

Lab 11

ADVANCED ROLES AND GROUPS MANAGEMENT USING IAM

STEP 1: Log In to the Amazon Web Service Console

This laboratory experience is about Amazon Web Services and you will use the AWS Management Console in order to complete all the lab steps.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown menu, and user information: 'Antonio Ang', 'Oregon', and a 'Support' link. Below the navigation bar, the main content area is titled 'Amazon Web Services'. It features a grid of service categories and their respective services:

- Compute**
 - EC2: Virtual Servers in the Cloud
 - Lambda PREVIEW: Run Code in Response to Events
- Storage & Content Delivery**
 - S3: Scalable Storage in the Cloud
 - Storage Gateway: Integrates On-Premises IT Environments with Cloud Storage
 - Glacier: Archive Storage in the Cloud
 - CloudFront: Global Content Delivery Network
- Database**
 - RDS: MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
 - DynamoDB: Predictable and Scalable NoSQL Data Store
 - ElastiCache: In-Memory Cache
 - Redshift: Managed Petabyte-Scale Data Warehouse Service
- Networking**
 - VPC: Isolated Cloud Resources
 - Direct Connect: Dedicated Network Connection to AWS
 - Route 53: Scalable DNS and Domain Name Registration
- Administration & Security**
 - Directory Service: Managed Directories in the Cloud
 - Identity & Access Management: Access Control and Key Management
 - Trusted Advisor: AWS Cloud Optimization Expert
 - CloudTrail: User Activity and Change Tracking
 - Config PREVIEW: Resource Configurations and Inventory
 - CloudWatch: Resource and Application Monitoring
- Deployment & Management**
 - Elastic Beanstalk: AWS Application Container
 - OpsWorks: DevOps Application Management Service
 - CloudFormation: Templated AWS Resource Creation
 - CodeDeploy: Automated Deployments
- Analytics**
 - EMR: Managed Hadoop Framework
 - Kinesis: Real-time Processing of Streaming Big Data
 - Data Pipeline: Orchestration for Data-Driven Workflows
- Application Services**
 - SQS: Message Queue Service
 - SWF: Workflow Service for Coordinating Application Components
 - AppStream: Low Latency Application Streaming
 - Elastic Transcoder: Easy-to-use Scalable Media Transcoding
 - SES: Email Sending Service
 - CloudSearch: Managed Search Service
- Mobile Services**
 - Cognito: User Identity and App Data Synchronization
 - Mobile Analytics: Understand App Usage Data at Scale
 - SNS: Push Notification Service
- Enterprise Applications**
 - WorkSpaces: Desktops in the Cloud
 - Zocalo: Secure Enterprise Storage and Sharing Service

On the right side, there's a section titled 'Additional Resources' with links to 'Getting Started', 'AWS Console Mobile App', 'AWS Marketplace', and 'Service Health'. The 'Service Health' section shows a status of 'All services operating normally' as of 'Nov 20 2014 12:57:00 GMT-0800'. Below this is a 'Set Start Page' section with a 'Console Home' button.

The AWS Management Console is a web control panel for managing all your AWS resources, from EC2 instances to SNS topics. The console enables cloud management for all aspects of the AWS account, including managing security credentials, or even setting up new IAM Users.

Log in to the AWS Management Console

In order to start the laboratory experience, open the Amazon Console by clicking this button:

[Open AWS Console](#)

Log in with the username **xxxxx** and the password **xxxxx**



Account:

User Name:

Password:

☐ I have an MFA Token [\(more info\)](#)

Sign In

[Sign-in using root account credentials](#)

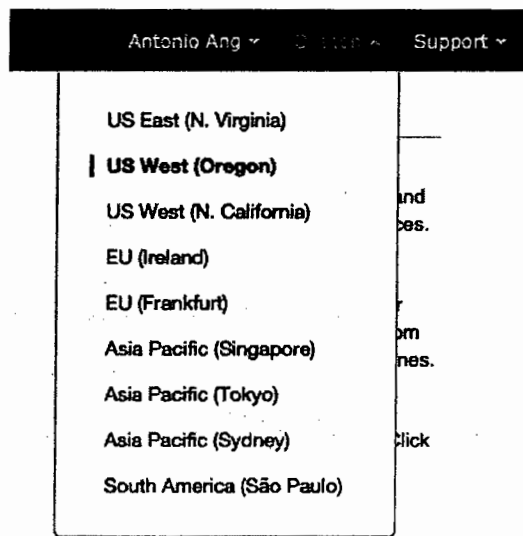
[Terms of Use](#) [Privacy Policy](#)
© 1996-2014, Amazon Web Services, Inc. or its affiliates.

Select the right AWS Region

Amazon Web Services is available in different regions all over the world, and the console lets you provision resources across multiple regions. You usually choose a region that best suits your business needs to optimize your customer's experience, but you must use the region **US**

West (Oregon) for this laboratory.

You can select the **US West (Oregon)** region using the upper right dropdown menu on the AWS Console page.



STEP 2: Create IAM User

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

You can create a new **IAM User** using the AWS Management Console.

Select the **Identity & Access Management (IAM)** service from the Management Console dashboard:



From the IAM dashboard, click on **Users** link in the sidebar menu.

A screenshot of the AWS IAM dashboard. The left sidebar shows a menu with "Dashboard" selected, and other options like "Details", "Groups", "Users", "Roles", "Policies", "Identity Providers", "Password Policy", "Credential Report", and "Encryption Keys". The main content area has a "Welcome to Identity and Access Management" header, followed by a sign-in link, "IAM Resources" (Users: 1, Roles: 0, Groups: 1, Identity Providers: 0, Customer Managed Policies: 0), and a "Security Status" section showing 2 out of 5 checks complete. The "Feature Spotlight" and "Additional Information" sections are on the right.

Dashboard

Details

Groups

Users

Roles

Policies

Identity Providers

Password Policy

Credential Report

Encryption Keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://985849789121.signin.aws.amazon.com/console> Customize | Copy Link

IAM Resources

Users: 1 Roles: 0

Groups: 1 Identity Providers: 0

Customer Managed Policies: 0

Security Status 2 out of 5 complete. 1 checks failed.

- Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- Apply an IAM password policy
- Rotate your access keys

Feature Spotlight

Information on AWS IAM

Additional Information

- IAM documentation
- Web Identity Federation Playground
- Policy Simulator
- Videos, IAM release history and additional resources

The **Users** page lists all available IAM Users, click on the **Create New Users** blue button for creating a new user.

A screenshot of the AWS IAM "Users" page. The left sidebar is the same as the dashboard. The main content area has a "Create New Users" button and a "User Actions" dropdown. Below is a search bar and a table with one user listed. The table has columns for checkboxes, User Name, Groups, Password, Password Last Used, Access Keys, and Creation Time.

Dashboard

Details

Groups

Users

Roles

Policies

Identity Providers

Password Policy

Credential Report

Encryption Keys

Create New Users User Actions

Search

Showing 1 results

<input type="checkbox"/>	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
<input type="checkbox"/>	student	1	✓	2015-01-28 10:59 UTC+0100	1 active	2015-01-28 10:59...

You can create up to 5 users at a time with usernames that don't exceed 64 characters.

You need to enter the following username(s): **lab-user** and then click **Create**.

Create User

Enter User Names:

1.

2.

3.

4.

5.

Maximum 64 characters each

☒ Generate an access key for each user

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

Cancel

Create

The AWS Management Console displays the list of all Access Key IDs and Secret Access Keys created for each user.


Create User

☒ Your 1 User(s) have been created successfully.

This is the last time these User security credentials will be available for download.

You can manage and recreate these credentials any time.

▼ Hide User Security Credentials

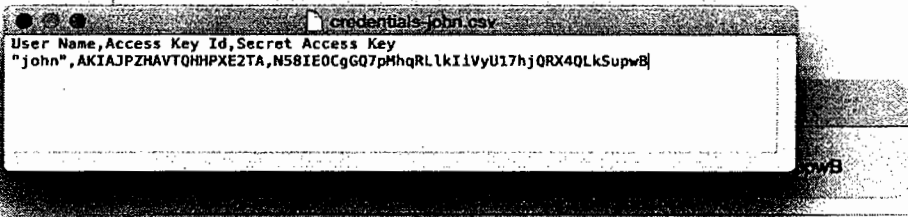
 John
Access Key ID: AKIAJPZHAVTQHHPXE2TA
Secret Access Key: N58IEOCgGQ7pMhqRLikIvYU17hQRX4QLkSupwB

Close

Download Credentials

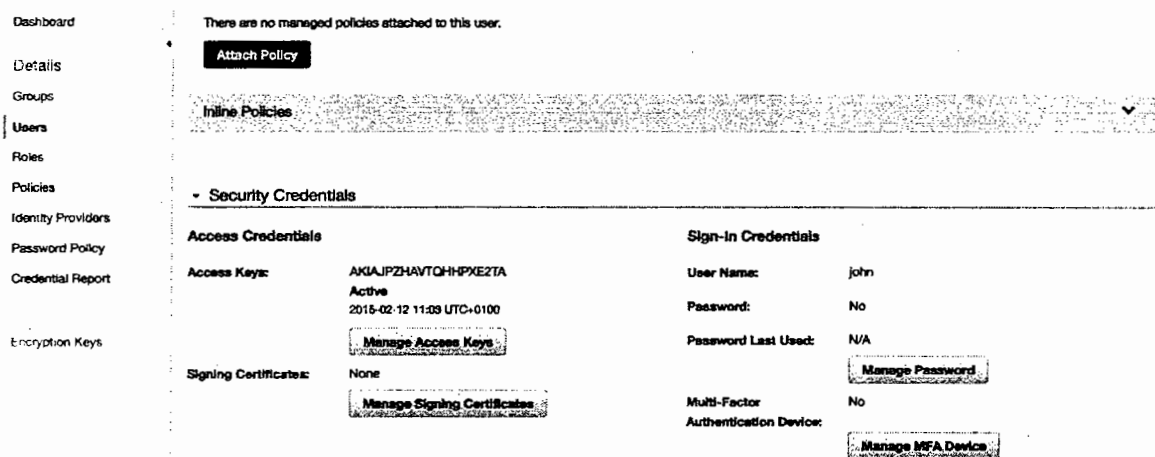
Click **Download Credentials** for downloading a csv file containing the security credentials (you won't be able to show them again if you click close).

Create User ☒ Your 1 User(s) have been created successfully.
This is the last time these User security credentials will be available for download.



Generate a user password

Each created user comes without a password, so you cannot use it for logging into the AWS Management Console. You can generate a password for a specific user by opening the user details page and clicking on the **Manage Password** grey button.



You can assign a specific password or let the system generate it for you. Forcing the user to create a new password at next sign-in usually is a good idea if you want to keep your user password secret.

Click **Apply** for generating it.

Manage Password

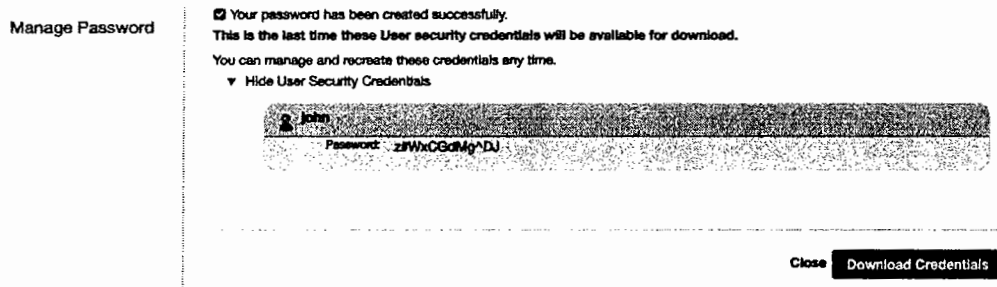
Users who will be using the AWS Management Console require a password. Select from the options below to manage the password for user john.

- ☒ Assign an auto-generated password
- ☐ Assign a custom password

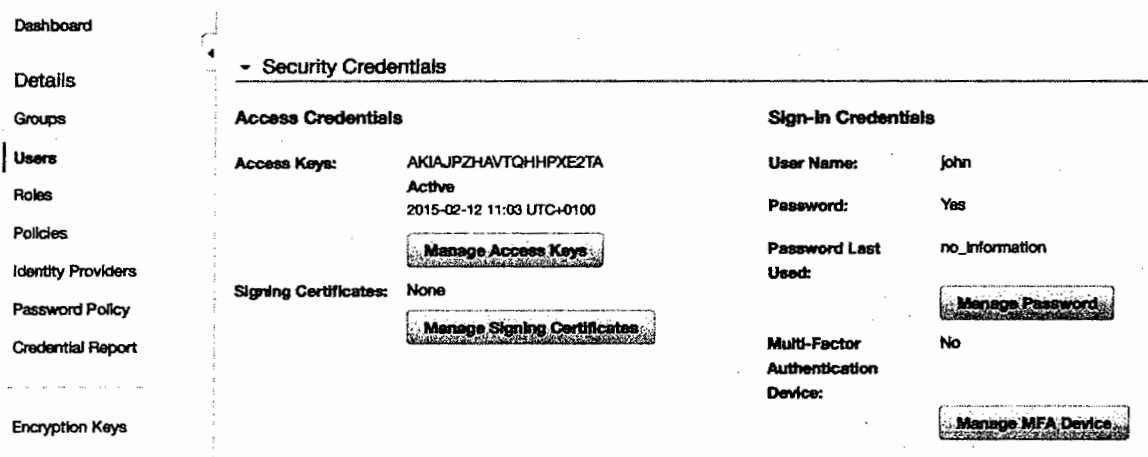
☐ Require user to create a new password at next sign-in

Cancel **Apply**

The management console will show you the password once, save it in a safe place before closing the tab.



Your user account is set up and you can use it for accessing the AWS Management Console.



STEP 3: Create IAM Group

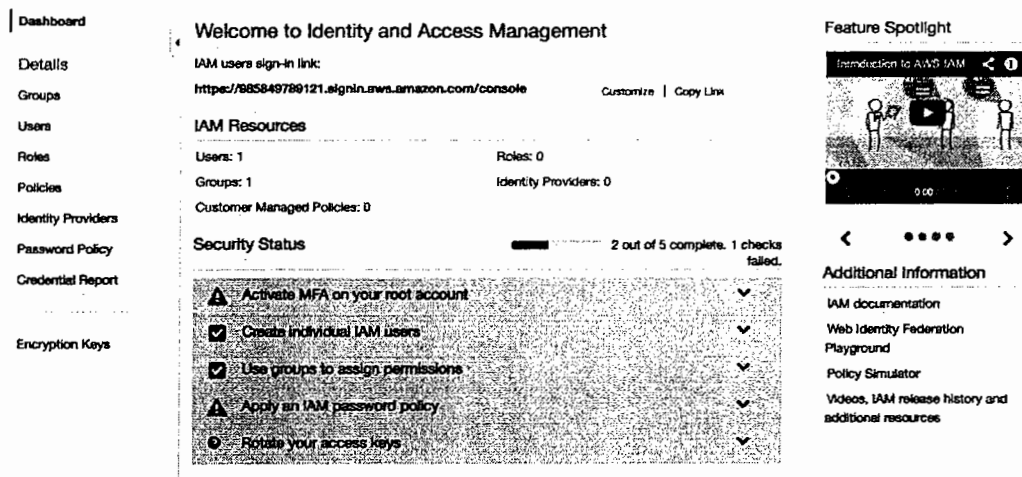
AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

You can create a new **IAM Group** using the AWS Management Console.

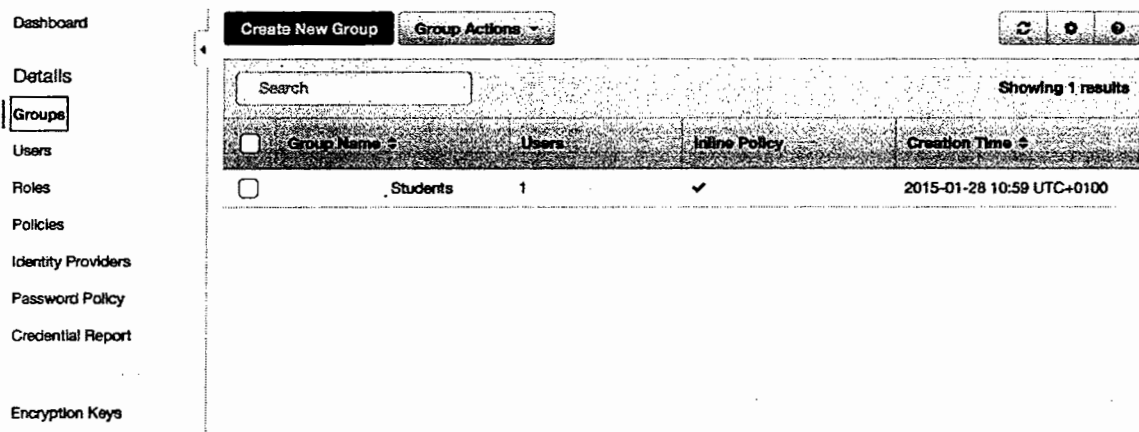
Select the **Identity & Access Management (IAM)** service from the Management Console dashboard:



From the IAM dashboard, click on **Groups** link in the sidebar menu.



The **Groups** page lists all available IAM Groups, click on the **Create New Group** blue button for creating a new IAM group.



The **Create New Group** wizard is composed by 3 simple steps. You need to insert the name of the IAM group during the first step. Use **lab-ec2-viewers** as **Group Name** and then click the **Next Step** button.

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:

mygroup

Example: Developers or ProjectAlpha
Maximum 128 characters

You need to select one or more policies to attach to the group. They will be inherited by any user of the group.

Please select the following policy(ies): **AmazonEC2ReadOnlyAccess**

Click **Next Step** to review your choices.

Create New Group Wizard

Step 1: Group Name

Step 2: Attach Policy

Step 3: Review

Attach Policy

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

Filter:	Policy Type	ec2
<input type="checkbox"/>	Policy Name	Attached Entities
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	0
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscaleRole	0
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	0
<input type="checkbox"/>	AmazonEC2ContainerServiceFullAccess	0
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	0
<input type="checkbox"/>	AmazonEC2FullAccess	0
<input checked="" type="checkbox"/>	AmazonEC2ReadOnlyAccess	0
<input type="checkbox"/>	AmazonEC2ReportsAccess	0
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	0

You are almost done, check all inserted data and the click **Create Group**.

The **Groups** page now lists the new group and you are able to assign the **lab-ec2-viewers** group to any available user.

Dashboard

Details

Groups

Users

Roles

Policies

Identity Providers

Password Policy

Credential Report

Encryption Keys

Create New Group

Group Actions

Search				Showing 2 results
<input type="checkbox"/>	Group Name	Users	Inline Policy	Creation Time
<input type="checkbox"/>	Students	1	✓	2015-01-28 10:59 UTC+0100
<input type="checkbox"/>	devops	0		2015-02-12 10:58 UTC+0100

STEP 4: Add IAM User to Group

You can attach an **IAM User** to one or more IAM groups using the AWS Management Console.

Select the **Identity & Access Management (IAM)** service from the Management Console dashboard:



From the IAM dashboard, click on **Users** link in the sidebar menu.

A screenshot of the AWS IAM dashboard. The left sidebar contains a menu with links: Dashboard, Details, Groups, Users, Roles, Policies, Identity Providers, Password Policy, Credential Report, and Encryption Keys. The main content area is titled "Welcome to Identity and Access Management" and includes a sign-in link, IAM Resources summary (Users: 1, Groups: 1, Roles: 0, Identity Providers: 0, Customer Managed Policies: 0), and a Security Status section with five checklist items: "Activate MFA on your root account", "Create individual IAM users", "Use groups to assign permissions", "Apply an IAM password policy", and "Rotate your access keys". The right sidebar features a "Feature Spotlight" video player and "Additional Information" links for documentation, playground, and simulator.

The **Users** page lists all available IAM Users, click on the **lab-user** user for opening the details page.

A screenshot of the AWS IAM "Users" page. It shows a table with two users: "john" and "student". The "john" user has 0 groups, no password, and 1 active access key. The "student" user has 0 groups, a password, and no access keys. Below the table, there are error messages indicating that the user is not authorized to perform certain actions like "listGroupsForUser" or "listAccessKeys" on the "student" resource.

Click **Add User to Groups**.

Dashboard
Details
Groups
Users
Roles
Policies
Identity Providers
Password Policy
Credential Report

Users > John

Summary

User ARN:

arn:aws:iam::820056889012:user/john

Has Password:

No

Groups (for this user):

0

Path:

/

Creation Time:

2015-02-12 11:03 UTC+0100

Groups

This user does not belong to any groups.

Add User to Groups

You can add a single user to more than one group by selecting them one by one.

Select the following groups for completing this step: **lab-ec2-viewers**

Add User to Groups

Select groups that user John will be added to.

Search					Showing 2 results
<input type="checkbox"/>	Group Name	Users	Inline Policy	Creation Time	
<input type="checkbox"/>	Students	1	✓	2015-01-28 10:59 UTC+0100	
<input checked="" type="checkbox"/>	devops	0		2015-02-12 10:58 UTC+0100	

Cancel Add to Groups

Click **Add to Groups** and the user will be assigned to the selected groups.

STEP 5: Create customer managed policy with policy generator

You can create customer managed policies to define sets of permissions to attach to principal entities (users, groups, and roles) in your AWS account.

Select the **Identity & Access Management (IAM)** service from the Management Console dashboard:



In the navigation pane, choose Policies, and then choose **Create Policy**.

- Choose the Select button that corresponds to the Policy Generator for build the policy using Policy Generator tool
 - ✓ On **Effect** Select Allow
 - ✓ On of **AWS Service** select **Amazon S3**

- ✓ On **Actions** select **ListBucket** item
- ✓ On **Amazon Resource Name ARN** specify ***** Then choose **Add Statement**

Create Policy

Step 1: Create Policy

Step 2: Set Permissions

Step 3: Review Policy

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see Overview of Policies in Using AWS Identity and Access Management.

Effect ☒ Allow ☐ Deny

AWS Service

Actions

Amazon Resource Name (ARN)

Add Conditions (optional)

Effect	Action	Resource	
Allow	s3:ListBucket	*	Remove

2. Select **Next Steps** and in Policy Name filed insert **lab-s3-policy**
3. After you complete your changes, choose Validate Policy and ensure that no errors display in a red box at the top of the screen. Correct any errors that are reported.
4. Choose Create Policy to save your new policy.

STEP 6: Attach policy to Users

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

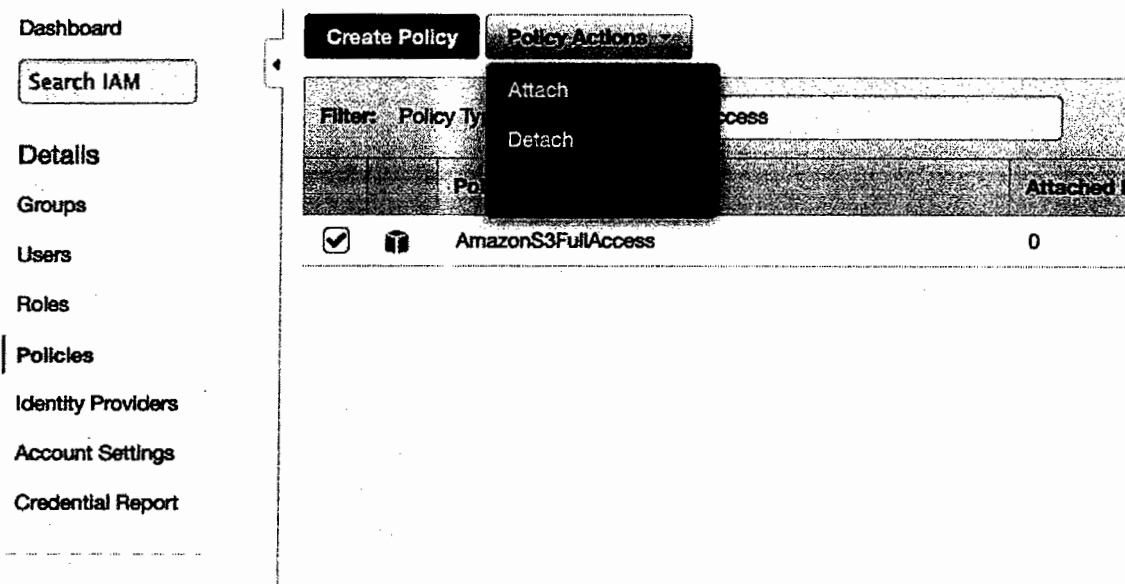
You can create customer managed policies to define sets of permissions to attach to principal entities (users, groups, and roles) in your AWS account.

Select the **Identity & Access Management** (IAM) service from the Management Console dashboard:



In the navigation pane, choose Policies.

1. In the list of policies, select the check box next to the name of the policy to attach. Use the Filter menu and the Search box to filter the list of policies with name **AmazonS3ReadOnlyAccess**.
2. Choose Policy Actions, and then choose Attach.
3. Select the **lab-user** User to attach the policy.
4. After selecting the User, choose **Attach Policy**.



Now the User **lab-user** has the attached policy and relative privileges

STEP 7: Create IAM Role

You can create a new **IAM Role** using the AWS Management Console.

Select the **Identity & Access Management (IAM)** service from the Management Console dashboard:



From the IAM dashboard, click on the **Roles** link in the sidebar menu then:

1. Click Create **New Role**
2. For Role name type the role name **lab-role**

3. On the Select Role Type page, select AWS Services Roles, then search for **Amazon EC2**, and click on **Select**
4. On the Attach Policy page, filter for the name **S3Full** and select the policy **AmazonS3FullAccess**
5. Click **Next Step** to review the role and copy your **Role ARN**
6. Then click **Create Role**

Create Role

Step 1: Set Role Name
Step 2: Select Role Type
Step 3: Establish Trust
Step 4: Attach Policy
Step 5: Review

Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name	lab-role	Edit Role Name
Role ARN	arn:aws:iam::178270562166:role/lab-role	
Trusted Entities	The identity provider(s) ec2.amazonaws.com	
Policies	arn:aws:iam::178270562166:policy/policy-lab	Edit Policies

Cancel
Previous
Create Role

STEP 8: Launch EC2 Instances with IAM Profile

You can launch an EC2 instance using the EC2 launch wizard.

Select the EC2 service from the Management Console dashboard:



From the dashboard, click **Launch Instance**.

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

IMAGES

AMIs

Bundle Tasks

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances

0 Elastic IPs

0 Volumes

0 Snapshots

0 Key Pairs

0 Load Balancers

0 Placement Groups

2 Security Groups

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US West (Oregon) region

The **Select an Amazon Machine Image (AMI)** page displays a list of basic configurations called **Amazon Machine Images (AMIs)** that serve as templates for your instance. Select the 64-bit **Amazon Linux AMI**.

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Tag Instance

6. Configure Security Group

7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only ①

Amazon Linux

Free tier eligible

Amazon Linux AMI 2014.09.1 (HVM) - ami-b5a7ea85

The Amazon Linux AMI is an EBS backed image. It includes the 3.14 kernel, Ruby 2.1, PHP 5.5, PostgreSQL 9.3, Docker 1.2, the AWS command line tools, and repository access to many other packages.

Root device type: ebs Virtualization type: hvm

Select

64-bit

Red Hat

Free tier eligible

Red Hat Enterprise Linux 7.0 (HVM), SSD Volume Type - ami-99bef1a9

Red Hat Enterprise Linux version 7.0 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm

Select

64-bit

On the **Select an Instance Type** page, do not change any option and click on **Next, Configure Instance Details**.

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Tag Instance

6. Configure Security Group

7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by:

All instance types

Current generation

Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs ①	Memory (GiB)	Instance Storage (GiB) ①	EBS-Optimized Available ①	Network Performance ①
General purpose	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
General purpose	General purpose	t2.small	1	2	EBS only	-	Low to Moderate

Cancel

Previous

Review and Launch

Next: Configure Instance Details

On the **3. Configure Instance** tab, select **Network** **172.31.0.0/16** and **Subnet** **172.31.16.0/24** make sure to select **IAM Role lab-role** and then click **Next, Add Storage**.

1 Choose AMI 2 Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of Instances ① 1 [Launch into Auto Scaling Group](#) ①

Purchasing option ① ☐ Request Spot Instances

Network ① vpc-cd811ba8 (172.31.0.0/16) (default) [Create new VPC](#)

Subnet ① No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP ① Use subnet setting (Enable) [Create new subnet](#)

IAM role ① **lab-role** [Create new IAM role](#)

Shutdown behavior ① Stop [Create new IAM role](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

On the **4. Add Storage** tab, do not change any option and click "**Review and Launch**" button.

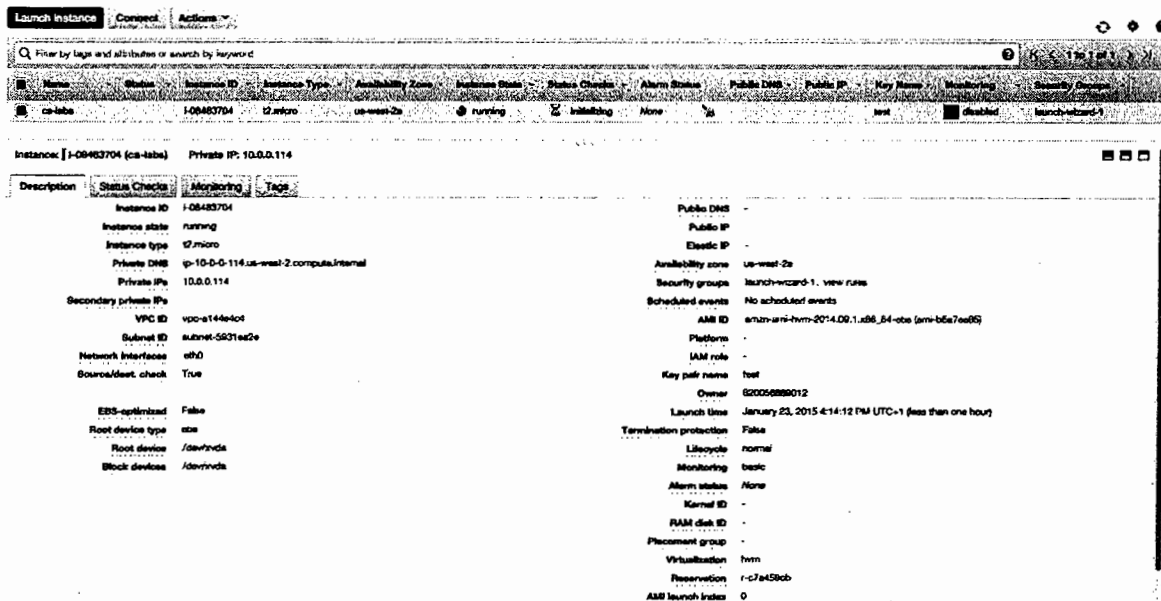
On the Review Instance Launch page, click **Launch**.

In the **Select an existing key pair or create a new key pair** dialog box, select **Create a new key pair**, then choose a KeyPair name and download it.

Select the acknowledgment check box, and then click **Launch Instances**.

A confirmation page will let you know that your instance is launching. Click **View Instances** to close the confirmation page and return to the console.

On the Instances screen, you can view the status of your instance. It will take a short time for your instance to be launched. When you launch an instance, its initial state is **pending**. After the instance starts, its state changes to **running**, and it receives a public DNS name.



STEP 9: Connect to a remote shell using an SSH connection

In order to manage a remote Linux server, you must employ an **SSH Client**. Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network. Common applications include remote command-line login and remote command execution.

Connect using Linux / Mac OS

Linux distributions and Mac OS are shipped with a fully working SSH client that accepts standard PEM Keys.

Starting a remote SSH session is easy:

- ✓ Open your **Terminal** application
- ✓ Write and run the following command: `ssh -i /path/to/your/keypair.pem user@server-ip`

`server-ip` is the Public IP of your server, you can find it in the EC2 instance details

`user` is the remote system user that will be used for the remote authentication

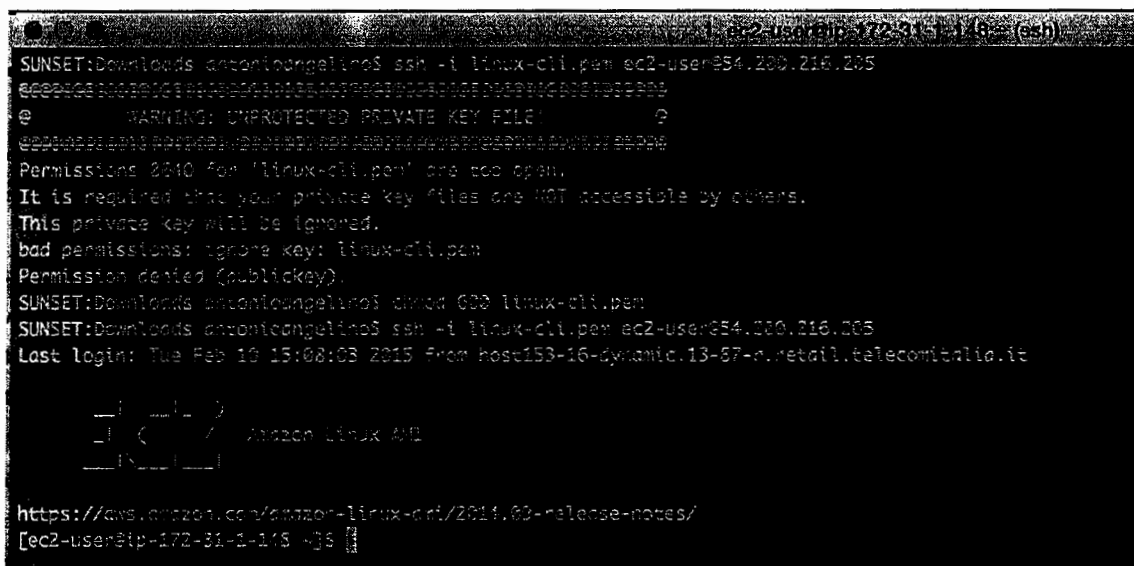
Amazon Linux AMIs typically use **ec2-user** as username.

Ubuntu AMIs login user is **ubuntu**, Debian AMIs use **admin** instead.

Assuming that you selected the Amazon Linux AMI, your assigned public IP is 123.123.123.123, and your keypair (named "keypair.pem") is stored in /home/youruser/keypair.pem, the right command to run is: **ssh -i /home/youruser/keypair.pem ec2-user@123.123.123.123**

Note: your SSH Client may refuse to start the connection, warning that the key file is unprotected. You should deny the file access to any other system user by changing its permissions. Issue the following command and then try again:

chmod 600 /home/youruser/keypair.pem



```
SUNSET:Downloads antonioangelino$ ssh -i linux-cli.pem ec2-user@54.200.216.205
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 2010 for 'linux-cli.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: linux-cli.pem
Permission denied (publickey).
SUNSET:Downloads antonioangelino$ chmod 600 linux-cli.pem
SUNSET:Downloads antonioangelino$ ssh -i linux-cli.pem ec2-user@54.200.216.205
Last login: Tue Feb 10 15:08:03 2015 from host153-16-dynamic.13-87-n.retail.telecomitalia.it

 _ _ _ _ _
| | ( ) /   Amazon Linux AMI
 _ _ _ _ _

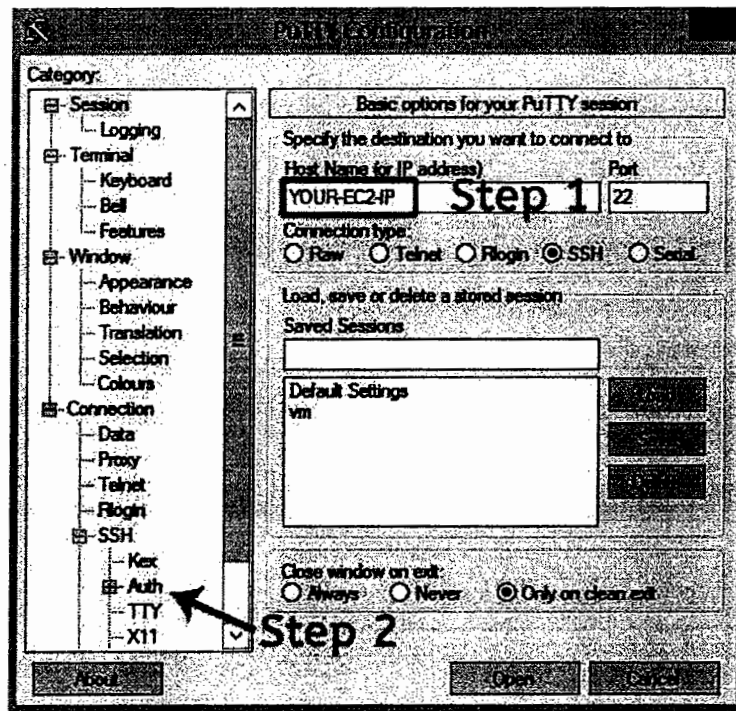
https://aws.amazon.com/amazon-linux-ami/2014.09-release-notes/
[ec2-user@ip-172-31-1-165 ~]$
```

Connect using Windows

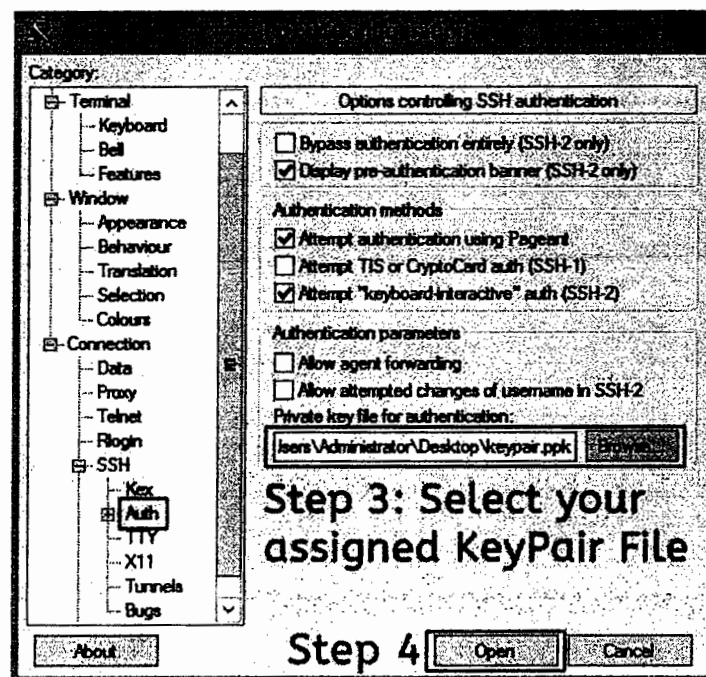
Windows has no SSH client, so you must use PuTTY and convert the PEM key to PPK using PuTTYgen.

Starting a remote SSH session using PuTTY is easy:

- ✓ Open PuTTY and insert the EC2 instance IP Address in the Host Name field.



- ✓ Select **Connection > SSH > Auth** section and then select the downloaded Keypair that you previously converted to PPK format.



- ✓ After some seconds, you will see the authentication form. **Login as ec2-user** and you will see the EC2 server welcome banner.

STEP 10: Test IAM Profile from EC2 Linux instance

Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles and specifying the role when you launch your instances

When are you logged on EC2 Instances you can use this command for retrieve the current IAM Profile

curl http://169.254.169.254/latest/meta-data/iam/info

```

$ ssh -i ec2-user@ec2-54-124-103-48.compute-1.amazonaws.com -p 22 ec2-user@ip-172-31-172-31
Last login: Tue Jan 12 07:26:54 2016 from 50.168.170.50

ec2-user@ip-172-31-172-31:~$ curl http://169.254.169.254/latest/meta-data/iam/info
{"Code": "Success",
 "LastUpdated": "2016-01-12T06:53:11Z",
 "InstanceProfileArn": "arn:aws:iam::111111111111:instance-profile/lab-role",
 "InstanceProfileId": "AIPAIQ07HYLQAKGSDGRM"}
ec2-user@ip-172-31-172-31:~$

```

The key **InstanceProfileArn** identify the ARN of role associated to EC2 instance

Now you can test the IAM Profile using AWS Cli for list bucket and create bucket without specify AK and SK. Remember that role **lab-role** has policy **AmazonS3FullAccess**

aws s3 ls for list bucket

aws s3 mb s3://bucket-name for make a bucket

```

[ec2-user@ip-172-31-25-88 ~]$ aws s3 ls
2016-01-12 07:27:57 bucket.lab. .com
2016-01-12 07:28:55 bucket2.lab. .com
[ec2-user@ip-172-31-25-88 ~]$ aws s3 mb s3://bucket3.lab. .com
make bucket: s3://bucket3.lab .com/
[ec2-user@ip-172-31-25-88 ~]$

```

Now you can call the AWS API specifying the AK and SK on command line. This overwrite the IAM Profile and you will be able to interact with EC2 service in read only mode because the policy associated to Group **lab-ec2-viewers** is the policy **AmazonEC2ReadOnlyAccess** and able to interact with S3 service in read only mode because the policy attached to user is **AmazonS3ReadOnlyAccess**

```
export AWS_ACCESS_KEY_ID=access-key-of-user-created-before
```

```
export AWS_SECRET_ACCESS_KEY=secret-key-of-user-created-before
```

now you can use cli

```
aws ec2 describe-instances --region us-east-2
```

 for list regions

```
aws s3 ls for list bucket
```

[illegible]

How you can see you have the privileges for describe instances and list bucket, but you not have the privileges for make bucket.