Contents

[Purpose 2](#_Toc74290800)

[Prerequisites 2](#_Toc74290801)

[Lab 2 using Web Management Console 3](#_Toc74290802)

[Create a policy 3](#_Toc74290803)

[Create group and attached a policy 6](#_Toc74290804)

[Create user and attached to the group 9](#_Toc74290805)

[Create a role and apply an aws-managed policy 13](#_Toc74290806)

[Login to User Web Console new user and assume roles 17](#_Toc74290807)

[Lab 2 using Command Line (Windows) 21](#_Toc74290808)

[Create group, user and attached to the group 21](#_Toc74290809)

[Predefined files 21](#_Toc74290810)

[Create a policy and attached it to the group 23](#_Toc74290811)

[Create a role, apply policy to assume role and attached an aws-managed policy 24](#_Toc74290812)

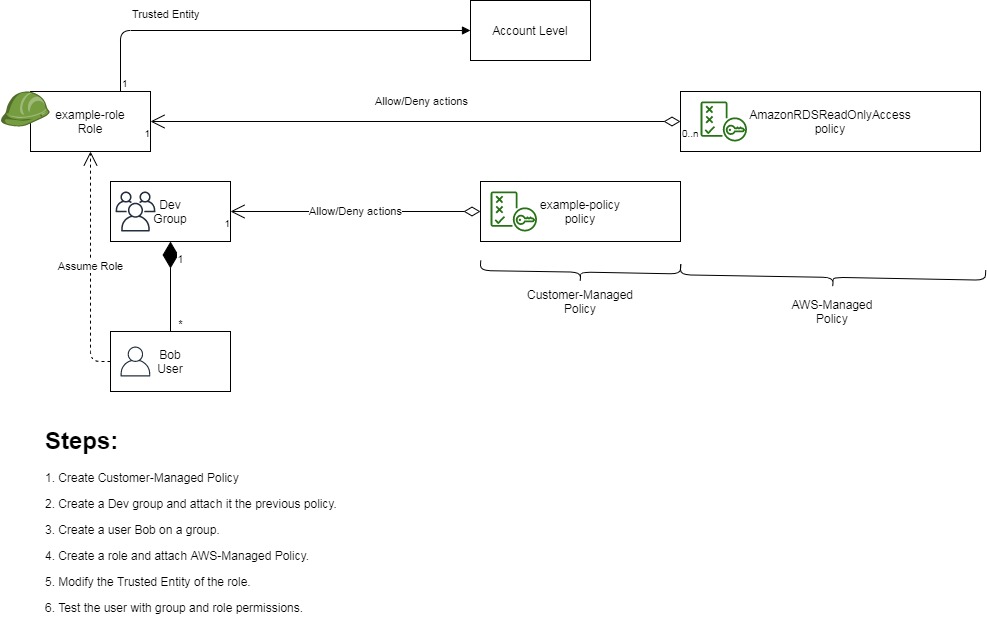
[Create keys for user and check applied policy 25](#_Toc74290813)

[Assume role and check new policy 25](#_Toc74290814)

[Evidences to send 26](#_Toc74290815)

# 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.

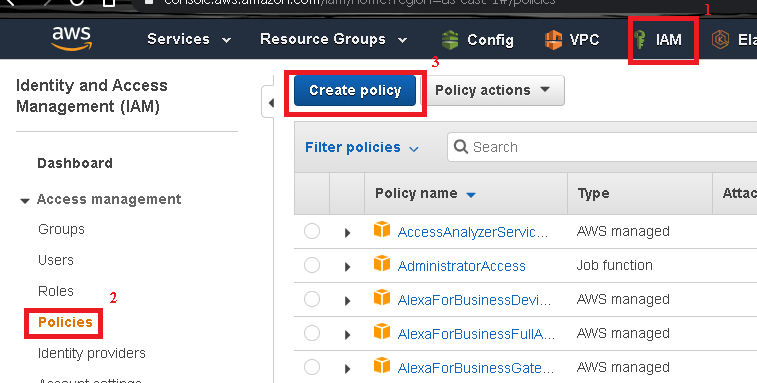


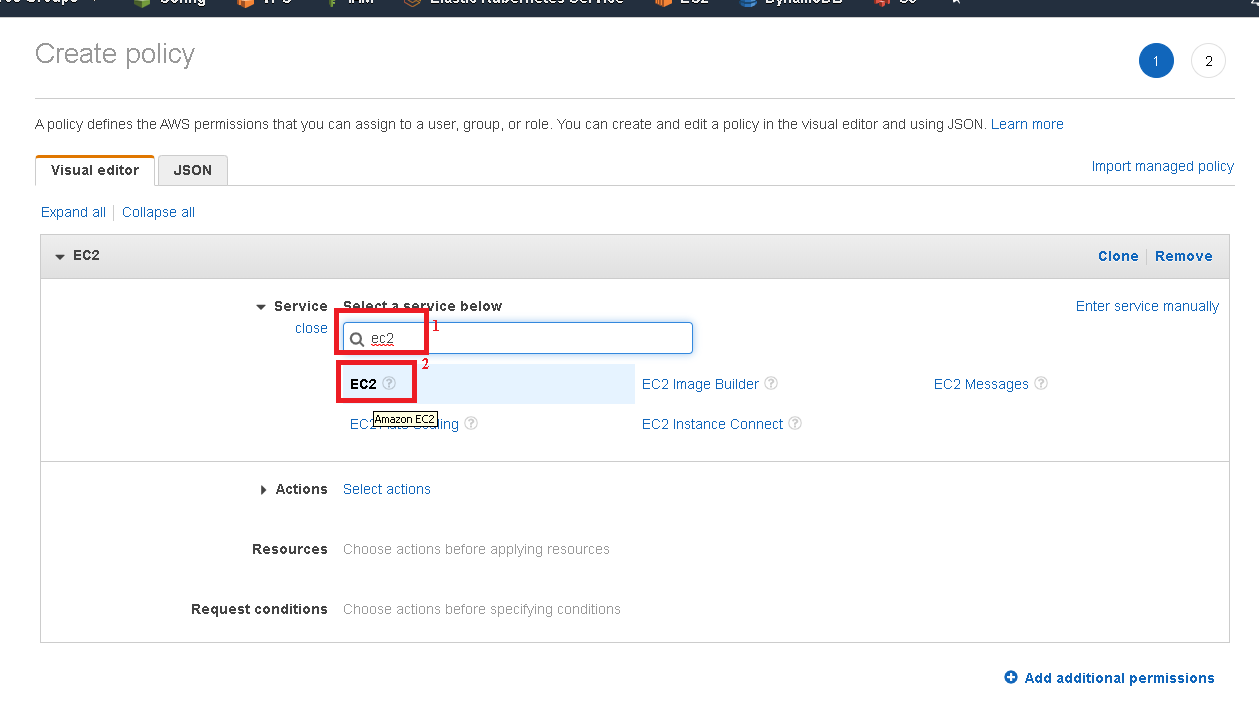
# Prerequisites

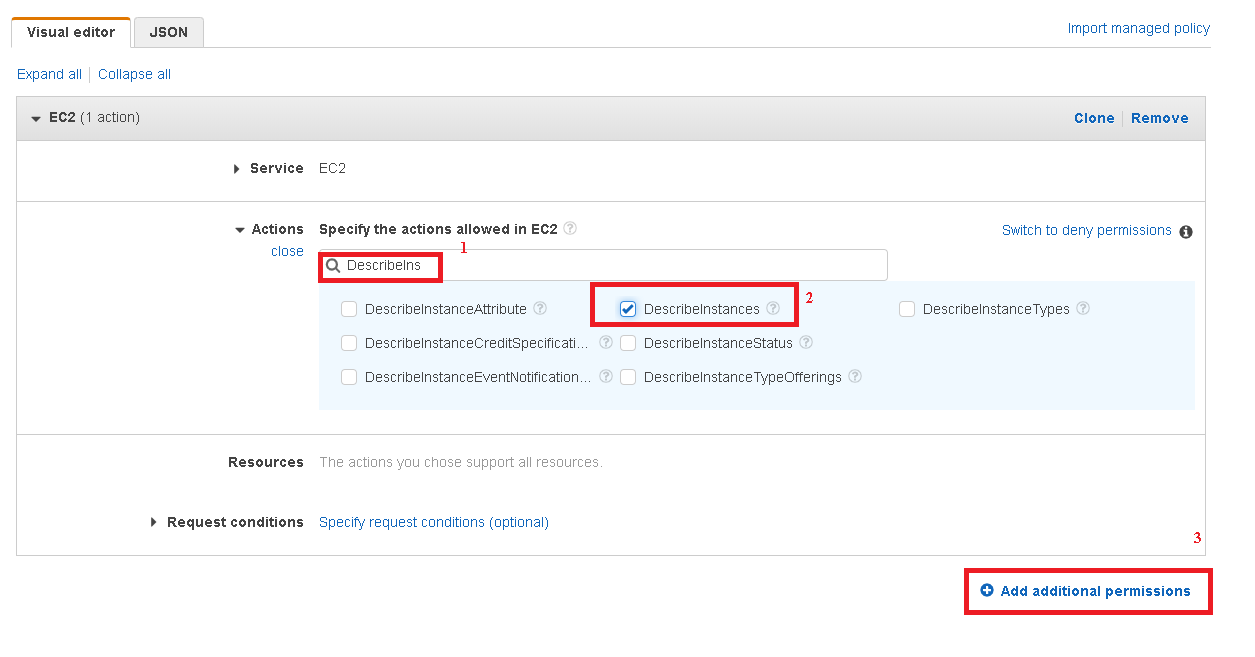
Labs1c1 have to be done and the context for Administrative user have to activated on Command Line Session.

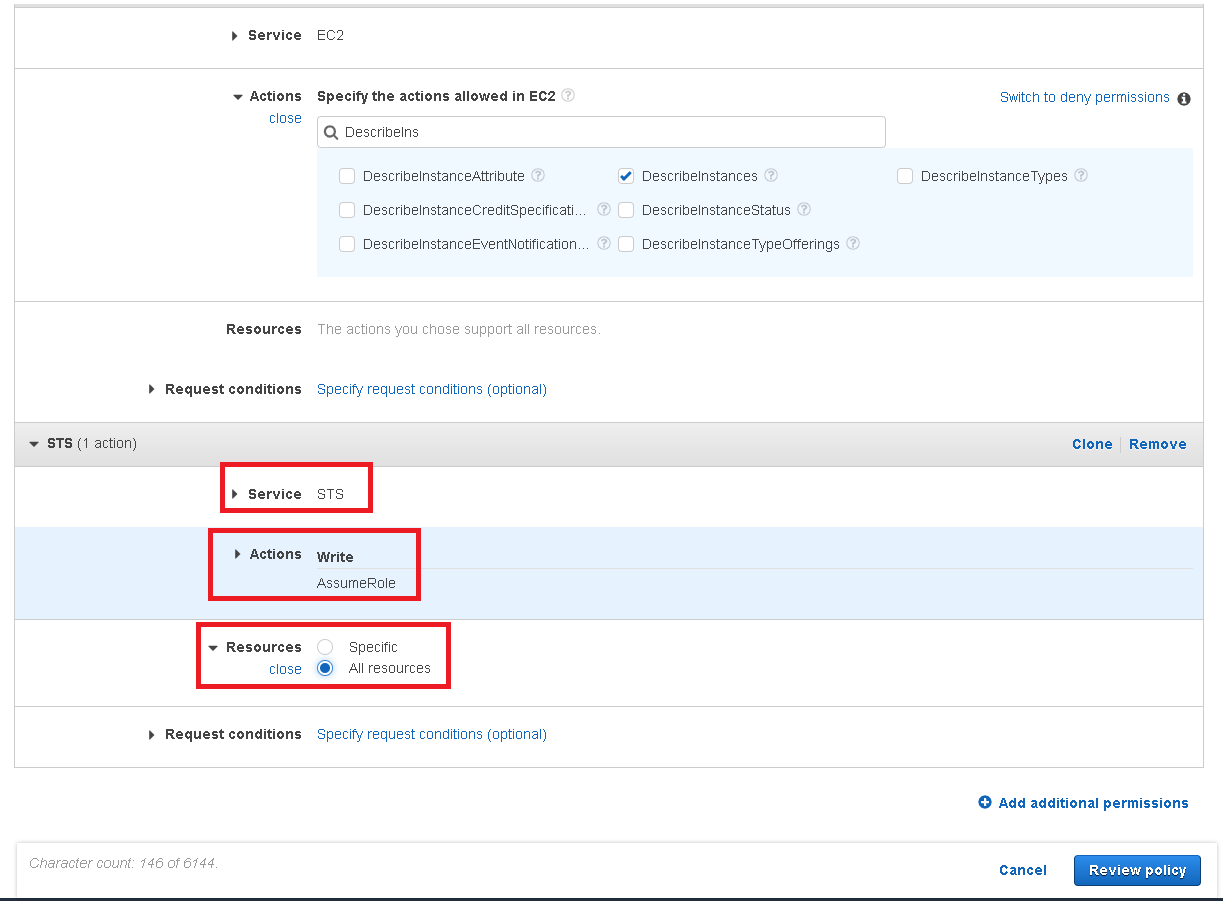
# Lab 2 using Web Management Console

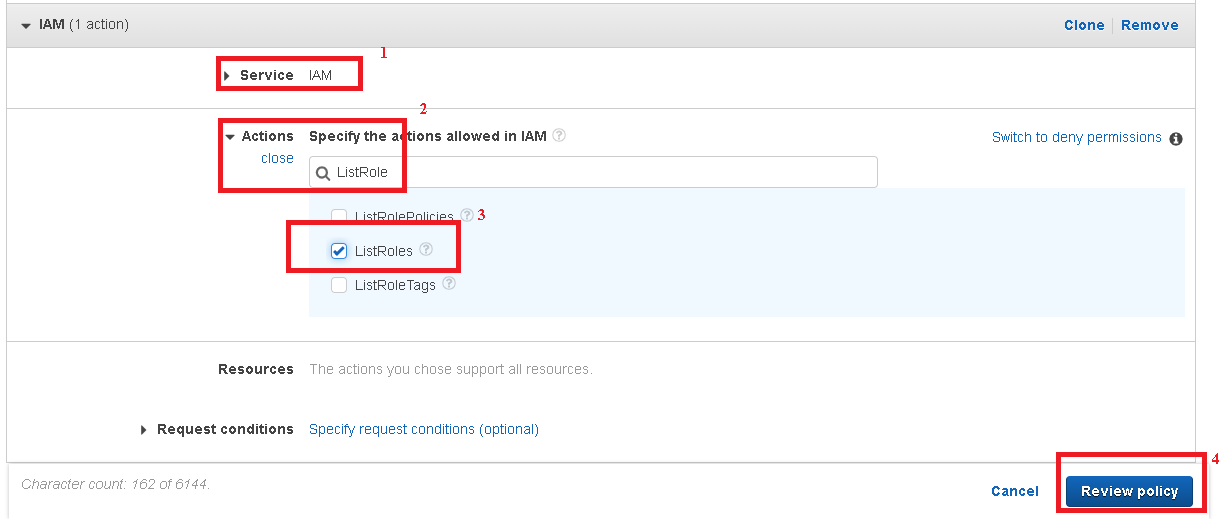
## Create a policy

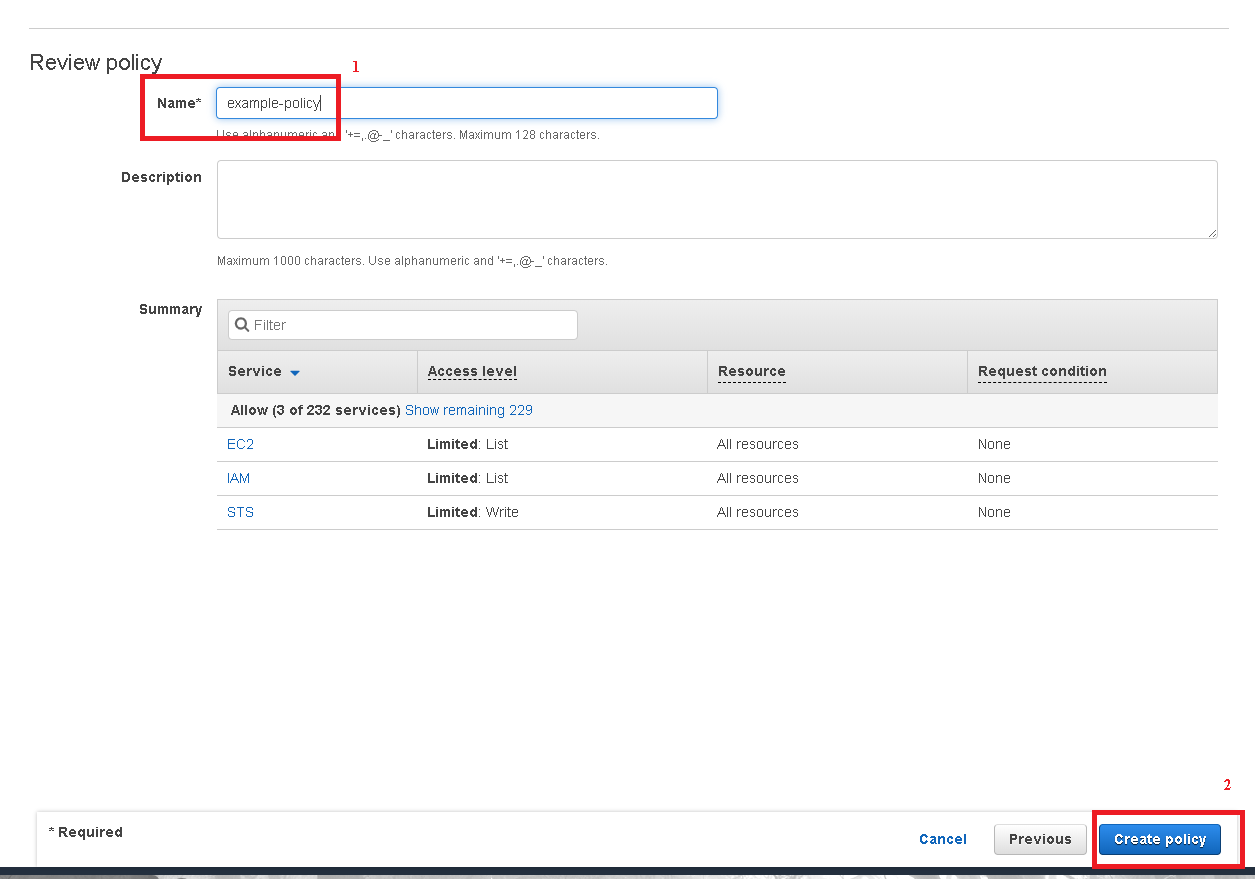


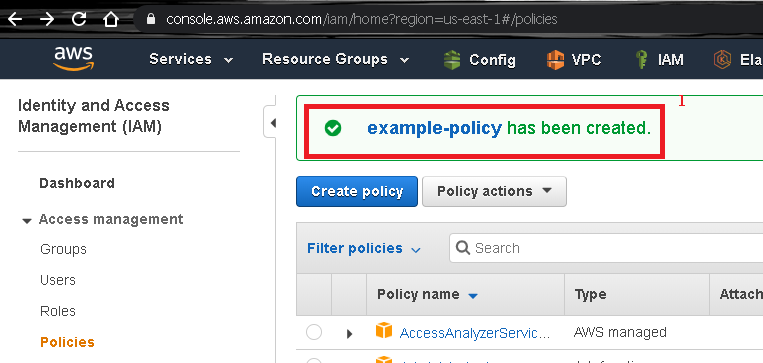


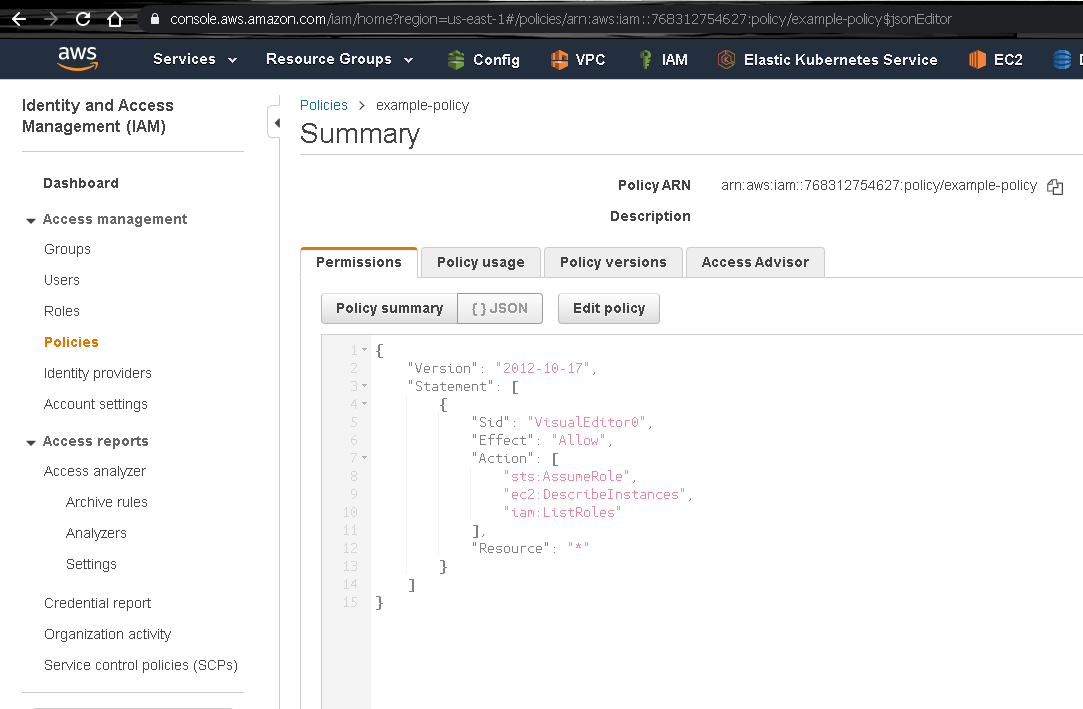




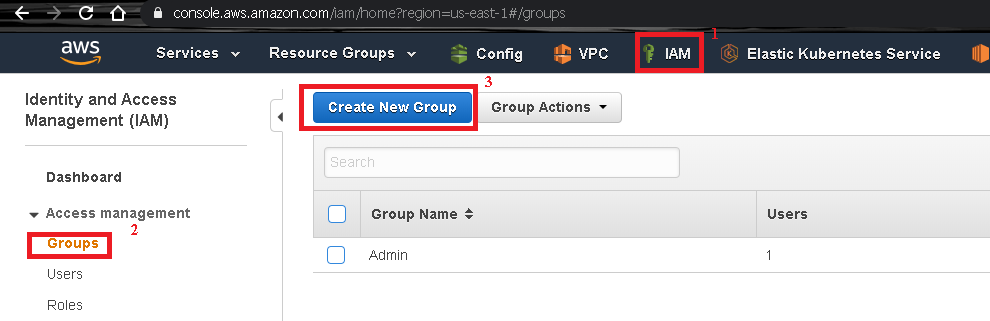


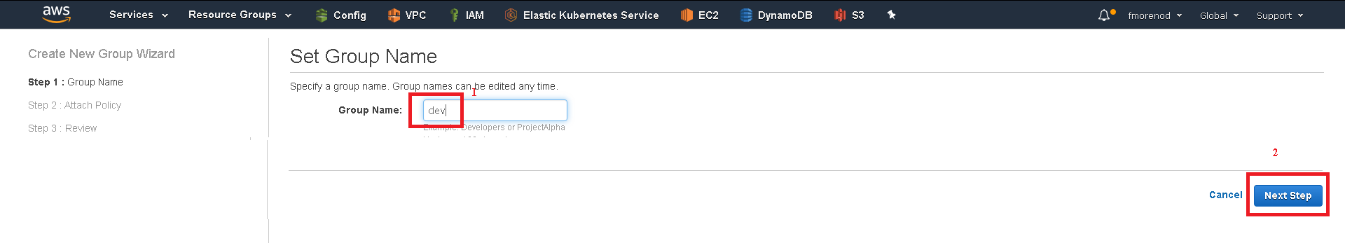


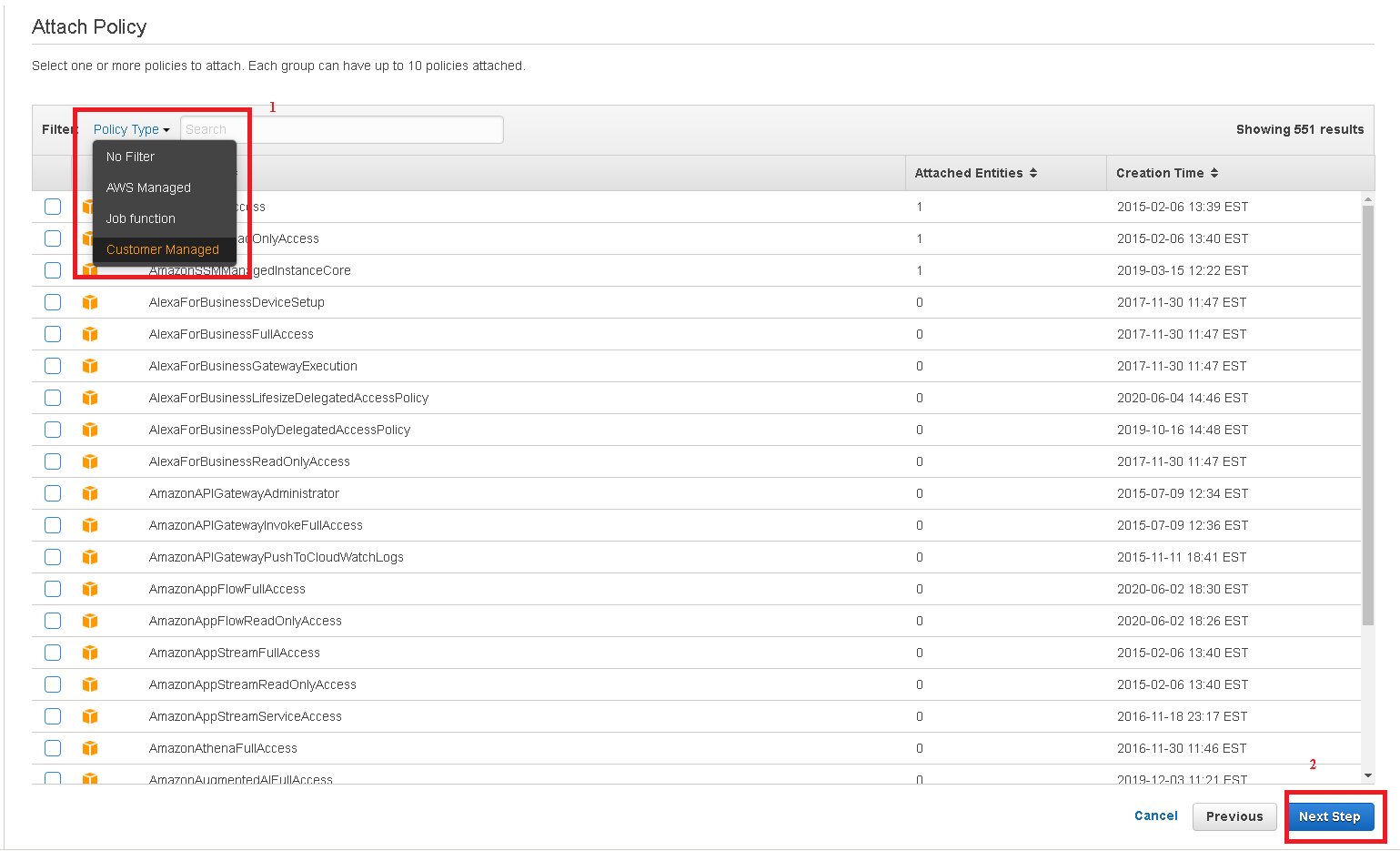


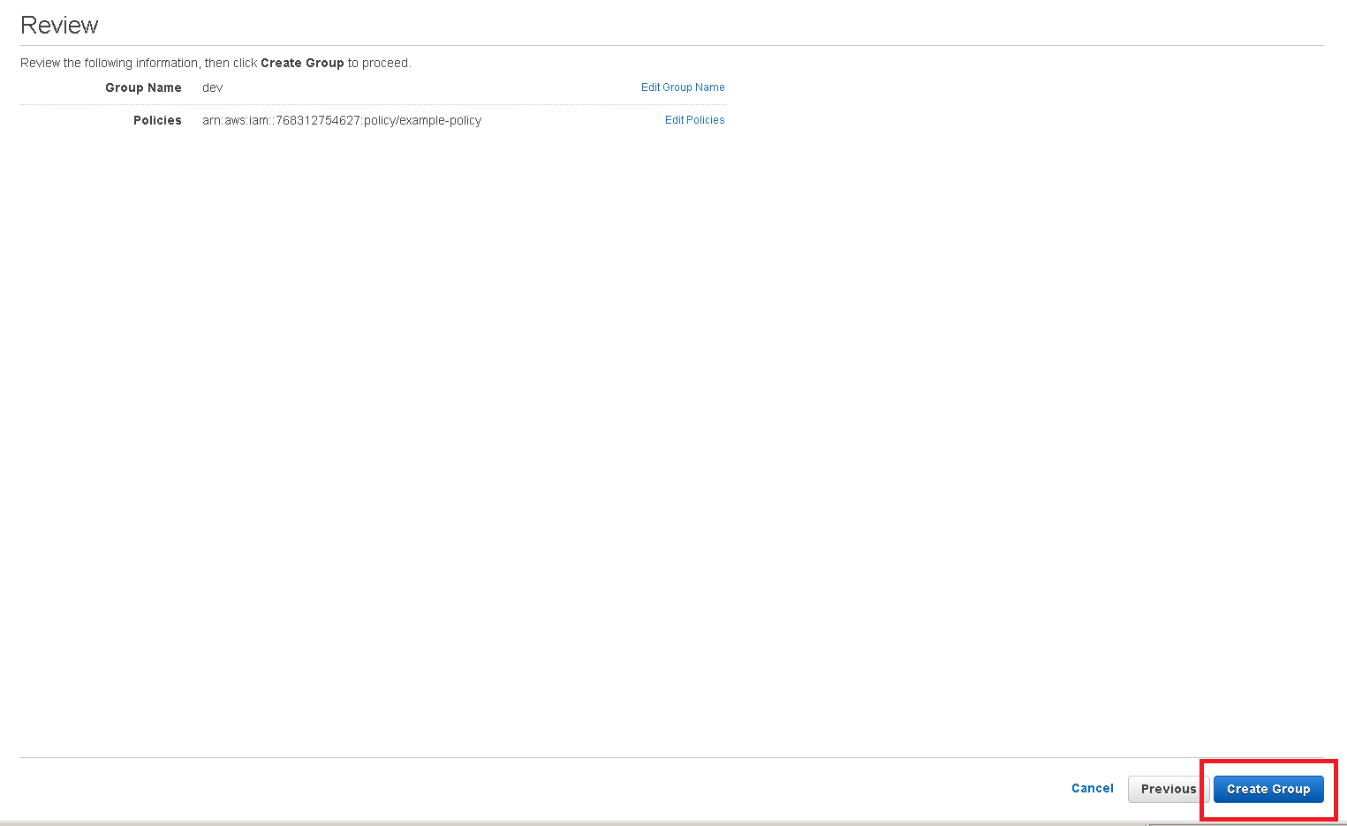
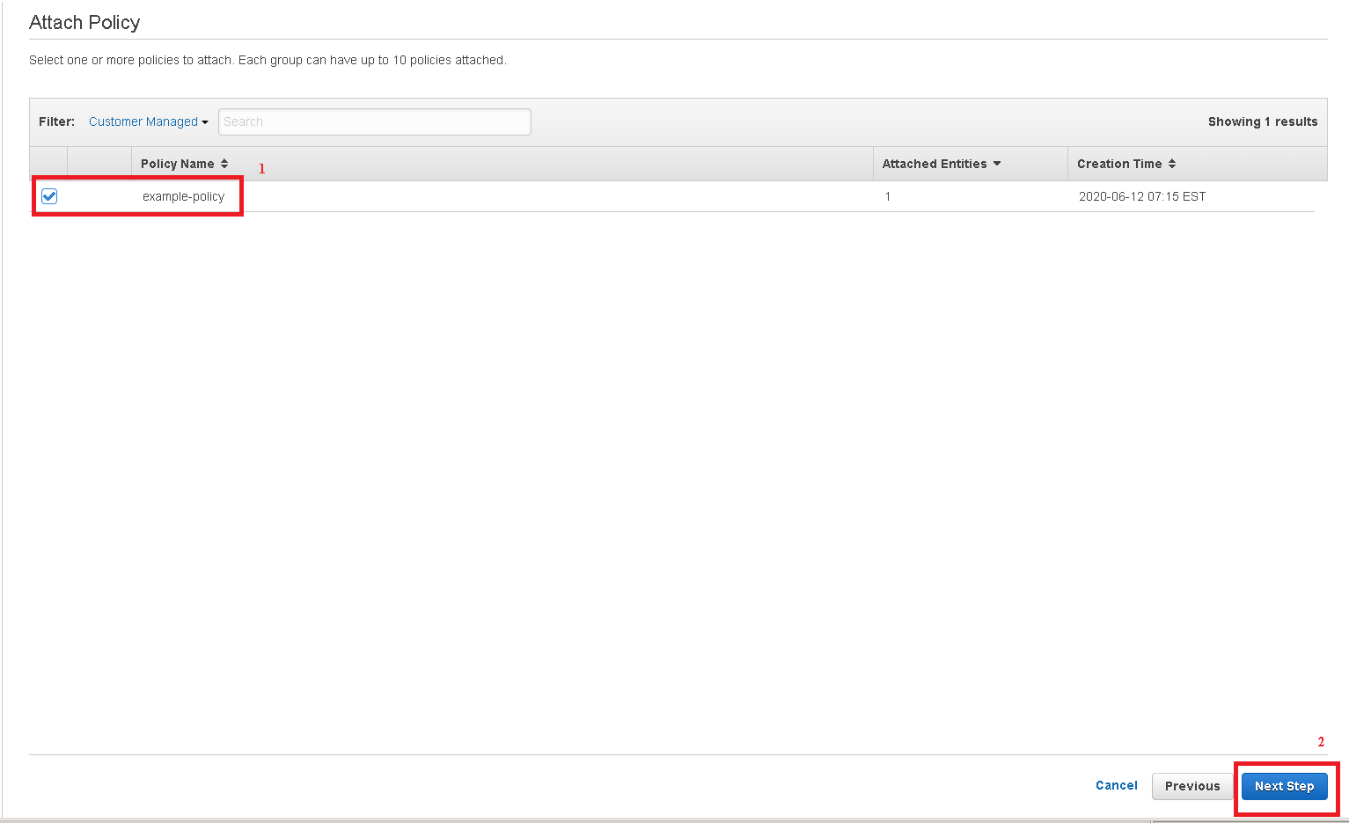


## Create group and attached a policy

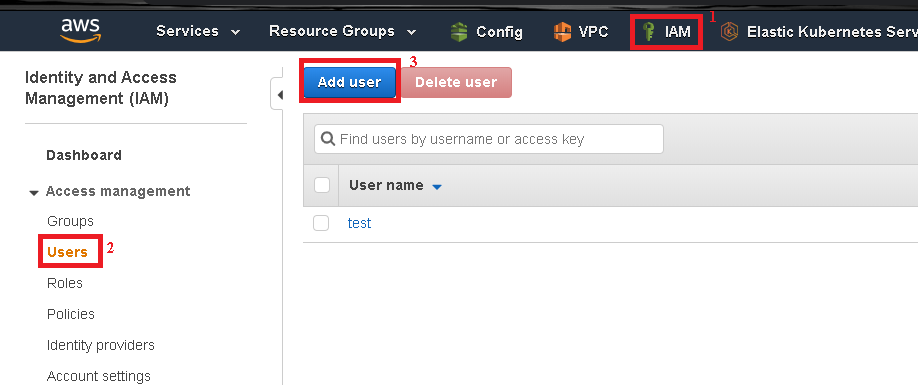


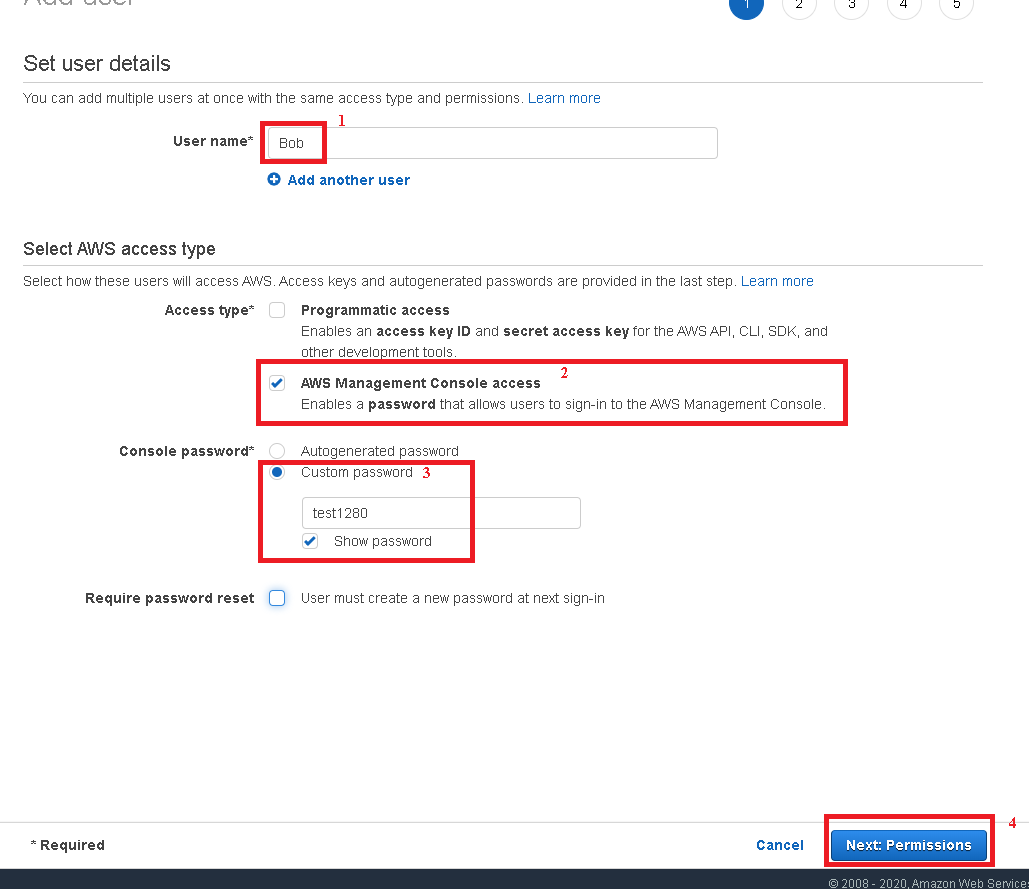


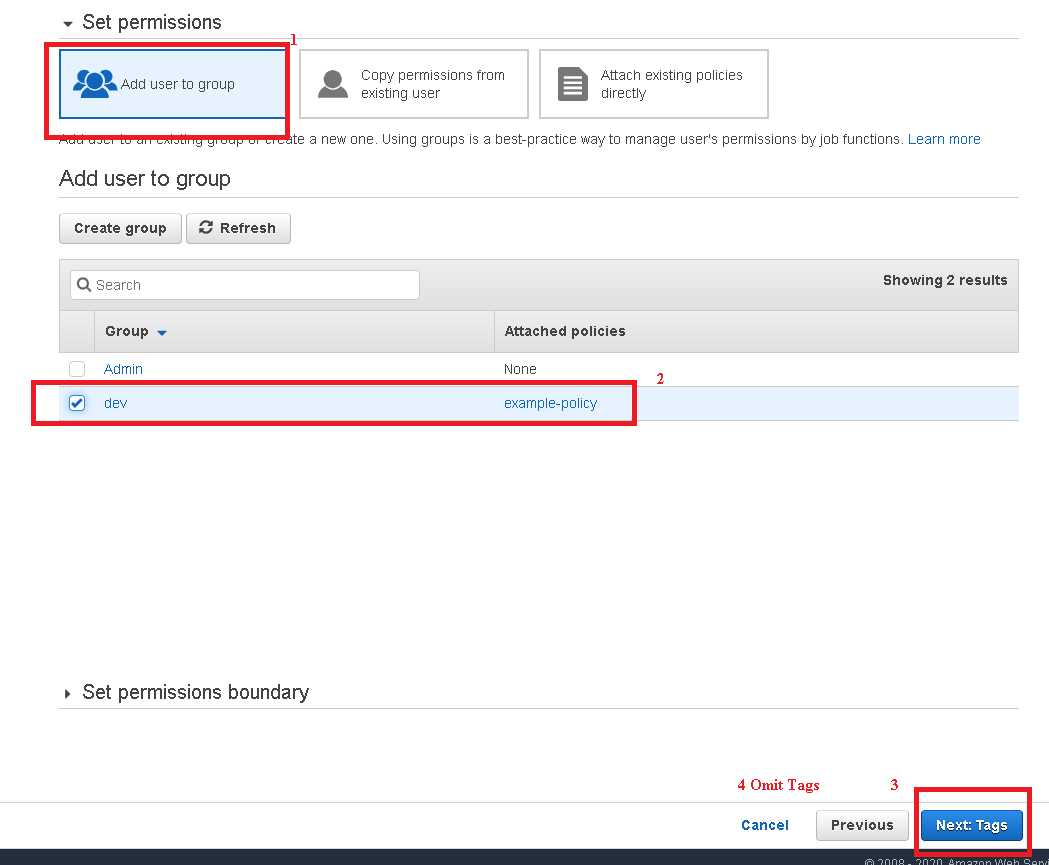


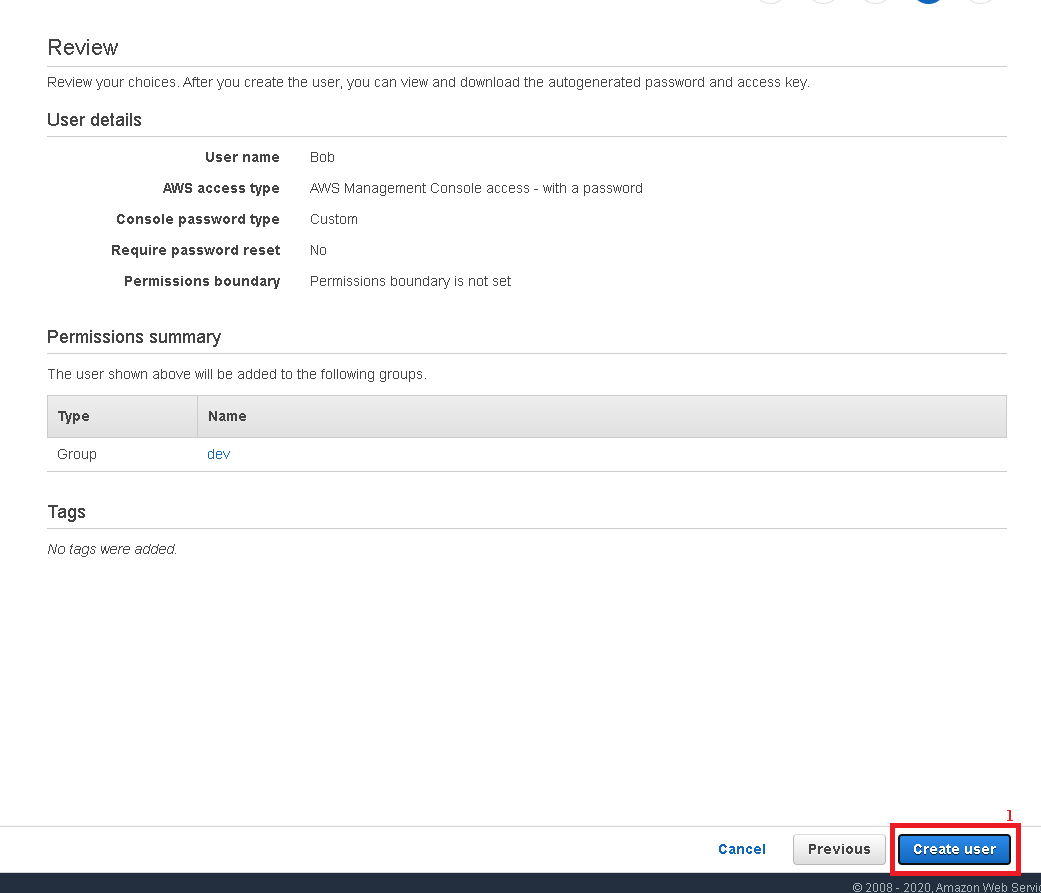


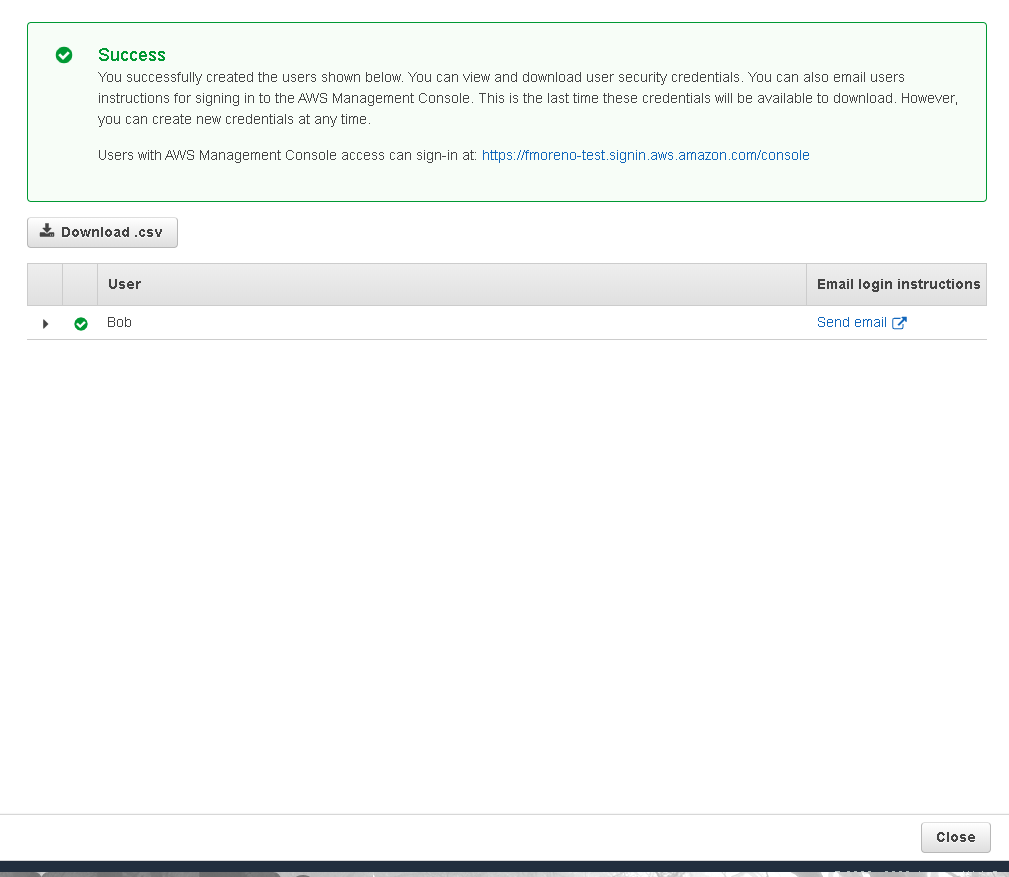
## Create user and attached to the group



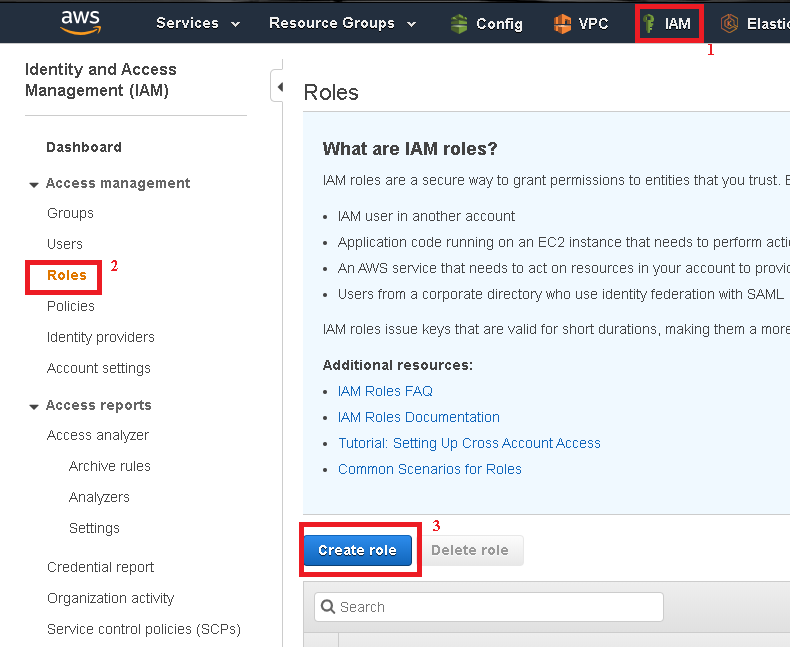


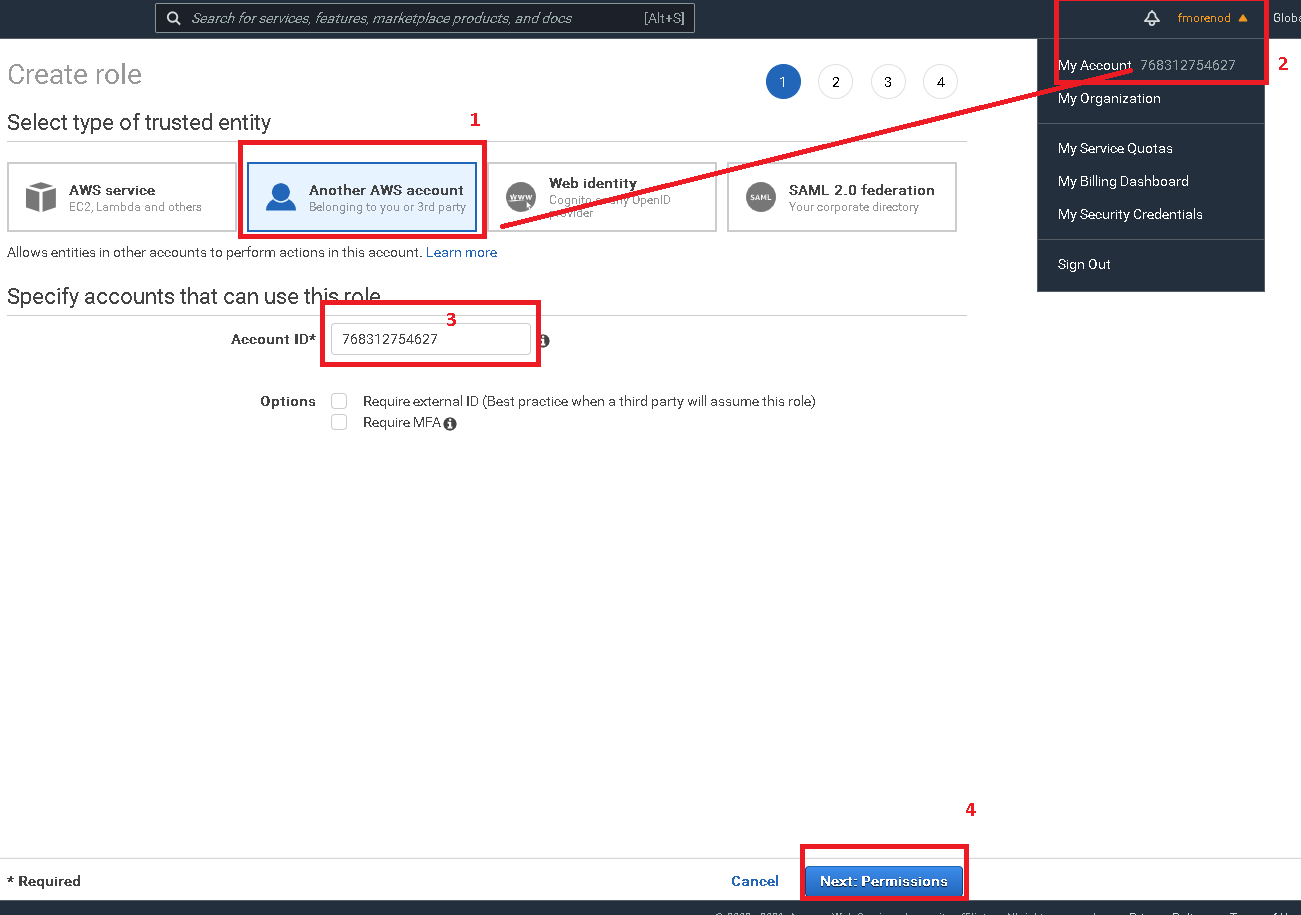


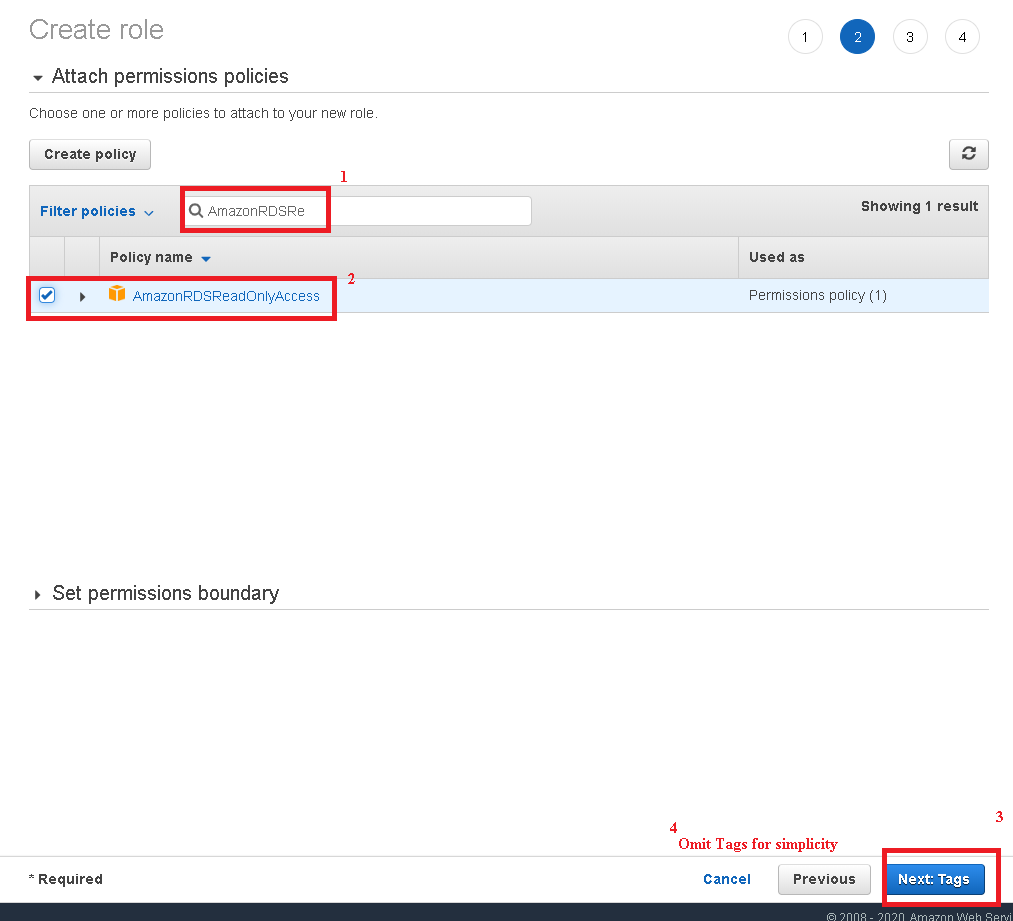


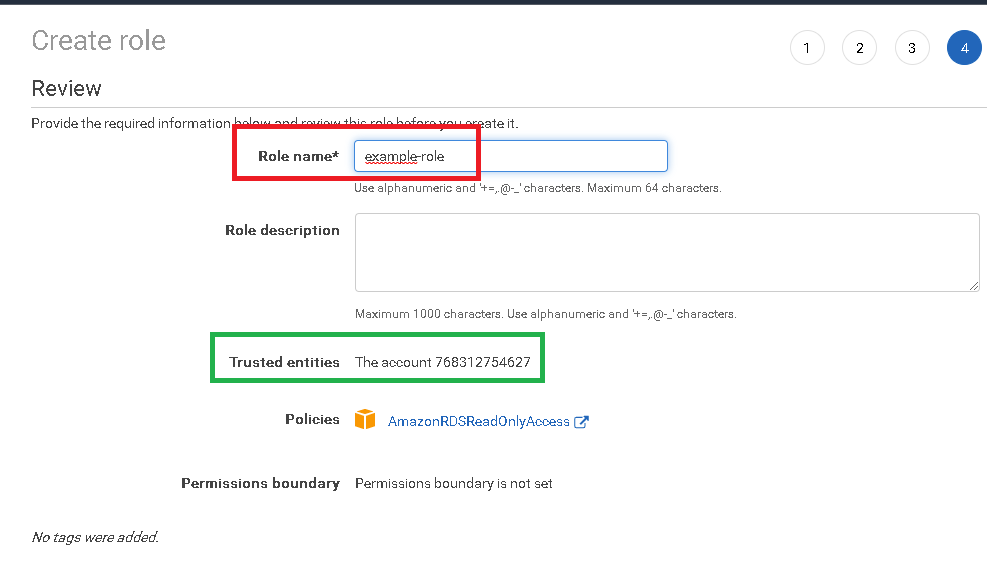


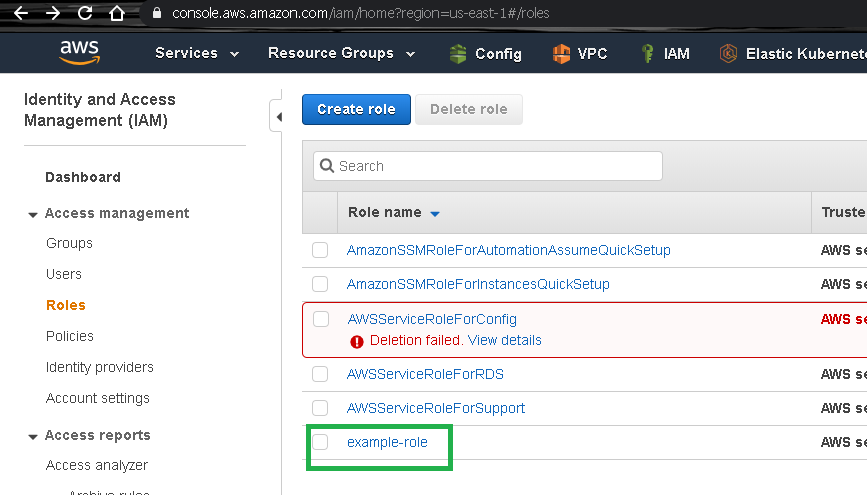
## Create a role and apply an aws-managed policy





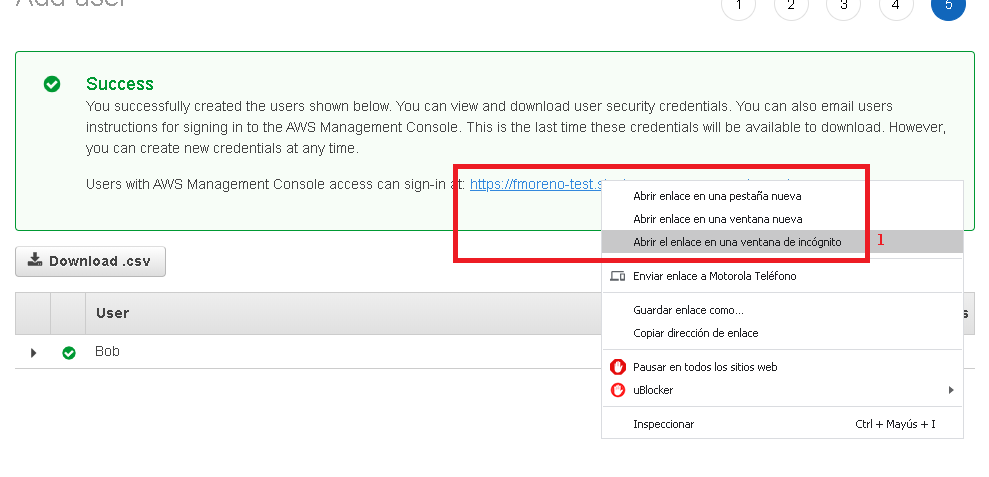


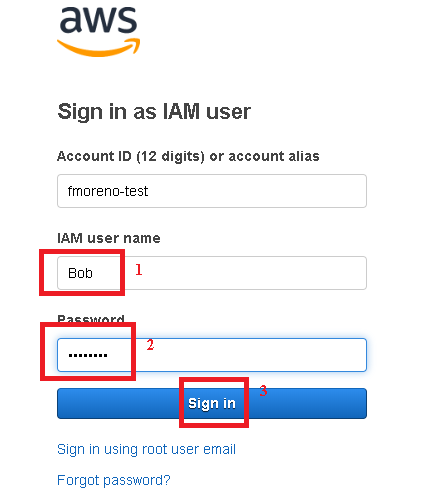




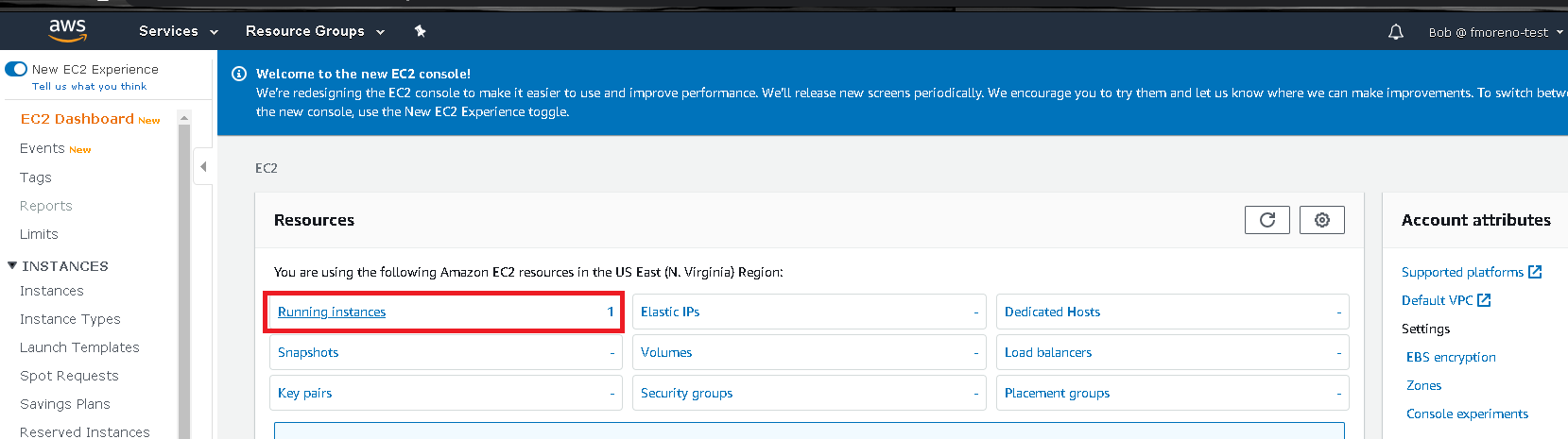
Click on example-role

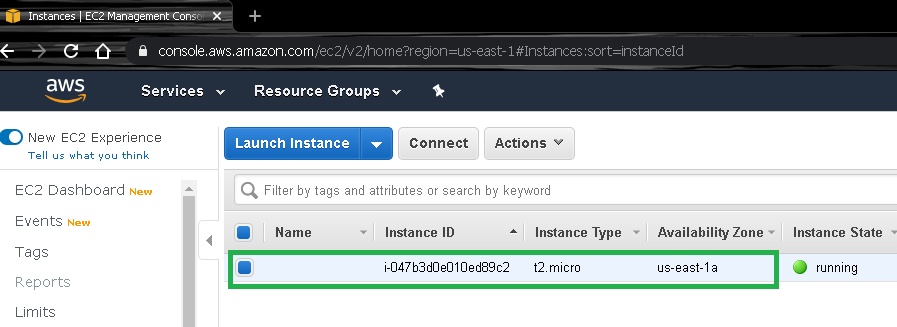
## Login to User Web Console new user and assume roles

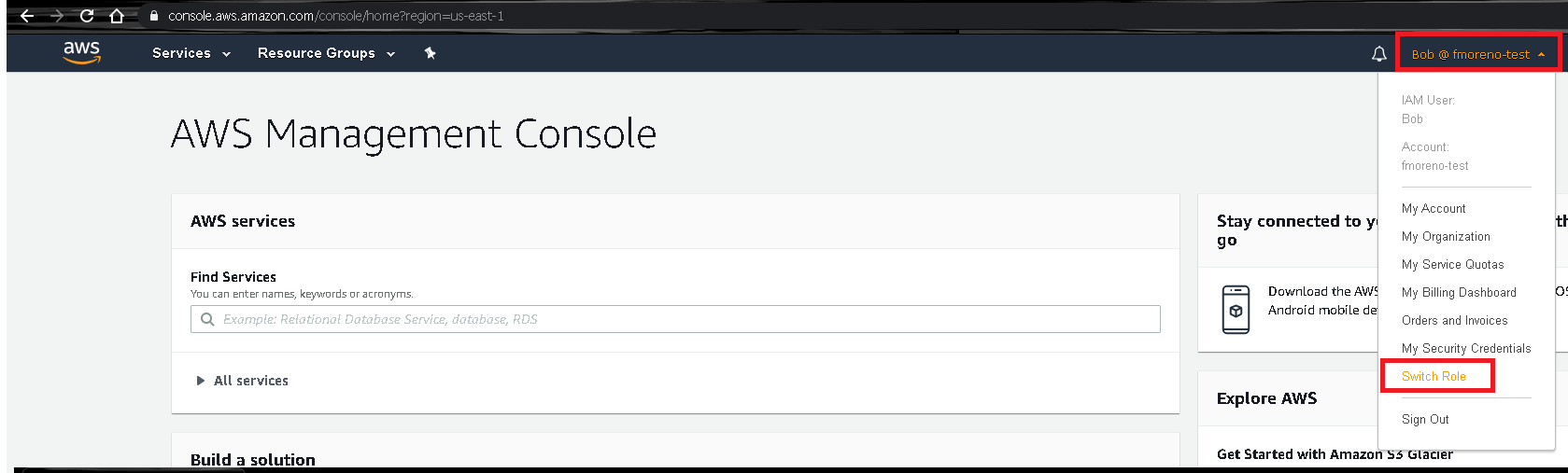


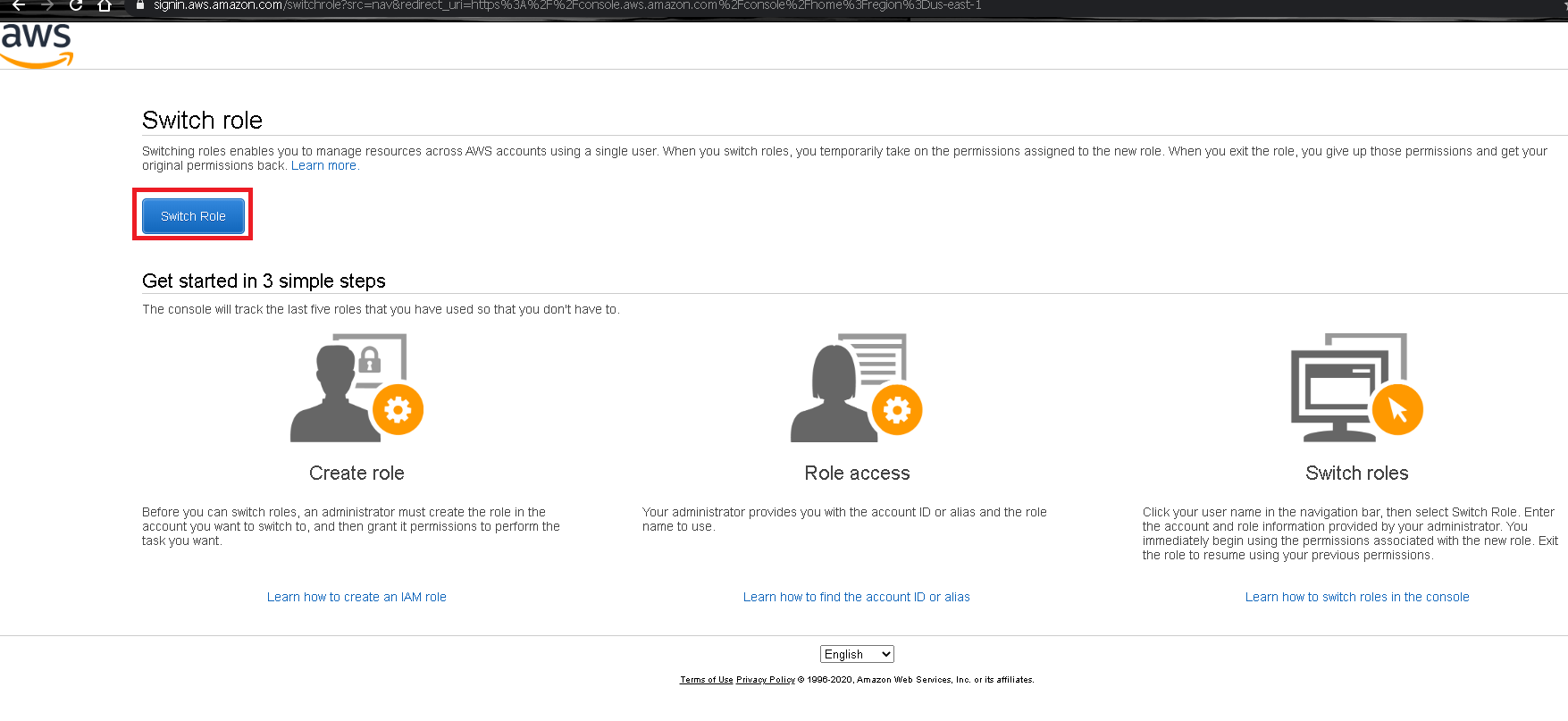


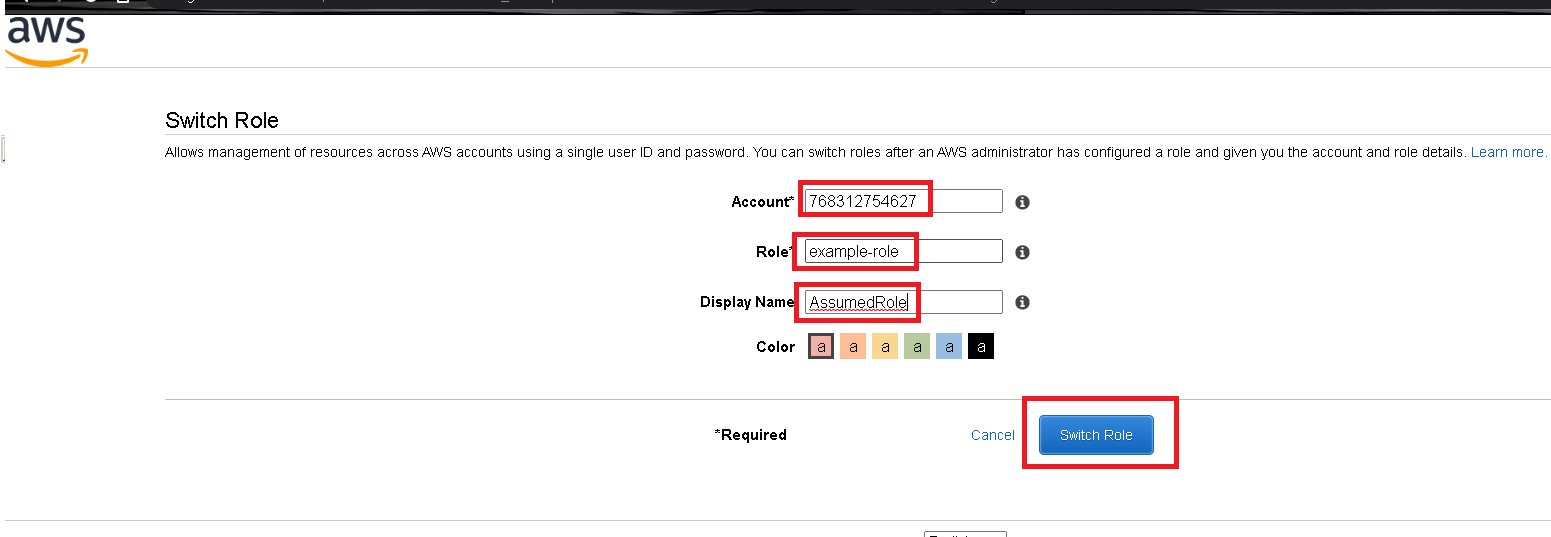
After entered to Web Management Console, go to EC2 Services and then:

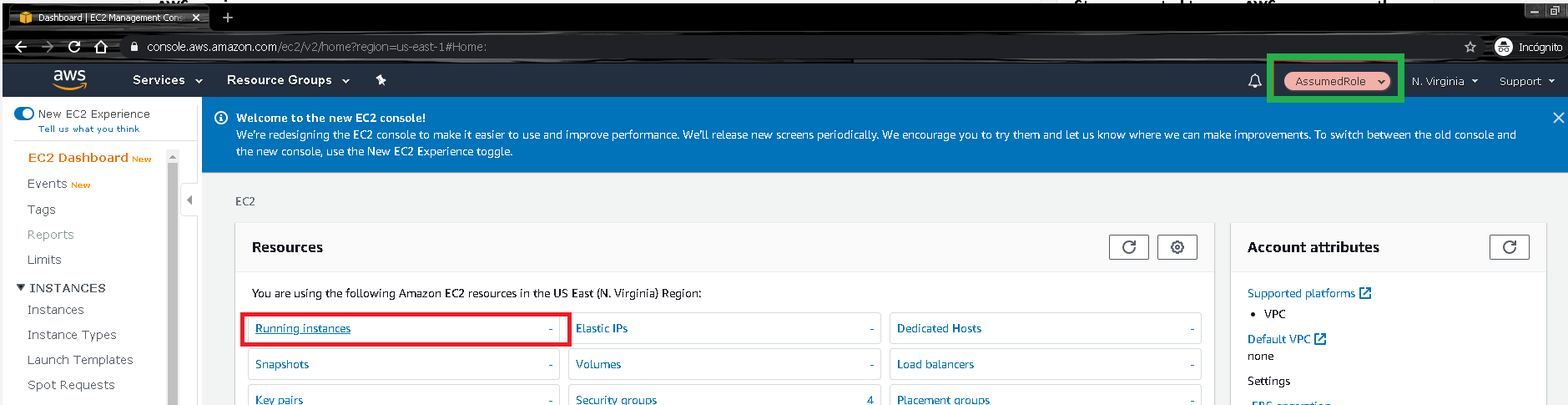


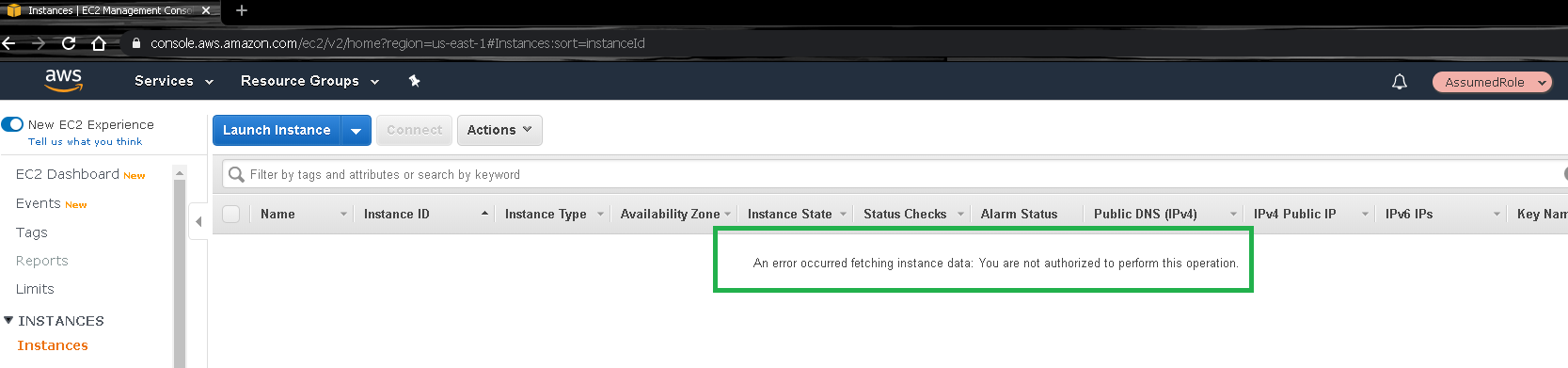


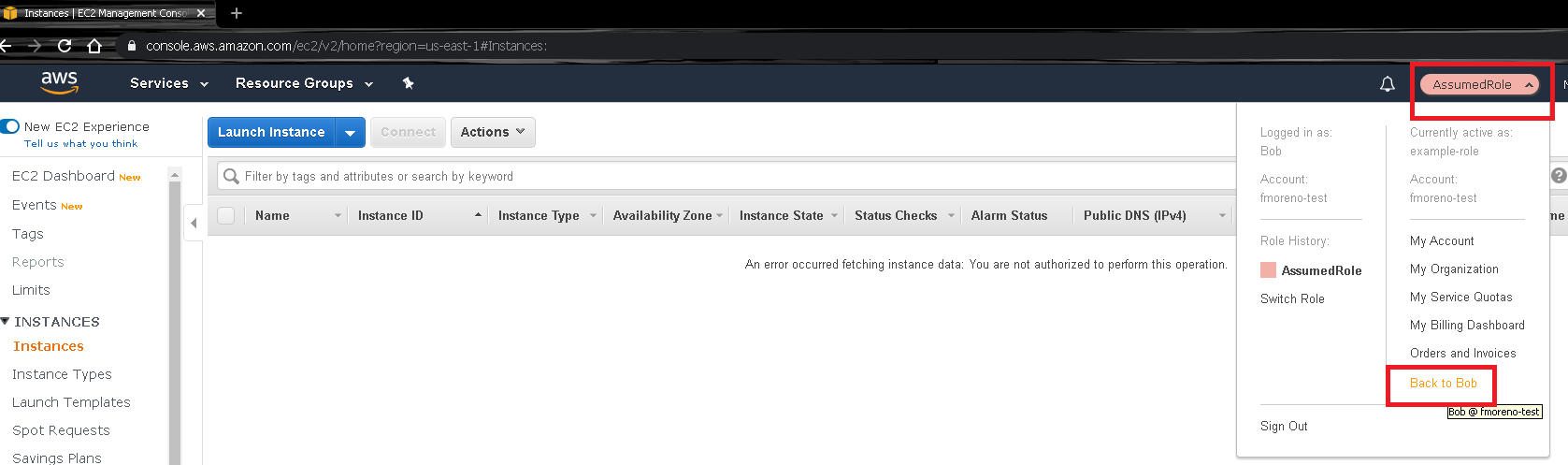












# Lab 2 using Command Line (Windows)

## Create group, user and attached to the group

rem Crear un grupo

aws iam create-group --group-name Dev

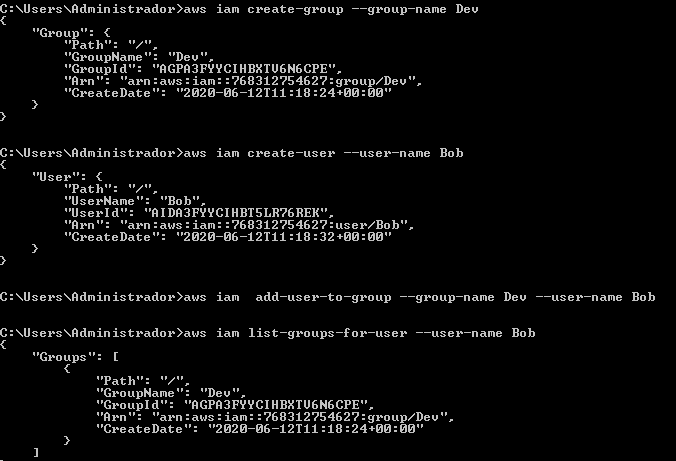
rem Crear los usuarios

aws iam create-user --user-name Bob

rem Agregar usuarios al grupo

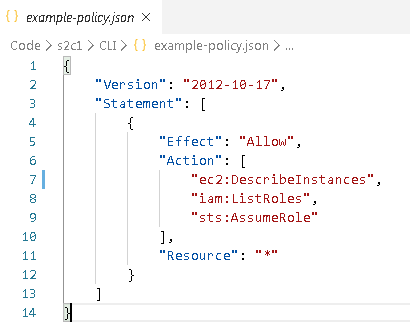
aws iam  add-user-to-group --group-name Dev --user-name Bob

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



## 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 cuenta debido a que puede ser diferente

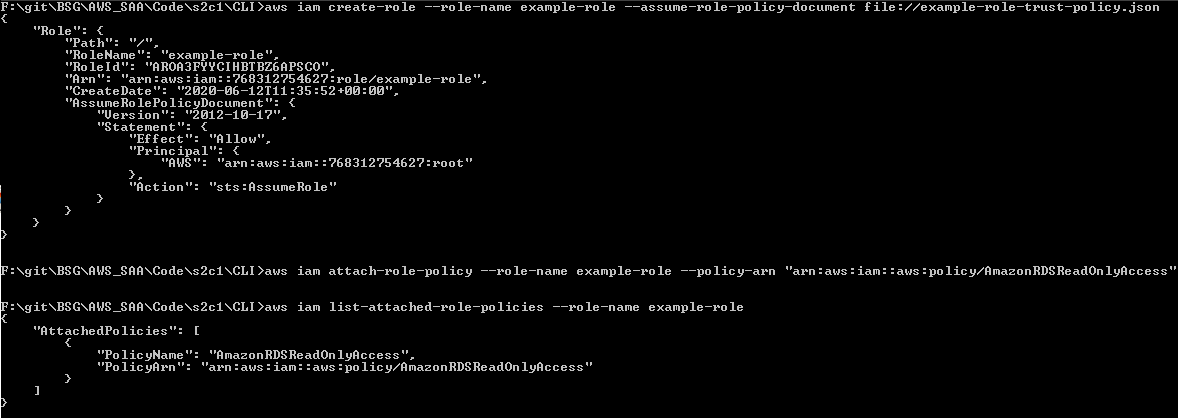
aws iam create-role --role-name example-role --assume-role-policy-document file://example-role-trust-policy.json

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

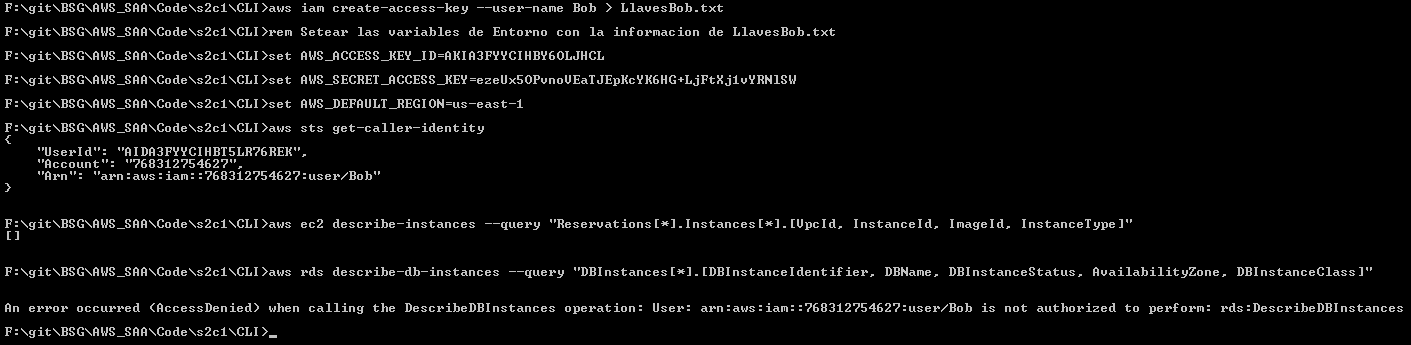
rem Revisar que se esten ejecutando como Bob

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, InstanceType]"

aws rds describe-db-instances --query "DBInstances[\*].[DBInstanceIdentifier, DBName, DBInstanceStatus, AvailabilityZone, 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

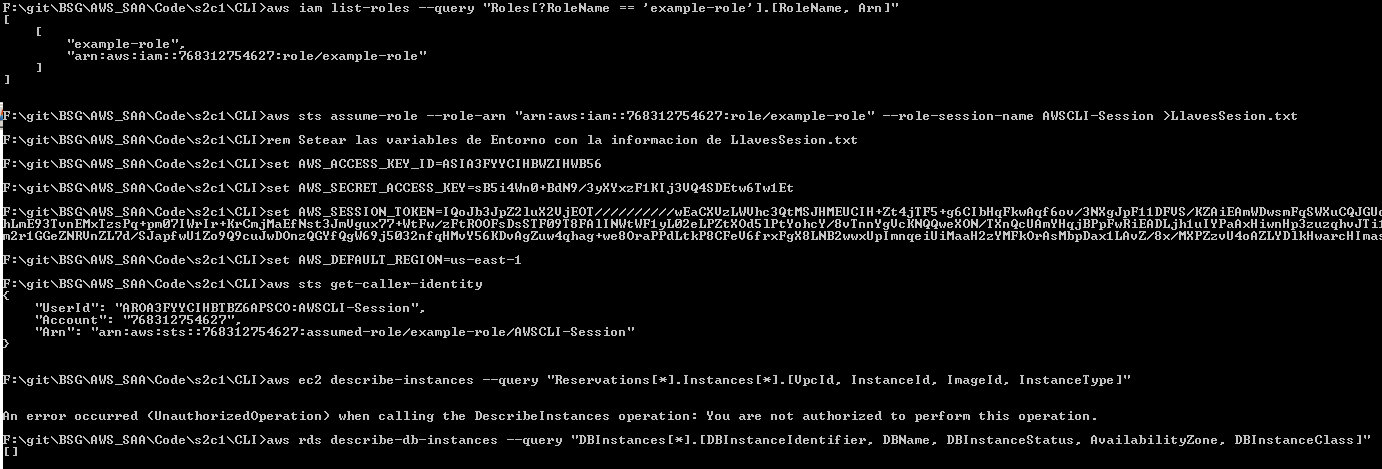
rem Verificar que esta ejecutando el usuario adecuado

aws sts get-caller-identity

rem Volver a ejecutar el listado de acciones

aws ec2 describe-instances --query "Reservations[\*].Instances[\*].[VpcId, InstanceId, ImageId, InstanceType]"

aws rds describe-db-instances --query "DBInstances[\*].[DBInstanceIdentifier, DBName, DBInstanceStatus, AvailabilityZone, 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](#_Login_to_User) (For Web Management Console) or the last 2 screens for [Assume role and check new policy](#_Assume_role_and) (For CLI).