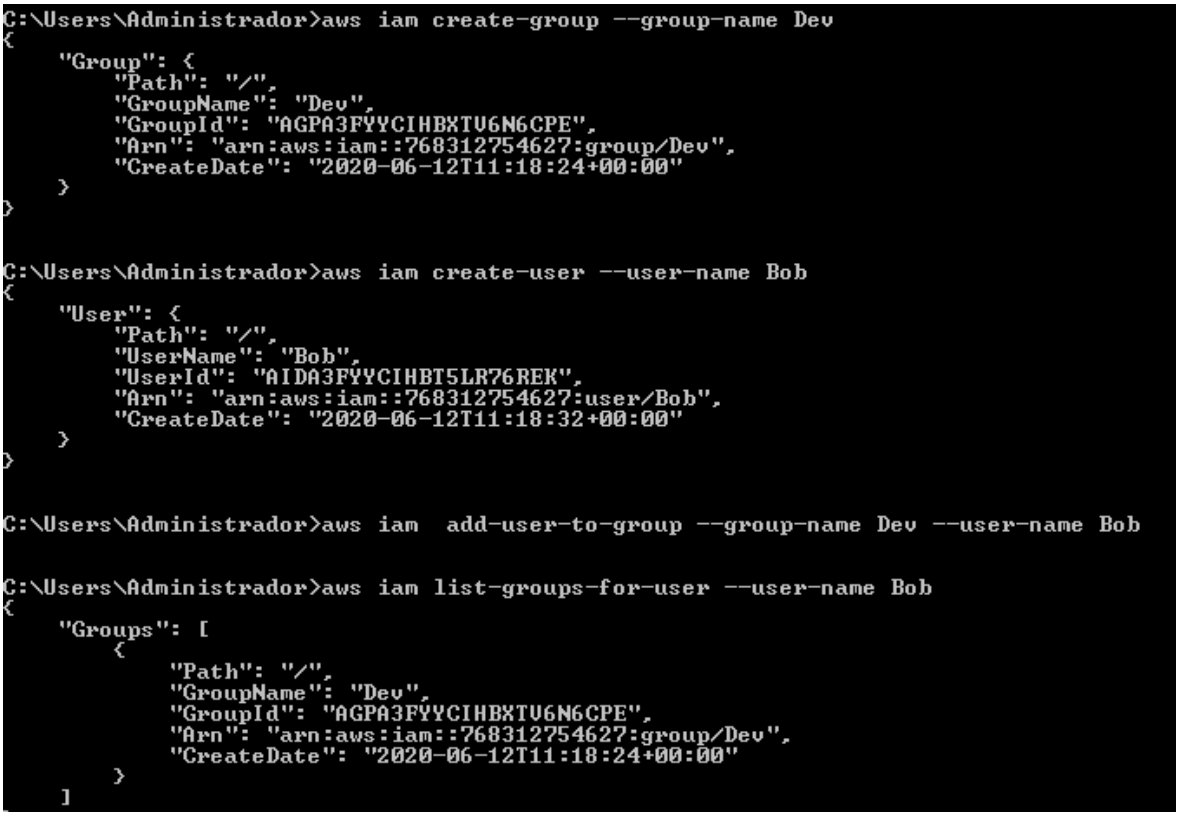

AssumedRole
Launch Instance
Connect
Actions
An error occurred fetching instance data: You are not authorized to perform this operation.


AssumedRole
Launch Instance
Connect
Actions
An error occurred fetching instance data: You are not authorized to perform this operation.
Logged in as: Bob
Currently active as: example-role
Account: fmoreno-test
Role History:
AssumedRole
Switch Role
My Account
My Organization
My Service Quotas
My Billing Dashboard
Orders and Invoices
Back to Bob
Sign Out

Lab 2 using Command Line (Windows)

Create group, user and attached to the group

```
rem Crear un grupo
aws iam create-group --group-name Dev
rem Crear los usuarios
aws iam create-user --user-name Bob
rem Agregar usuarios al grupo
aws iam  add-user-to-group --group-name Dev --user-name Bob
aws iam list-groups-for-user --user-name Bob
```



Predefined files

There 2 previous files on the same folder: example-policy.json and example-role-trust-policy.json

example-policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "iam:ListRoles",
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}
```

example-role-trust-policy.json

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": { "AWS": "arn:aws:iam::768312754627:root" },
        "Action": "sts:AssumeRole"
    }
}
```

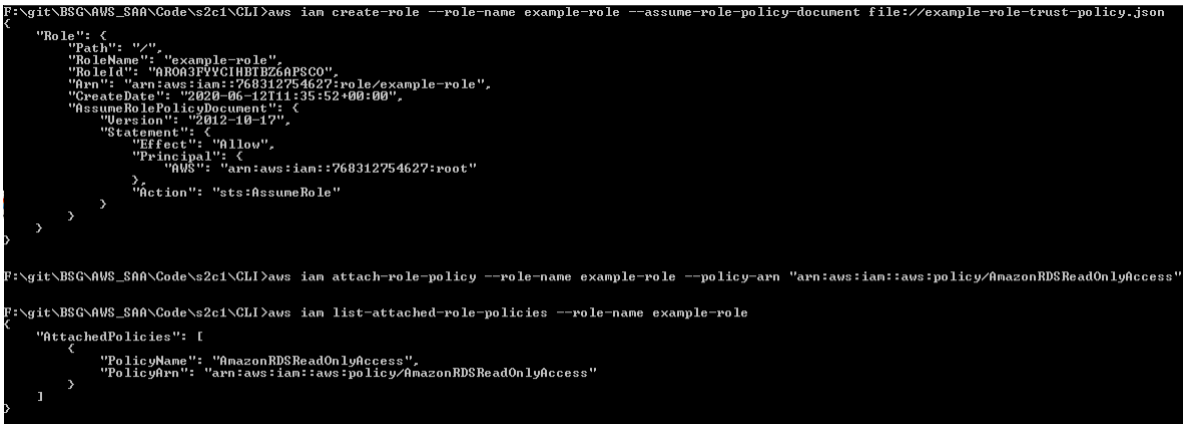
Create a policy and attached it to the group

```
rem Crear la politica
aws iam create-policy --policy-name example-policy --policy-
document file://example-policy.json
rem Asignar la politica al grupo, reemplazando el Account Number
aws iam attach-group-policy --group-name Dev --policy-
arn "arn:aws:iam::768312754627:policy/example-policy"
rem Revisar que el listado de politicas asignadas al usuario
aws iam list-attached-group-policies --group-name Dev
aws iam list-group-policies --group-name Dev
aws iam list-attached-user-policies --user-name Bob
aws iam list-policies --scope Local
```

```
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam create-policy --policy-name example-policy --policy-document file://example-policy.json
{
    "Policy": {
        "PolicyName": "example-policy",
        "PolicyId": "ANPA3FYYCIHBUNBQXKBBN",
        "Arn": "arn:aws:iam::768312754627:policy/example-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2020-06-12T11:34:00+00:00",
        "UpdateDate": "2020-06-12T11:34:00+00:00"
    }
}

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam attach-group-policy --group-name Dev --policy-arn "arn:aws:iam::768312754627:policy/example-policy"

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam list-attached-group-policies --group-name Dev
{
    "AttachedPolicies": [
        {
            "PolicyName": "example-policy",
            "PolicyArn": "arn:aws:iam::768312754627:policy/example-policy"
        }
    ]
}


F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam list-group-policies --group-name Dev
{
    "PolicyNames": []
}


F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam list-attached-user-policies --user-name Bob
{
    "AttachedPolicies": []
}


F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam list-policies --scope Local
{
    "Policies": [
        {
            "PolicyName": "example-policy",
            "PolicyId": "ANPA3FYYCIHBUNBQXKBBN",
            "Arn": "arn:aws:iam::768312754627:policy/example-policy",
            "Path": "/",
            "DefaultVersionId": "v1",
            "AttachmentCount": 1,
            "PermissionsBoundaryUsageCount": 0,
            "IsAttachable": true,
            "CreateDate": "2020-06-12T11:34:00+00:00",
            "UpdateDate": "2020-06-12T11:34:00+00:00"
        }
    ]
}
```

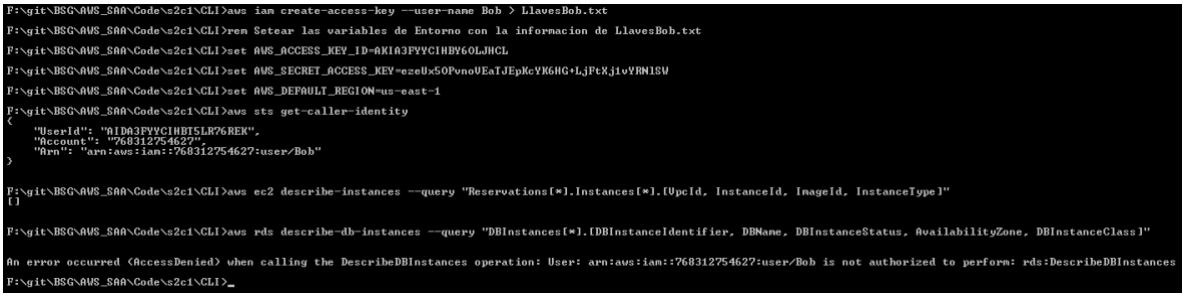
Create a role, apply policy to assume role and attached an aws-managed policy

```
rem Crear un Role y asignarle un Trust Policy modificando el nombre de la cu
enta debido a que puede ser diferente
aws iam create-role --role-name example-role --assume-role-policy-
document file://example-role-trust-policy.json
rem Agregar una politica manejada por AWS al role
aws iam attach-role-policy --role-name example-role --policy-
arn "arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess"
rem Verificar listado de politicas asociadas al role
aws iam list-attached-role-policies --role-name example-role
```



Create keys for user and check applied policy

```
rem Crear llaves de acceso al usuario
aws iam create-access-key --user-name Bob > LlavesBob.txt
rem Setear las variables de Entorno con la informacion de LlavesBob.txt
rem Revisar que se esten ejecutando como Bob
aws sts get-caller-identity
rem Revisar que acciones puedo realizar como Bob. Falla con RDS
aws ec2 describe-instances --
query "Reservations[*].Instances[*].[VpcId, InstanceId, ImageId, InstanceTyp
e]"
aws rds describe-db-instances --
query "DBInstances[*].[DBInstanceIdentifier, DBName, DBInstanceStatus, Avail
abilityZone, DBInstanceClass]"
```



Assume role and check new policy

```
rem Obtener el ARN del rol a aplicar
aws iam list-roles --query "Roles[?RoleName == 'example-
role'].[RoleName, Arn]"
rem Asumir el role al usuario actual y ponerle un nombre de sesion
aws sts assume-role --role-arn "arn:aws:iam::768312754627:role/example-
role" --role-session-name AWSCLI-Session >LlavesSesion.txt
rem Setear las variables de Entorno con la informacion de LlavesSesion.txt
rem Verificar que esta ejecutando el usuario adecuado
```

```
aws sts get-caller-identity
rem Volver a ejecutar el listado de acciones
aws ec2 describe-instances --
query "Reservations[*].Instances[*].[VpcId, InstanceId, ImageId, InstanceTyp
e]"
aws rds describe-db-instances --
query "DBInstances[*].[DBInstanceIdentifier, DBName, DBInstanceStatus, Avail
abilityZone, DBInstanceClass]"
```

Evidences to send

To have a review, the student has to send some screenshots to instructor email:

1. See instances using the role and switch of role, which are the last 2 screens of Login to User Web Console new user and assume roles (For Web Management Console) or the last 2 screens for Assume role and check new policy (For CLI).