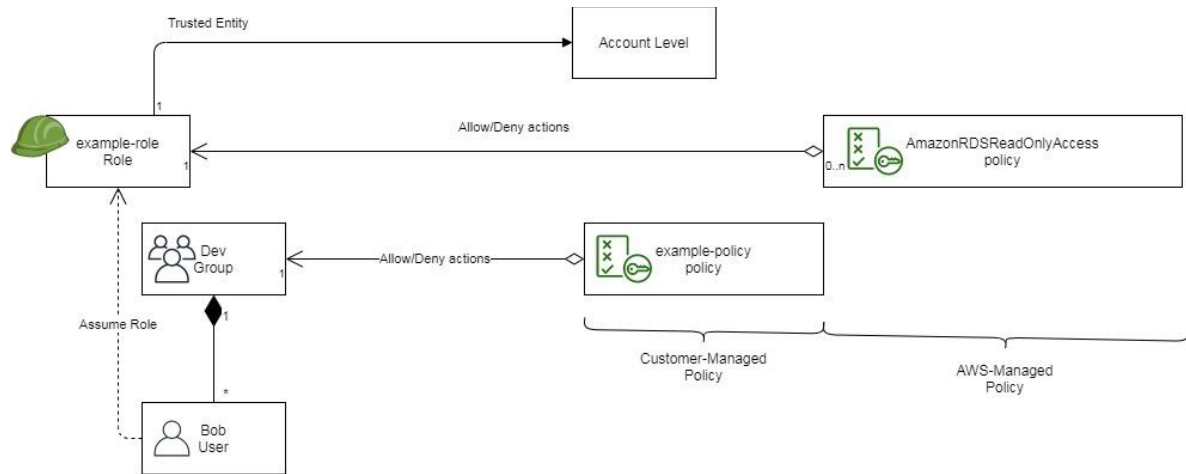


Contents

Purpose	2
Prerequisites	2
Lab 2 using Web Management Console	3
Create a policy.....	3
Create group and attached a policy.....	6
Create user and attached to the group	9
Create a role and apply an aws-managed policy	13
Login to User Web Console new user and assume roles	17
Lab 2 using Command Line (Windows).....	21
Create group, user and attached to the group	21
Predefined files	21
Create a policy and attached it to the group	23
Create a role, apply policy to assume role and attached an aws-managed policy	24
Create keys for user and check applied policy.....	25
Assume role and check new policy	25
Evidences to send.....	26

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.

Create a policy

The screenshot shows the AWS IAM console interface. The top navigation bar includes links for Services, Resource Groups, Config, VPC, IAM (highlighted with a red box and '1'), and ElastiCache. The left sidebar shows the 'Identity and Access Management (IAM)' section with a 'Policies' link highlighted by a red box and '2'. The main content area displays the 'Create policy' button, which is highlighted with a red box and '3', and a table of existing policies.

	Policy name	Type	Attac
<input type="radio"/>	AccessAnalyzerService...	AWS managed	
<input type="radio"/>	AdministratorAccess	Job function	
<input type="radio"/>	AlexaForBusinessDevi...	AWS managed	
<input type="radio"/>	AlexaForBusinessFullA...	AWS managed	
<input type="radio"/>	AlexaForBusinessGate...	AWS managed	

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 using JSON. [Learn more](#)

Visual editor JSON [Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ EC2

▼ Service **Select a service below** [Enter service manually](#)

close

Q ec2

EC2

Amazon EC2

EC2 Image Builder EC2 Messages EC2 Instance Connect

► Actions [Select actions](#)

Resources

Choose actions before applying resources

Request conditions

Choose actions before specifying conditions

[Add additional permissions](#)

Expand all Collapse all

EC2 (1 action)

Clone Remove

Service

EC2

Actions

Specify the actions allowed in EC2 ?

Switch to deny permissions ?

close

DescribeInstances

DescribeInstanceAttribute ?

DescribeInstances ?

DescribeInstanceTypes ?

DescribeInstanceCreditSpecification ?

DescribeInstanceStatus ?

DescribeInstanceEventNotification ?

DescribeInstanceTypeOfferings ?

Resources

The actions you chose support all resources.

Request conditions

Specify request conditions (optional)

Add additional permissions

Service

EC2

Actions

Specify the actions allowed in EC2 ?

Switch to deny permissions ?

close

DescribeInstances

DescribeInstanceAttribute ?

DescribeInstances ?

DescribeInstanceTypes ?

DescribeInstanceCreditSpecification ?

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

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

Service IAM

Actions Specify the actions allowed in IAM ?

Switch to deny permissions ?

close

ListRole

ListRolePolicies ?

ListRoles ?

ListRoleTags ?

Resources The actions you chose support all resources.

Request conditions Specify request conditions (optional)

Character count: 162 of 6144.

Cancel Review policy

Review policy

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

* Required

Cancel

Previous

Create policy

← → ↻ 🏠 console.aws.amazon.com/iam/home?region=us-east-1#/policies

aws Services ▾ Resource Groups ▾ Config VPC IAM El

Identity and Access Management (IAM)

Dashboard

▼ Access management

- Groups
- Users
- Roles
- Policies**

✔ example-policy has been created.

Create policy Policy actions ▾

Filter policies ▾ 🔍 Search

	Policy name ▾	Type	Attach
○ ▶	AccessAnalyzerServic...	AWS managed	

← → ↻ 🏠 console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn:aws:iam::768312754627:policy/example-policy\$jsonEditor

aws Services ▾ Resource Groups ▾ Config VPC IAM Elastic Kubernetes Service EC2

Identity and Access Management (IAM)

Dashboard

▼ Access management

- Groups
- Users
- Roles
- Policies**

Identity providers

Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Policies > example-policy

Summary

Policy ARN [arn:aws:iam::768312754627:policy/example-policy](#)

Description

Permissions Policy usage Policy versions Access Advisor

Policy summary {} JSON Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "sts:AssumeRole",
9         "ec2:DescribeInstances",
10        "iam:ListRoles"
11      ],
12       "Resource": "*"
13     }
14   ]
15 }
```

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

Identity and Access Management (IAM)

Create New Group Group Actions

Dashboard

Access management

Groups Users Roles

Search

<input type="checkbox"/>	Group Name ↕	Users
<input type="checkbox"/>	Admin	1

aws Services Resource Groups Config VPC IAM Elastic Kubernetes Service EC2 DynamoDB S3

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

Cancel **Next Step**

Attach Policy

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

Showing 551 results

Filter: Policy Type Search

No Filter
AWS Managed
Customer Managed

<input type="checkbox"/>		Attached Entities ↕	Creation Time ↕
<input type="checkbox"/>	AmazonEC2FullAccess	1	2015-02-06 13:39 EST
<input type="checkbox"/>	AmazonEKSFullAccess	1	2015-02-06 13:40 EST
<input type="checkbox"/>	AmazonSSMManagedInstanceCore	1	2019-03-15 12:22 EST
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	2017-11-30 11:47 EST
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 11:47 EST
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	2017-11-30 11:47 EST
<input type="checkbox"/>	AlexaForBusinessLifeSizeDelegatedAccessPolicy	0	2020-06-04 14:46 EST
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	0	2019-10-16 14:48 EST
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	2017-11-30 11:47 EST
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	2015-07-09 12:34 EST
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 12:36 EST
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	0	2015-11-11 18:41 EST
<input type="checkbox"/>	AmazonAppFlowFullAccess	0	2020-06-02 18:30 EST
<input type="checkbox"/>	AmazonAppFlowReadOnlyAccess	0	2020-06-02 18:26 EST
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-06 13:40 EST
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	2015-02-06 13:40 EST
<input type="checkbox"/>	AmazonAppStreamServiceAccess	0	2016-11-18 23:17 EST
<input type="checkbox"/>	AmazonAthenaFullAccess	0	2016-11-30 11:46 EST
<input type="checkbox"/>	AmazonAugmentedAIRuntimeFullAccess	0	2019-12-03 11:21 EST

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 ▾

Showing 1 results

	Policy Name ↕	Attached Entities ▾	Creation Time ↕
<input checked="" type="checkbox"/>	example-policy	1	2020-06-12 07:15 EST

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

The screenshot shows the AWS IAM console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', 'Config', 'VPC', 'IAM' (highlighted with a red box and number 1), and 'Elastic Kubernetes Serv...'. The left sidebar shows 'Identity and Access Management (IAM)' with a sub-menu 'Access management' containing 'Groups', 'Users' (highlighted with a red box and number 2), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The main content area has 'Add user' (highlighted with a red box and number 3) and 'Delete user' buttons. Below these is a search bar 'Find users by username or access key' and a list of users with 'test' visible. A progress indicator at the bottom shows steps 1 through 5, with step 1 being the current step.

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [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** ²
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ **Custom password** ³

☒ Show password

Require password reset ☐ User must create a new password at next sign-in

* Required

Cancel [Next: Permissions](#) ⁴

© 2008 - 2020, Amazon Web Services

▼ 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 functions. [Learn more](#)

Add user to group

Create group

Refresh

Search

Showing 2 results

Group ▼	Attached policies
<input type="checkbox"/> Admin	None
<input checked="" type="checkbox"/> dev	example-policy

► Set permissions boundary

4 Omit Tags

3

Cancel

Previous

Next: Tags

© 2008 – 2020 Amazon Web Services

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.

[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.

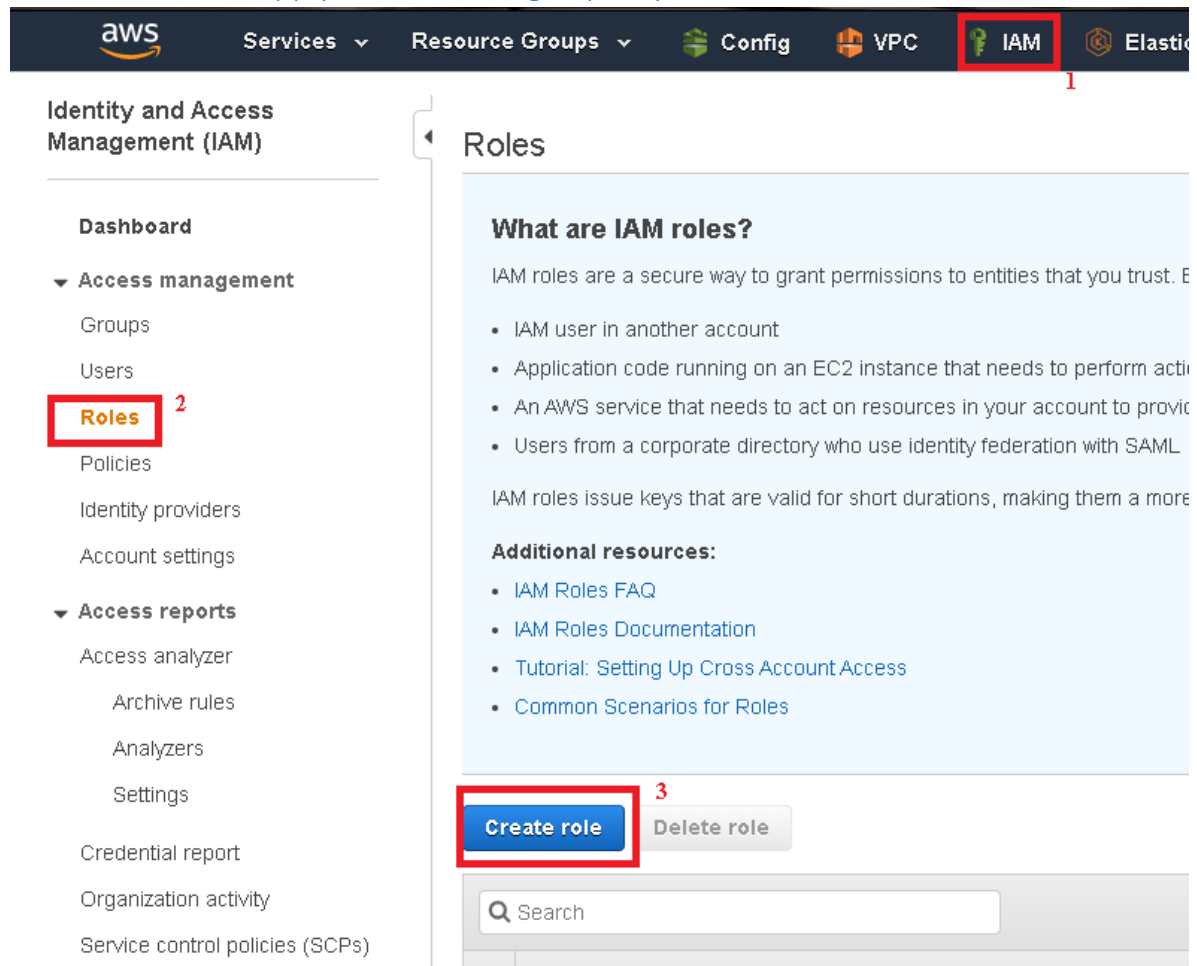
Users with AWS Management Console access can sign-in at: <https://fmoreno-test.signin.aws.amazon.com/console>

 **Download .csv**

	User	Email login instructions
▶ 	Bob	Send email 

Close

Create a role and apply an aws-managed policy



The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo and links to Services, Resource Groups, Config, VPC, IAM (highlighted with a red box and labeled 1), and Elastic. The left sidebar, titled 'Identity and Access Management (IAM)', contains a 'Dashboard' section and two main categories: 'Access management' and 'Access reports'. Under 'Access management', 'Roles' is highlighted with a red box and labeled 2. The main content area, titled 'Roles', features a section 'What are IAM roles?' which explains that IAM roles are a secure way to grant permissions to entities that you trust. It lists four use cases: IAM user in another account, application code running on an EC2 instance, an AWS service that needs to act on resources, and users from a corporate directory. Below this, 'Additional resources' are listed, including IAM Roles FAQ, IAM Roles Documentation, Tutorial: Setting Up Cross Account Access, and Common Scenarios for Roles. At the bottom of the main content area, the 'Create role' button is highlighted with a red box and labeled 3, next to a 'Delete role' button. A search bar is also visible at the bottom of the console.

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. E

- IAM user in another account
- Application code running on an EC2 instance that needs to perform acti
- An AWS service that needs to act on resources in your account to provi
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

Create role **Delete role**

Q Search

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

Create role

1

2

3

4

Select type of trusted entity

AWS service

EC2, Lambda and others

Another AWS account

Belonging to you or 3rd party

Web identity

Cognito, many OpenID providers

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

Account ID*

768312754627

Options

☐

Require external ID (Best practice when a third party will assume this role)

☐

Require MFA

* 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 ↺

Filter policies ▼

1

Showing 1 result

	Policy name ▼	Used as
2 <input checked="" type="checkbox"/>	 AmazonRDSReadOnlyAccess	Permissions policy (1)

► Set permissions boundary

* Required

4 Omit Tags for simplicity

Cancel

Previous

3 Next: Tags

© 2008 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Create role

1

2

3

4

Review

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

Role name* example-role

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

Role description

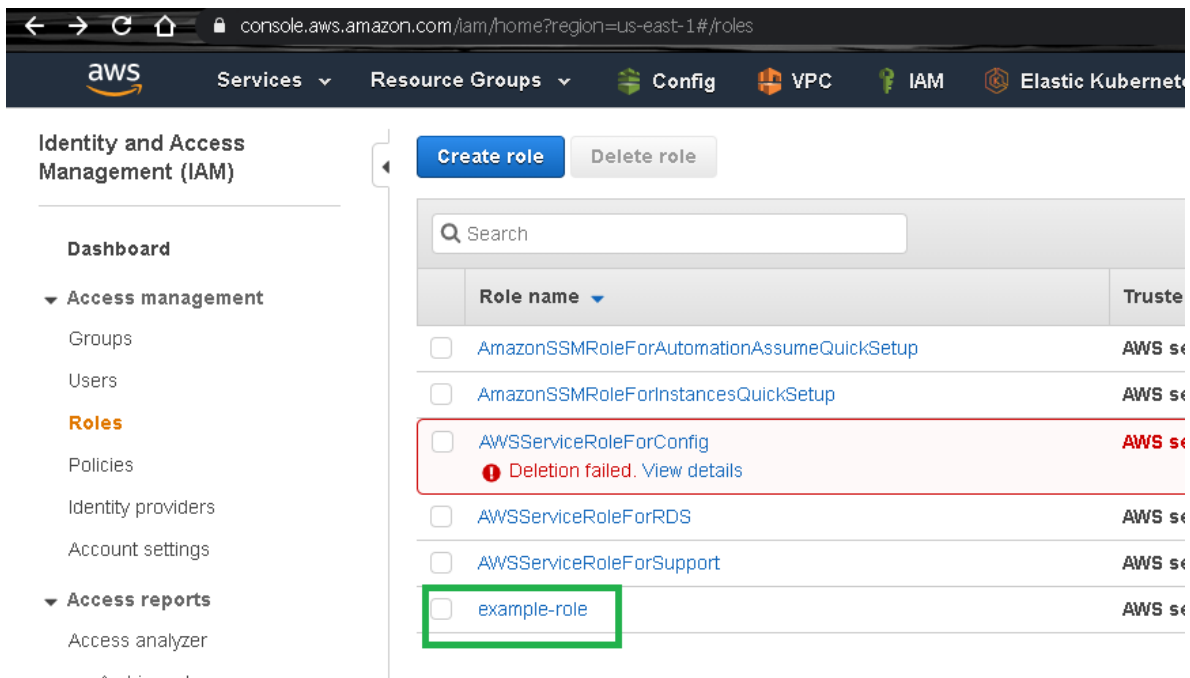
Maximum 1000 characters. Use alphanumeric and '+', '@', '_' characters.

Trusted entities The account 768312754627

Policies  AmazonRDSReadOnlyAccess [↗](#)

Permissions boundary Permissions boundary is not set

No tags were added.



The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', 'Config', 'VPC', 'IAM', and 'Elastic Kubernetes'. The left sidebar shows the 'Identity and Access Management (IAM)' section with a menu including 'Dashboard', 'Access management' (Groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Access advisor), and 'Account settings'. The main content area has 'Create role' and 'Delete role' buttons. Below them is a search bar and a table of roles. The table has columns for 'Role name' and 'Trusted entities'. The roles listed are: 'AmazonSSMRoleForAutomationAssumeQuickSetup' (AWS s4), 'AmazonSSMRoleForInstancesQuickSetup' (AWS s4), 'AWSServiceRoleForConfig' (AWS s4) with a red error message 'Deletion failed. View details', 'AWSServiceRoleForRDS' (AWS s4), 'AWSServiceRoleForSupport' (AWS s4), and 'example-role' (AWS s4). The 'example-role' row is highlighted with a green border.

Role name	Trusted entities
<input type="checkbox"/> AmazonSSMRoleForAutomationAssumeQuickSetup	AWS s4
<input type="checkbox"/> AmazonSSMRoleForInstancesQuickSetup	AWS s4
<input type="checkbox"/> AWSServiceRoleForConfig Deletion failed. View details	AWS s4
<input type="checkbox"/> AWSServiceRoleForRDS	AWS s4
<input type="checkbox"/> AWSServiceRoleForSupport	AWS s4
<input type="checkbox"/> example-role	AWS s4

Click on example-role

/ 144 4001

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://fmoreno-test-1-123456789012.us-east-1.console.aws.amazon.com/>

Download .csv

User
Bob

Context menu options:

- Abrir enlace en una pestaña nueva
- Abrir enlace en una ventana nueva
- Abrir el enlace en una ventana de incógnito
- Enviar enlace a Motorola Teléfono
- Guardar enlace como...
- Copiar dirección de enlace
- Pausar en todos los sitios web
- uBlocker
- Inspeccionar



Sign in as IAM user

Account ID (12 digits) or account alias

fmoreno-test

IAM user name

Bob

1

Password

.....

2

Sign in

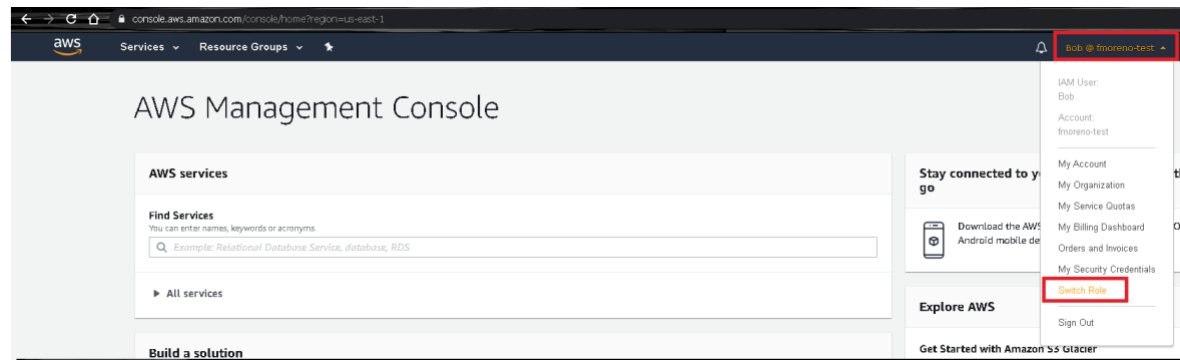
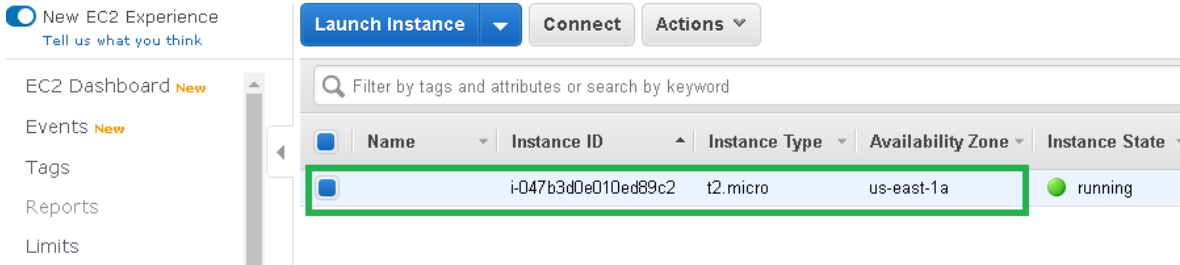
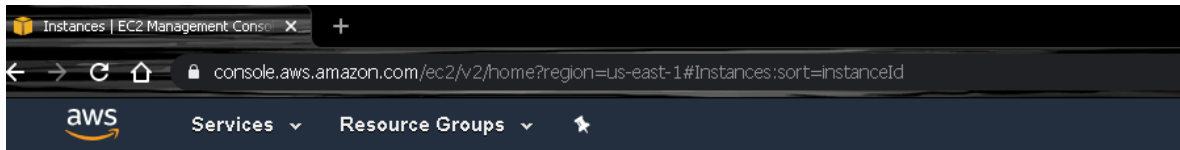
3

[Sign in using root user email](#)

[Forgot password?](#)

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

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'aws' logo, 'Services', 'Resource Groups', and a user profile 'Bob @ fmoreno-test'. Below the navigation bar, there's a 'Welcome to the new EC2 console' message. The main content area is titled 'EC2' and 'Resources'. It states 'You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:'. A table of resources is displayed, with 'Running instances' highlighted by a red box and the number '1'. Other resources listed include Elastic IPs, Dedicated Hosts, Snapshots, Volumes, Load balancers, Key pairs, Security groups, and Placement groups. On the right side, there's a sidebar with 'Account attributes' including 'Supported platforms', 'Default VPC', 'Settings', 'EBS encryption', 'Zones', and 'Console experiments'.



Switch role

Switching roles enables you to manage resources across AWS accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

[Switch Role](#)

Get started in 3 simple steps

The console will track the last five roles that you have used so that you don't have to.



Create role

Before you can switch roles, an administrator must create the role in the account you want to switch to, and then grant it permissions to perform the task you want.

[Learn how to create an IAM role](#)



Role access

Your administrator provides you with the account ID or alias and the role name to use.

[Learn how to find the account ID or alias](#)



Switch roles

Click your user name in the navigation bar, then select Switch Role. Enter the account and role information provided by your administrator. You immediately begin using the permissions associated with the new role. Exit the role to resume using your previous permissions.

[Learn how to switch roles in the console](#)

English

[Terms of the Privacy Policy](#) © 1998-2020, Amazon Web Services, Inc. or its affiliates.

aws

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

a

a

a

a

a

a

*Required

Cancel

Switch Role

Dashboard | EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#home

aws

Services

Resource Groups

AssumedRole

N. Virginia

Support

New EC2 Experience

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Welcome to the new EC2 console!

EC2

Resources

Account attributes

Supported platforms

VPC

Default VPC

none

Settings

Running instances

Elastic IPs

Dedicated Hosts

Snapshots

Volumes

Load balancers

Key pairs

Security groups

4

Placement groups

Instances | EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#instances

aws

Services

Resource Groups

AssumedRole

New EC2 Experience

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

Name

Instance ID

Instance Type

Availability Zone

Instance State

Status Checks

Alarm Status

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

Key Name

An error occurred fetching instance data: You are not authorized to perform this operation.

Instances | EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#instances

aws

Services

Resource Groups

AssumedRole

New EC2 Experience

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

Name

Instance ID

Instance Type

Availability Zone

Instance State

Status Checks

Alarm Status

Public DNS (IPv4)

An error occurred fetching instance data: You are not authorized to perform this operation.

Logged in as: Bob

Account: fmoreno-test

Role History: AssumedRole

Switch Role

Sign Out

Currently active as: example-role

Account: fmoreno-test

My Account

My Organization

My Service Quotas

My Billing Dashboard

Orders and Invoices

Back to Bob

Bob @ fmoreno-test

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

```
C:\Users\Administrador>aws iam create-group --group-name Dev
{
  "Group": {
    "Path": "/",
    "GroupName": "Dev",
    "GroupId": "AGPA3FYVCIHBTU6N6CPE",
    "Arn": "arn:aws:iam::768312754627:group/Dev",
    "CreateDate": "2020-06-12T11:18:24+00:00"
  }
}

C:\Users\Administrador>aws iam create-user --user-name Bob
{
  "User": {
    "Path": "/",
    "UserName": "Bob",
    "UserId": "AIDA3FYVCIHBT5LR76REK",
    "Arn": "arn:aws:iam::768312754627:user/Bob",
    "CreateDate": "2020-06-12T11:18:32+00:00"
  }
}

C:\Users\Administrador>aws iam add-user-to-group --group-name Dev --user-name Bob

C:\Users\Administrador>aws iam list-groups-for-user --user-name Bob
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "Dev",
      "GroupId": "AGPA3FYVCIHBTU6N6CPE",
      "Arn": "arn:aws:iam::768312754627:group/Dev",
      "CreateDate": "2020-06-12T11:18:24+00:00"
    }
  ]
}
```

Predefined files

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

{ } example-policy.json ×

Code > s2c1 > CLI > { } example-policy.json > ...

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:DescribeInstances",
8                  "iam:ListRoles",
9                  "sts:AssumeRole"
10             ],
11             "Resource": "*"
12         }
13     ]
14 }
```

example-policy.json

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

`{}` example-role-trust-policy.json ×

Code > s2c1 > CLI > `{}` example-role-trust-policy.json > ...

```
1  {
2    "Version": "2012-10-17",
3    "Statement": {
4      "Effect": "Allow",
5      "Principal": { "AWS": "arn:aws:iam::768312754627:root" },
6      "Action": "sts:AssumeRole"
7    }
8  }
9  |
```

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": "ANP93FYVC1HBUNBQXKBBN",
    "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": "ANP93FYVC1HBUNBQXKBBN",
      "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 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
```



```

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam create-role --role-name example-role --assume-role-policy-document file://example-role-trust-policy.json
{
  "Role": {
    "Path": "/",
    "RoleName": "example-role",
    "RoleId": "AROA3FYVC1HBT5LR76REX",
    "Arn": "arn:aws:iam::768312754627:role/example-role",
    "CreateDate": "2020-06-12T11:35:52+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::768312754627:root"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}

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

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

```

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]"

```

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws iam create-access-key --user-name Bob > LlavesBob.txt
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>rem Setear las variables de Entorno con la informacion de LlavesBob.txt
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>set AWS_ACCESS_KEY_ID=AKIA3FYVC1HBT5LR76REX
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>set AWS_SECRET_ACCESS_KEY=oeU50PnoUEaTJEpkcYK6HG+LjPeXjivVRN1SU
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>set AWS_DEFAULT_REGION=us-east-1
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws sts get-caller-identity
{
  "UserId": "AIDA3FYVC1HBT5LR76REX",
  "Account": "768312754627",
  "Arn": "arn:aws:iam::768312754627:user/Bob"
}

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws ec2 describe-instances --query "Reservations[*].Instances[*].[VpcId, InstanceId, ImageId, InstanceType]"
[]

F:\git\BSG\AWS_SAA\Code\s2c1\CLI>aws rds describe-db-instances --query "DBInstances[*].[DBInstanceIdentifier, DBName, DBInstanceStatus, AvailabilityZone, DBInstanceClass]"
An error occurred (AccessDenied) when calling the DescribeDBInstances operation: User: arn:aws:iam::768312754627:user/Bob is not authorized to perform: rds:DescribeDBInstances
F:\git\BSG\AWS_SAA\Code\s2c1\CLI>_

```

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]"
```

```
F:\git\BSG\AWS_SAA\Code\2c1\CLI>aws iam list-roles --query "Roles[?RoleName == 'example-role'].[RoleName, Arn]"
[
  {
    "example-role":
      "arn:aws:iam::768312754627:role/example-role"
  }
]

F:\git\BSG\AWS_SAA\Code\2c1\CLI>aws sts assume-role --role-arn "arn:aws:iam::768312754627:role/example-role" --role-session-name AWSCLI-Session >LlavesSession.txt
F:\git\BSG\AWS_SAA\Code\2c1\CLI>rem Setear las variables de Entorno con la informacion de LlavesSession.txt
F:\git\BSG\AWS_SAA\Code\2c1\CLI>set AWS_ACCESS_KEY_ID=ASIA3FYVC1HBMZ1HVB56
F:\git\BSG\AWS_SAA\Code\2c1\CLI>set AWS_SECRET_ACCESS_KEY=BSi4Wn0+BdM9/3yWYx2F1W1j3UQ48Detu6TwiEt
F:\git\BSG\AWS_SAA\Code\2c1\CLI>set AWS_SESSION_TOKEN=19eJh3JpZ21uX2UjE0T////////wEaCWUzLWUhe3QtMSJHMEUCIH+Zc4jTF5+g6C1bHqFka0qf6ew/3NkgJpF11DFUS/KZ0iEanMDvenFgSWu0CQJGUhInE931onEMxIz=Pq+pm071UuIr+KrcAjMaEFNat3Jn0gux77+UeFu/zFtROOFsDsSTF09T0Fa11NMUvF1oL02eLpZtX0d51PtYohcY/8vInnVgUcKNQweXOM/TXnQcUAmYHqjBPpFvRiEADLjhiu1VPa0xdiomH3uzqhuJTILm2r1GGcZNR0uZL7d/SJapfu1Zo999cujuD0nzQGYfQgU69J5032nfqHMoY56Kd08gZau4qhag+ueB0raFFdLEtP8CFeU6frxPgX8LNB2uoxUplnqeiU1Maah2zYMFk0r0zMBpDax1La0Z/8x/MSFPZzvU4o0ZLYD1kduarcHina
F:\git\BSG\AWS_SAA\Code\2c1\CLI>set AWS_DEFAULT_REGION=us-east-1
F:\git\BSG\AWS_SAA\Code\2c1\CLI>aws sts get-caller-identity
{
  "UserId": "AROA3FYVC1HBMZ6APSCO:AWSCLI-Session",
  "Account": "768312754627",
  "Arn": "arn:aws:sts::768312754627:assumed-role/example-role/AWSCLI-Session"
}

F:\git\BSG\AWS_SAA\Code\2c1\CLI>aws ec2 describe-instances --query "Reservations[*].Instances[*].[VpcId, InstanceId, ImageId, InstanceType]"
An error occurred (UnauthorizedOperation) when calling the DescribeInstances operation: You are not authorized to perform this operation.
F:\git\BSG\AWS_SAA\Code\2c1\CLI>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](#) (For Web Management Console) or the last 2 screens for [Assume role and check new policy](#) (For CLI).