

AWS Fundamental



Principle of Least Privilege

Minimal Privilege

- The principles of least privilege is practise of limiting access to minimal level that will allow normal functioning.
- A user should only have access to data, hardware that they need, to be able to perform their assigned duties.



Use Case

Alice is an intern who has joined your organization as an intern System Administrator. Since your infrastructure is hosted in AWS, you need to give access to Alice to view the AWS console. What kind of Access will you give ?

- Share with her the ROOT Credentials of the AWS.
- Create a new user Alice with full Permission for everything.
- Create a new user Alice with ReadOnlyAccess.

It goes Deeper than Expected

A software developer wants to access an application server to see the logs. You being a system administrator, you need to provide him access. How will you give access?

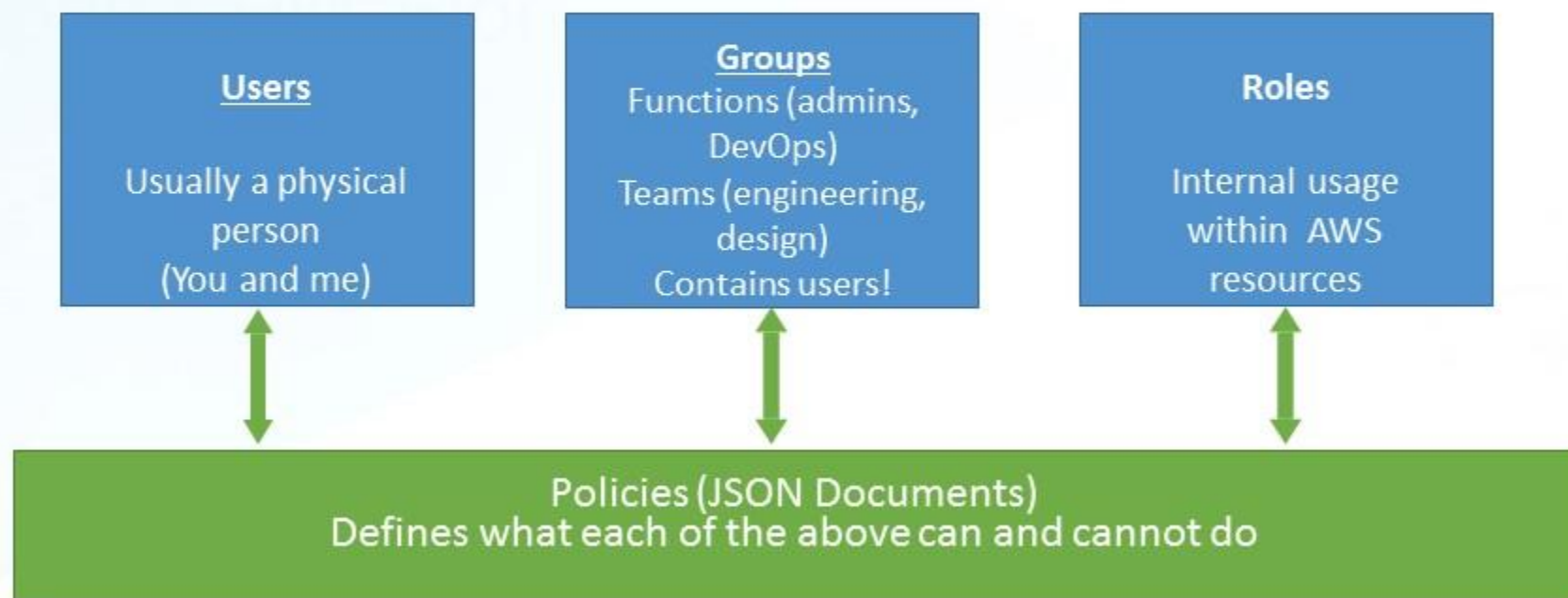
- Create the user with the user add command & Share credentials.
- Create the user with user add command and add him to sudoers list.
- Ask the developer on what log file he wants to access, verify if his access is justified and only allow him to have access to that specific log file and nothing else.

IAM Introduction

IAM Introduction

- IAM (Identity and Access Management)
- Your whole AWS security is there:
 - Users
 - Groups
 - Roles
- Root account should never be used (and shared)
- Users must be created with proper permissions
- IAM is at the center of AWS
- Policies are written in JSON (JavaScript Object Notation)

IAM Introduction



IAM Introduction

- IAM has a **global** view
- Permissions are governed by Policies (JSON)
- MFA (Multi Factor Authentication) can be setup
- IAM has predefined “managed policies”
- We’ll see IAM policies in details in the future
- It’s best to give users the minimal amount of permissions they need to perform their job (least privilege principles)

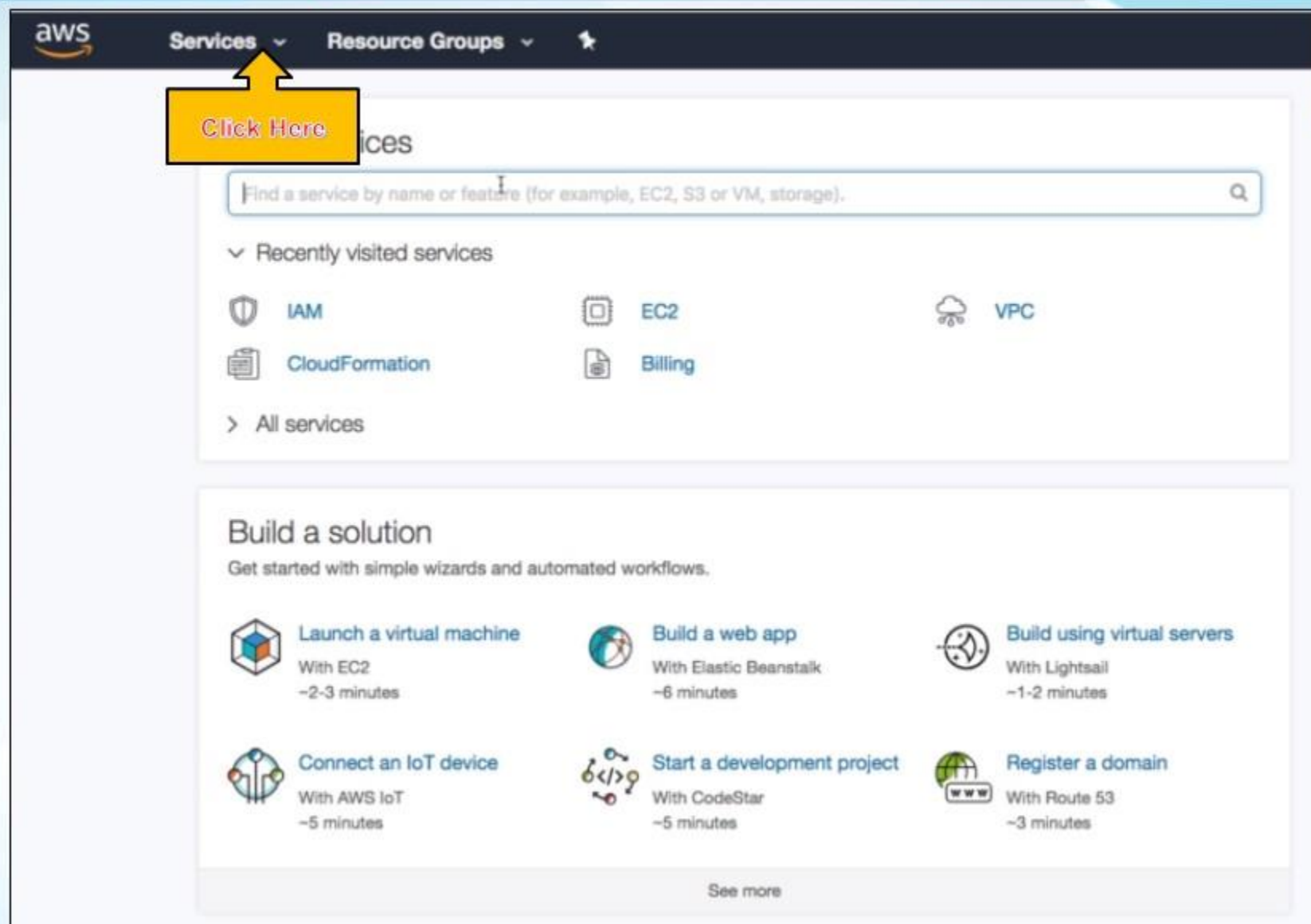
IAM Federation

- Big enterprises usually integrate their own repository of users with IAM
- This way, one can login into AWS using their company credentials
- Identity Federation uses the SAML standard (Active Directory)

IAM |0| Brain Dump

- One IAM **User** per PHYSICAL PERSON
- One IAM **Role** per Application
- IAM credentials should NEVER BE SHARED
- Never, ever, ever, ever, write IAM credentials in code. EVER.
- And even less, NEVER EVER EVER COMMIT YOUR IAM credentials
- **Never use the ROOT account except for initial setup.**
- **Never use ROOT IAM Credentials**

IAM Hands On



The screenshot shows the AWS Management Console interface. At the top, there is a dark navigation bar with the AWS logo, a 'Services' dropdown menu, a 'Resource Groups' dropdown menu, and a search icon. A yellow callout box with the text 'Click Here' and an arrow points to the 'Services' dropdown menu. Below the navigation bar, there is a search bar with the placeholder text 'Find a service by name or feature (for example, EC2, S3 or VM, storage)'. Below the search bar, there is a section titled 'Recently visited services' which lists several services: IAM, CloudFormation, EC2, Billing, and VPC. Below this section, there is a link '> All services'. Further down, there is a section titled 'Build a solution' with the subtitle 'Get started with simple wizards and automated workflows.' This section contains six cards, each with an icon, a title, and a description of the solution and its duration: 'Launch a virtual machine' (With EC2, ~2-3 minutes), 'Build a web app' (With Elastic Beanstalk, ~6 minutes), 'Build using virtual servers' (With Lightsail, ~1-2 minutes), 'Connect an IoT device' (With AWS IoT, ~5 minutes), 'Start a development project' (With CodeStar, ~5 minutes), and 'Register a domain' (With Route 53, ~3 minutes). At the bottom of the 'Build a solution' section, there is a 'See more' link.

aws Services Resource Groups

Click Here

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

- IAM
- CloudFormation
- EC2
- Billing
- VPC

> All services

Build a solution

Get started with simple wizards and automated workflows.

- Launch a virtual machine**
With EC2
~2-3 minutes
- Build a web app**
With Elastic Beanstalk
~6 minutes
- Build using virtual servers**
With Lightsail
~1-2 minutes
- Connect an IoT device**
With AWS IoT
~5 minutes
- Start a development project**
With CodeStar
~5 minutes
- Register a domain**
With Route 53
~3 minutes

See more

Billing

Find a service by name or feature (for example, EC2, S3 or VM, storage).



Compute

EC2

Lightsail 

Elastic Container Service

EKS

Lambda

Batch

Elastic Beanstalk



Storage

S3

EFS

Glacier

Storage Gateway



Database

RDS

DynamoDB

ElastiCache

Neptune



Developer Tools

CodeStar

CodeCommit

CodeBuild

CodeDeploy

CodePipeline

Cloud9

X-Ray



Management Tools

CloudWatch

AWS Auto Scaling

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Systems Manager

Trusted Advisor

Managed Services

The screenshot displays the AWS Management Console interface. At the top, the navigation bar includes the AWS logo, a 'Services' dropdown menu, a 'Resource Groups' dropdown menu, and a star icon. On the left side, a sidebar lists various console sections: History, Console Home, IAM, EC2, VPC, CloudFormation, and Billing. The main content area shows a search bar with 'iam' entered. Below the search bar, the 'IAM' service is highlighted, with a yellow callout box containing the text 'Click Here' and an arrow pointing to it. The service description 'IAM: Manage User Access and Encryption Keys' is visible. Below the search results, there are three categories of services: 'Storage' (with a folder icon), 'Database' (with a database icon), and 'Management Tools' (with a document icon). Each category lists several services: Storage includes S3, EFS, Glacier, and Storage Gateway; Database includes Amazon RDS, Amazon ElastiCache, Amazon Redshift, Amazon DynamoDB, and Amazon Aurora; Management Tools includes CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, OpsWorks, and Service Catalog. Other services listed in the main area include CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, Cloud9, and X-Ray.

aws Services ^ Resource Groups ☆

History

Console Home

IAM

EC2

VPC

CloudFormation

Billing

iam

IAM
Manage User Access and Encryption Keys

Click Here

CodeStar

CodeCommit

CodeBuild

CodeDeploy

CodePipeline

Cloud9

X-Ray

Storage

S3

EFS

Glacier

Storage Gateway

Database

Management Tools

CloudWatch

AWS Auto Scaling

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

IAM Management Console

← → ↻ https://console.aws.amazon.com/iam/home?region=eu-west-3#/home

Services ▾ Resource Groups ▾

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123367.signin.aws.amazon.com/console

Customize

IAM Resources

Users: 0

Groups: 0

Customer Managed Policies: 0

Roles: 2

Identity Providers: 0

Security Status

Delete your root access keys

▼

Activate MFA on your root account

▼

Create individual IAM users

▼


Use groups to assign permissions

▼

Apply an IAM password policy

▼

1 out of 5 complete.


Prabhav ▾
Global ▾
Support ▾

Feature

Customize

1 out of 5 complete.

▼

▼

▼

▼

▼

Additional

IAM best

IAM doc

Web Ide

Policy S

Videos, resource

IAM does not require region selection.

US East (N. Virginia)

US East (Ohio)

US West (N. California)

US West (Oregon)

Asia Pacific (Mumbai)

Asia Pacific (Seoul)

Asia Pacific (Singapore)

Asia Pacific (Sydney)

Asia Pacific (Tokyo)

Canada (Central)

EU (Frankfurt)

EU (Ireland)

EU (London)

EU (Paris)

South America (São Paulo)

The screenshot displays the AWS IAM Management Console interface. The browser's address bar shows the URL: <https://console.aws.amazon.com/iam/home?region=eu-west-3#/home>. The console header includes the AWS logo, 'Services', and 'Resource Groups' dropdowns. The left sidebar contains a 'Search IAM' bar and a list of navigation items: Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management'. It features an 'IAM users sign-in link' section with a URL and a 'Customize' link. Below this is the 'IAM Resources' section, which displays counts for Users (0), Roles (2), Groups (0), and Identity Providers (0). The 'Security Status' section shows a progress bar indicating '1 out of 5 complete'. It lists five security tasks: 'Delete your root access keys' (completed, green checkmark), 'Activate MFA on your root account' (warning, orange triangle), 'Create individual IAM users' (warning, orange triangle), 'Use groups to assign permissions' (warning, orange triangle), and 'Apply an IAM password policy' (warning, orange triangle). A yellow callout box with an arrow points to the 'Click Here' text in the 'Create individual IAM users' row.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123367.signin.aws.amazon.com/console> [Copy](#) [Customize](#)

IAM Resources

Users: 0 Roles: 2

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status

1 out of 5 complete.

- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users [Click Here](#)
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console> 

[Customize](#)

IAM Resources

Users: 0

Roles: 2

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

 1 out of 5 complete.



Delete your root access keys



Delete your AWS root account access keys, because they provide unrestricted access to your AWS resources. Instead, use IAM user access keys or temporary security credentials. [Learn More](#)

[Manage Security Credentials](#)



Activate MFA on your root account



Create individual IAM users



Use groups to assign permissions



Apply an IAM password policy



[Click Here](#)

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console>

[Customize](#)

IAM Resources

Users: 0

Roles: 2

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

1 out of 5 complete.



Delete your root access keys



Activate MFA on your root account



Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

Manage MFA

Click Here

Individual IAM users



Groups to assign permissions



Apply an IAM password policy



The screenshot shows the AWS IAM Management Console interface. The browser address bar displays the URL: `https://console.aws.amazon.com/iam/home?region=eu-west-3#/security_credential`. The page title is "Your Security Credentials". Below the title, there is instructional text: "Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [AWS IAM User Guide](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference."

A list of credential types is shown with expandable options (+):

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)
- CloudFormation roles
- X.509 certificates
- Account keys

A modal warning box is displayed in the foreground with the following text:

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

Buttons in the modal:

- [Continue to Security Credentials](#)
- [Get Started with IAM Users](#)

Below the modal, there is a link: [Don't show me this message again](#).

A yellow callout box with the text "Click Here" and an arrow points to the "Continue to Security Credentials" button.



Services ▾

Resource Groups ▾



Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- + Multi-factor authentication (MFA)
- + Account access key ID and secret access key
- + CloudHSM
- + X.509 certificate
- + Account identifiers

Click Here

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) to learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.



Password



Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must use an MFA device.

[Activate MFA](#)[Click Here](#)

Access keys (access key ID and secret access key)



Temporary session key pairs



X.509 certificate



Account identifiers

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [AWS IAM console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS account. To activate MFA, you must first provide a user name and password.

Activate MFA

- + Access keys (access key ID and secret access key)
- + CloudFront key pairs
- + X.509 certificate
- + Account identifiers

Manage MFA device

Select the type of MFA device to activate:

- ☒ A virtual MFA device
- ☐ A hardware MFA device

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#).

Cancel

Next Step

Click Here

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.



Password



Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS account. You can use a hardware MFA device, a software MFA device, or a virtual MFA device.

Activate MFA



Access key



CloudFront



X.509 certificate



Account information

Manage MFA device

To activate a virtual MFA device, you must first install an AWS MFA-compatible application on the user's smartphone, PC, or other device. You can find a list of AWS MFA-compatible applications [here](#). After the application is installed, click Next Step to configure the virtual MFA.

☐ Don't show me this dialog box again.

Cancel

Previous

Next Step

Click Here

Your Security

Use this page to manage

To learn more about the ty

+ Password

- Multi-fact

You use MFA to increas
MFA device.

Activate MFA

+ Access ke

+ CloudFron

+ X.509 cert

+ Account k

Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.



► [Show secret key for manual configuration](#)

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1

Authentication code 2

Cancel

Previous

Activate virtual MFA

Your Security

Use this page to manage

To learn more about the ty

+ Password

- Multi-fact

You use MFA to increas
MFA device.

Activate MFA

+ Access ke

+ CloudFron

+ X.509 cert

+ Account k

Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.



► Show secret key for manual configuration

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1 662498

Authentication code 2 327933

Cancel

Previous

Activate virtual MFA

Click Here

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must provide a user name, password, and MFA device.

Activate MFA

- + Access keys (access key ID and secret access key)
- + CloudFront key pairs
- + X.509 certificate
- + Account identifiers

Manage MFA device

The MFA device was successfully associated with your account.



Finish

Click Here

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.



Password



Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must provide a user name, password, MFA device.

Device type	Serial number
Virtual MFA	arn:aws:iam::387124123361:mfa/root-account-mfa-device



Access keys (access key ID and secret access key)





CloudFront key pairs



X.509 certificate



Account identifiers

 Services ▾ Resource Groups ▾ 

Dashboard

Groups

Users

Roles

Policies


Identity providers

Account settings

Credential report

Encryption keys








Welcome to Identity and Access Management

IAM users sign-in link:
<https://387124123361.signin.aws.amazon.com/console>  [Customize](#)

IAM Resources

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status 2 out of 5 complete.

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


Click Here

The screenshot displays the AWS IAM console interface. At the top, the AWS logo is on the left, and navigation links for 'Services', 'Resource Groups', and a star icon are on the right. A left-hand sidebar contains a search bar labeled 'Search IAM' and a list of navigation items: 'Dashboard' (highlighted), 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. The main content area is titled 'Welcome to Identity and Access Management'. It includes a sign-in link for IAM users: <https://387124123361.signin.aws.amazon.com/console>, with a 'Customize' link to its right. Below this, the 'IAM Resources' section shows counts: 'Users: 0', 'Groups: 0', 'Roles: 2', and 'Identity Providers: 0'. The 'Customer Managed Policies: 0' link is also present. The 'Security Status' section features a progress bar indicating '2 out of 5 complete'. It lists three items: 'Delete your root access keys' (checked), 'Activate MFA on your root account' (checked), and 'Create individual IAM users' (warning icon). A yellow arrow points to the 'Create individual IAM users' item, which is highlighted with a yellow box containing the text 'Click Here'. Below this list, a paragraph explains the importance of creating IAM users and provides a 'Learn More' link. A 'Manage Users' button is located below the paragraph. At the bottom of the Security Status section, two more items are partially visible: 'Create groups to assign permissions' and 'IAM password policy'.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console> [Customize](#)

IAM Resources

Users: 0 Roles: 2

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status

2 out of 5 complete.

- ✓ Delete your root access keys
- ✓ Activate MFA on your root account
- ⚠ Create individual IAM users

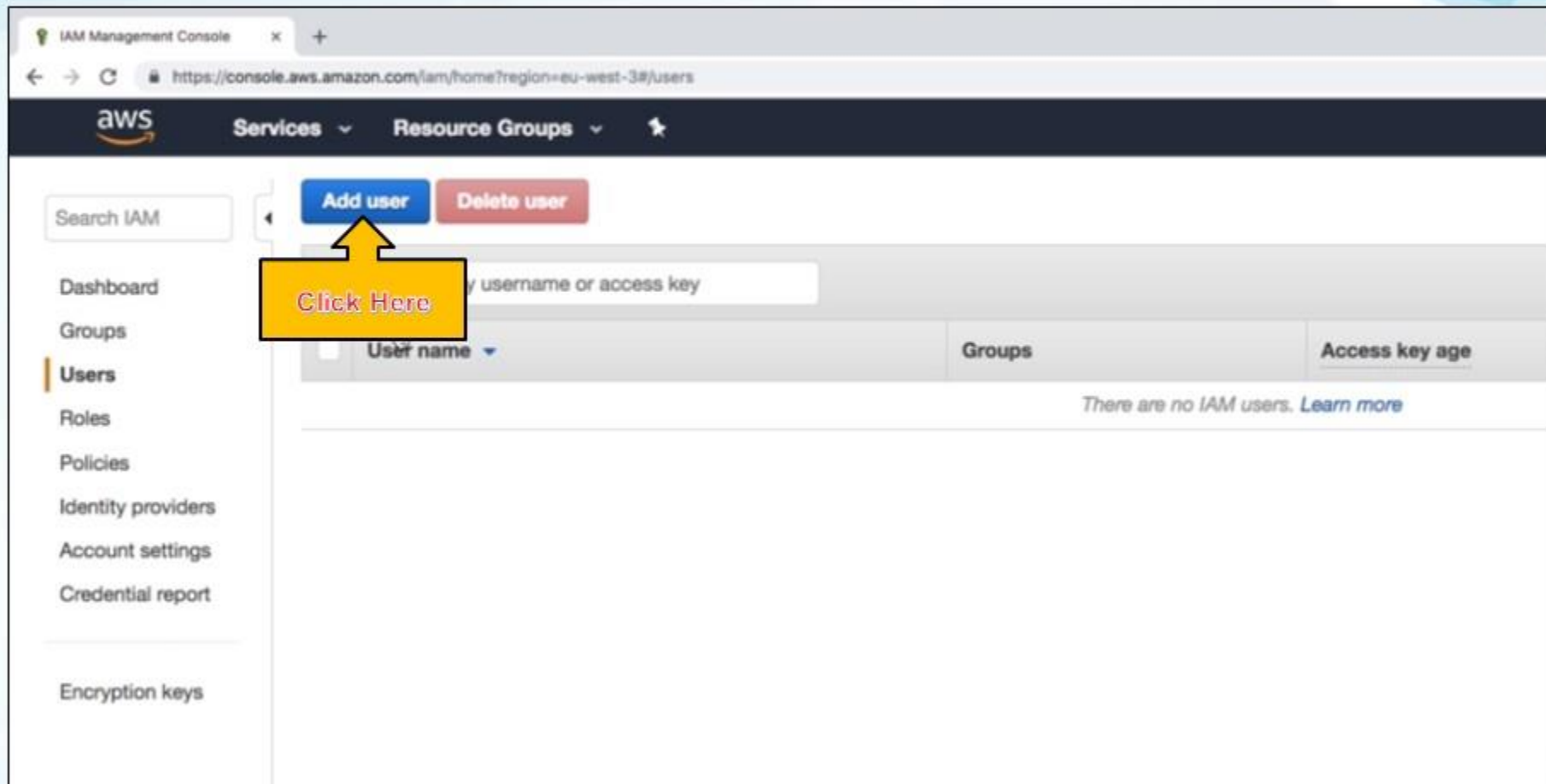
Create IAM users and give them only the permissions they need. Do not use your AWS root account for day-to-day interaction with AWS, because the root account provides unrestricted access to your AWS resources. [Learn More](#)

[Manage Users](#)

⚠ Create groups to assign permissions

⚠ IAM password policy

Click Here



Add user

1

2

3

4

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

- Console password* ☒ Autogenerated password
☐ Custom password

- Require password reset ☒ User must create a new password at next sign-in
I here, automatically set the IAM User's `ChangePasswordPolicy` to allow them to change

* Required

Cancel

Next: Permissions

Click Here

▼ Set permissions



Add user to group



Copy permissions from
existing user



Attach existing policies
directly

Click Here



Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

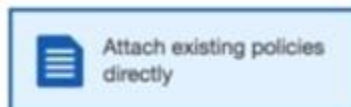
► Set permissions boundary

Cancel

Previous

Next: Review

Set permissions



Create policy



Filter policies

Search

Showing 358 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and ...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFor...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness re...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Alex...
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusi...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete ...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Am...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user'...

Set permissions boundary

Cancel

Previous

Next: Review

Click Here

Click Here

Add user

1

2

3

4

Review

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

User details

User name	stephane
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess
Managed policy	IAMUserChangePassword

Cancel

Previous

Create user

Click Here

Add user

1

2

3

4



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://387124123361.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
▶	✔ stephane	AKIAVUITFK3Q7MTKILYT	***** Show	***** Show	Send email ↗

Add user

Please download the credentials.csv now

**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://387124123361.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password
▶	✓ stephane	AKIAVUITFK3Q7MTKILYT	***** Show	***** Show

Email login instructions

[Send email](#)

Or save the password here to a text file

Close

Add user

1

2

3

4



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://387124123361.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password
▶	✔ stephane	AKIAVUITFK3Q7MTKILYT	***** Show	***** Show

Email login instructions

Send email

The screenshot displays the AWS IAM console interface. At the top, the AWS logo is on the left, and navigation links for 'Services', 'Resource Groups', and a star icon are on the right. The left sidebar contains a search bar labeled 'Search IAM' and a list of navigation items: 'Dashboard', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. A yellow callout box with an arrow points to the 'Users' link, containing the text 'Click Here'. The main content area features two buttons at the top: 'Add user' (blue) and 'Delete user' (red). Below these is a search bar labeled 'Find users by username or access key'. A table lists the users, with one user named 'stephane' shown. The table has columns for 'User name' and 'Groups'.

User name	Groups
stephane	None

Dashboard

[Groups](#)[Users](#)[Roles](#)[Policies](#)[Identity providers](#)[Account settings](#)[Credential report](#)[Encryption keys](#)

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console>

[Customize](#)

IAM Resources

Users: 1

Roles: 2

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

3 out of 5 complete.



Delete your root access keys



Activate MFA on your root account



Create individual IAM users



Use groups to assign permissions





Use IAM groups to assign permissions to your IAM users to simplify managing and auditing permissions in your account. [Learn More](#)

[Manage Groups](#)

Click Here

IAM password policy



 Services ▾ Resource Groups ▾ 

Dashboard

Groups

Users

Roles

Policies

Identity providers


Account settings

Credential report

Encryption keys

Create New Group

Group Actions ▾


Click Here

<input type="checkbox"/>	Group Name ↕	Users
No records found.		

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:

Example: Developers or ProjectAlpha
Maximum 128 characters

Cancel

Next Step

Click Here

Attach Policy

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

Filter: Policy Type

Showing 358 results

	Policy Name ↕	Attached Entities ↕	Creation Time ↕	Edited Time ↕
<input checked="" type="checkbox"/>	AdministratorAccess	1	2015-02-06 19:39 UTC+0200	2015-02-06 19:39 UTC+0200
	IAMUserChangePassword	1	2016-11-15 01:25 UTC+0200	2016-11-16 00:18 UTC+0200
	AlexaForBusinessDeviceSetup	0	2017-11-30 17:47 UTC+0200	2017-11-30 17:47 UTC+0200
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 17:47 UTC+0200	2018-06-26 01:53 UTC+0200
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	2017-11-30 17:47 UTC+0200	2017-11-30 17:47 UTC+0200
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	2017-11-30 17:47 UTC+0200	2018-06-26 01:52 UTC+0200
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	2015-07-09 19:34 UTC+0200	2015-07-09 19:34 UTC+0200
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 19:36 UTC+0200	2015-07-09 19:36 UTC+0200
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudW...	0	2015-11-12 00:41 UTC+0200	2015-11-12 00:41 UTC+0200
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-06 19:40 UTC+0200	2018-09-10 19:29 UTC+0200
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	2015-02-06 19:40 UTC+0200	2016-12-07 22:00 UTC+0200
<input type="checkbox"/>	AmazonAppStreamServiceAccess	0	2016-11-19 05:17 UTC+0200	2018-08-13 20:19 UTC+0200

Cancel

Previous

Next Step

Click Here

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Review

Review the following information, then click **Create Group** to proceed.

Group Name	admin	Edit Group Name
Policies	arn:aws:iam::aws:policy/AdministratorAccess	Edit Policies

Cancel

Previous

Create Group

Click Here

The screenshot displays the AWS IAM console interface. At the top, the AWS logo is on the left, and navigation links for 'Services' and 'Resource Groups' are in the center. A left-hand sidebar contains a search bar labeled 'Search IAM' and a list of navigation items: 'Dashboard', 'Groups' (which is highlighted with an orange bar), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. The main content area has a dark header with a 'Create New Group' button and a 'Group Actions' dropdown menu. Below this is a table of IAM groups. The table has a 'Filter' input at the top, followed by a header row with a checkbox, 'Group Name', and 'Users'. A single row is visible, representing the 'admin' group, which is highlighted in light blue. A yellow arrow points to the 'admin' group name, and a yellow box with the text 'Click Here' is positioned below the arrow.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

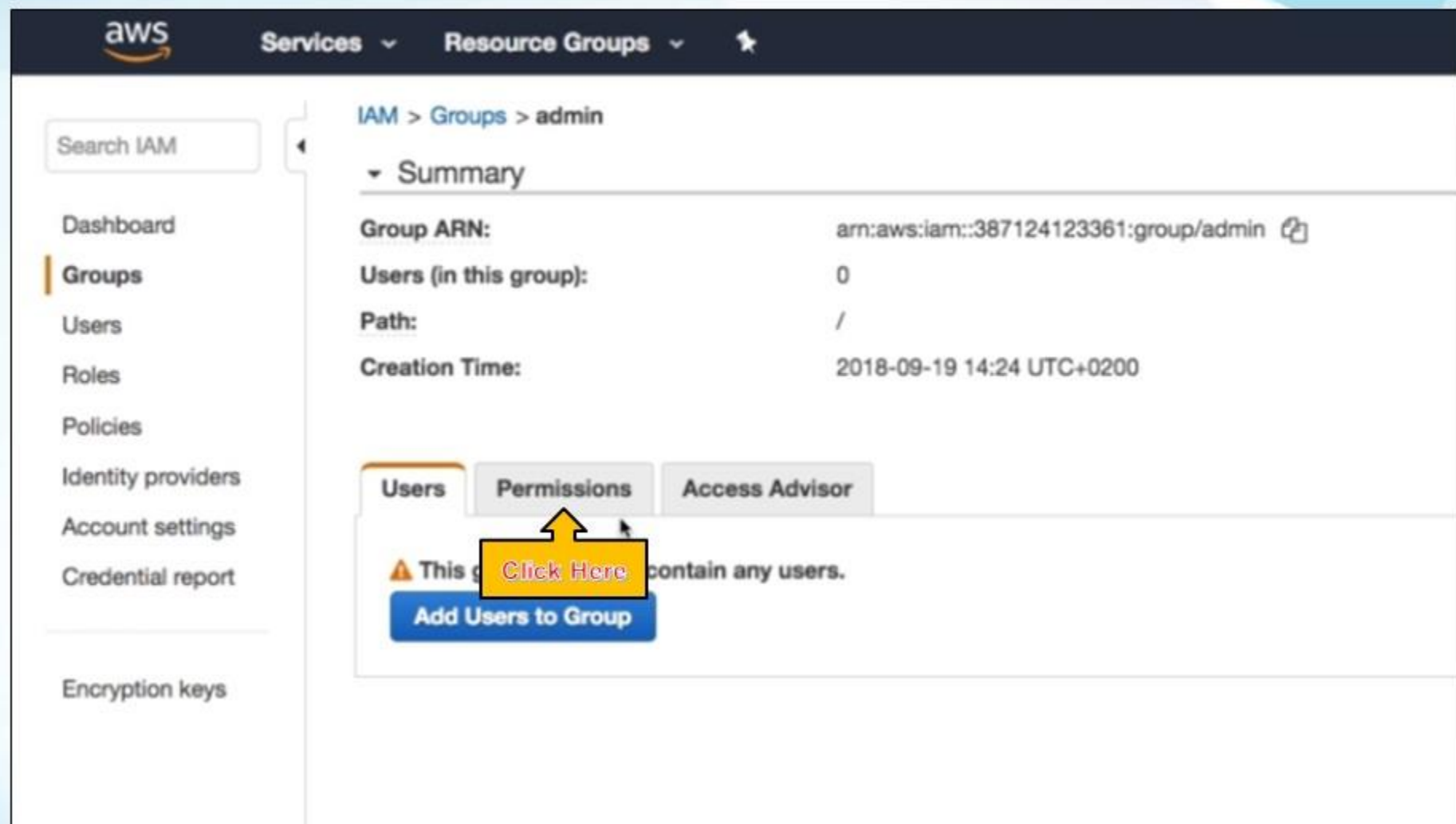
Encryption keys

Create New Group Group Actions

Filter

<input type="checkbox"/>	Group Name	Users
<input type="checkbox"/>	admin	0

Click Here



aws Services ▾ Resource Groups ▾ ⭐

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers


Account settings

Credential report

Encryption keys

IAM > Groups > admin

▼ Summary

Group ARN: arn:aws:iam::387124123361:group/admin 

Users (in this group): 0

Path: /

Creation Time: 2018-09-19 14:24 UTC+0200

Users Permissions Access Advisor

⚠ This group contains any users. [Click Here](#)

Add Users to Group

Encryption keys

- Summary

Creation Time: 2018-09-19 14:24 UTC+0200

Access Advisor

[Click Here](#)

and Policies

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

Attach Policy

Policy Name	Actions
 AdministratorAccess	Show Policy Detach Policy Simulate Policy

Inline Policies

aws Services ▾ Resource Groups ▾ ⚙

Search IAM

- Dashboard
- Groups**
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Encryption keys

IAM > Groups > admin

▾ Summary

Group ARN:	arn:aws:iam::387124123361:group/admin
Users (in this group):	0
Path:	/
Creation Time:	2018-09-19 14:24 UTC+0200

Users Permissions Access Advisor

This group does not contain any users.

Add Users to Group

Click Here

aws

Services

Resource Groups

Add Users to Group

Select users to add to the group admin

Filter

<input type="checkbox"/>	User Name ↕	Groups	Password	Password Last Used ↕
<input type="checkbox"/>	stephane	0	✓	Never

Click Here

Select users to add to the group admin

<input type="text" value="Filter"/>						Showing 1 results
<input type="checkbox"/>	User Name ↕	Groups	Password	Password Last Used ↕	Access Keys	Creation Time ↕
<input checked="" type="checkbox"/>	stephane	0	✓	Never	1 active	2018-09-19 14:23 UTC...

Cancel

Add Users

Click Here

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

IAM > Groups > admin

Summary

Group ARN: arn:aws:iam::387124123361:group/admin 

Users (in this group): 1


Path: /

Creation Time: 2018-09-19 14:24 UTC+0200

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

This view shows 1 users in this group: 1 User

[Click Here](#)

User	Actions
 stephane	Remove User from Group

IAM > Groups > admin

▼ Summary

Group ARN: arn:aws:iam::387124123361:group/admin 

Users (in this group): 1

Path: /

Creation Time: 2018-09-19 14:24 UTC+0200

Users

Permissions

Access Advisor

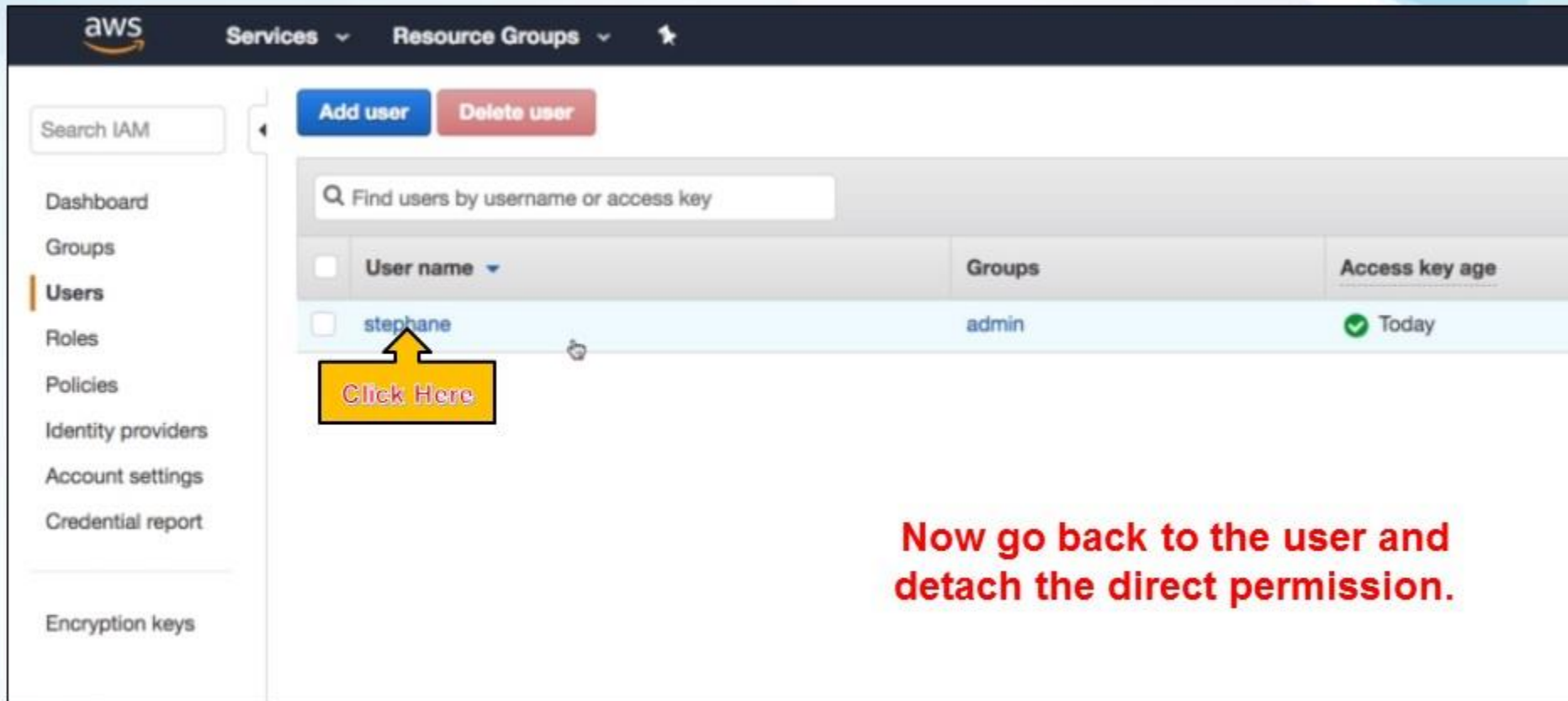
Managed Policies

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

[Attach Policy](#)

Policy Name	Actions
 AdministratorAccess	Show Policy Detach Policy Simulate Policy

Inline Policies



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with links to Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The 'Users' link is highlighted. The main content area has a top bar with 'Add user' and 'Delete user' buttons. Below this is a search bar labeled 'Find users by username or access key'. A table lists IAM users with columns for 'User name', 'Groups', and 'Access key age'. One user, 'stephane', is listed with the group 'admin' and an access key age of 'Today'. A yellow callout box with an arrow points to the 'stephane' user, containing the text 'Click Here'.

User name	Groups	Access key age
stephane	admin	Today

Click Here

Now go back to the user and detach the direct permission.

Users > stephane

Summary

User ARN arn:aws:iam::387124123361:user/stephane

Path /

Creation time 2018-09-19 14:23 UTC+0200

Permissions

Groups (1)

Security credentials

Access Advisor

Permissions policies (3 policies applied)

Add permissions

Add inline policy

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy
Show 2 more	

Permissions boundary (not set)

Click Here

Users > stephane

Summary

User ARN

arn

Path

/

Creation time

20

Detach policy

Are you sure you want to detach policy **AdministratorAccess** from user **stephane** ?[Cancel](#)[Detach](#)

Click Here

Permissions

Groups (1)

Security credentials

Access Advisor


▼ Permissions policies (3 policies applied)

[Add permissions](#)


Policy name ▼

Policy type ▼

Attached directly

▶  AdministratorAccess

AWS managed policy

▶  IAMUserChangePassword

AWS managed policy

[Show 2 more](#)

[Dashboard](#)[Click Here](#)[Users](#)[Roles](#)[Policies](#)[Identity providers](#)[Account settings](#)[Credential report](#)[Encryption keys](#)[Users](#) > stephane

Summary

Policy has been detached from the user stephane



User ARN `arn:aws:iam::387124123361:user/stephane` 

Path /

Creation time 2018-09-19 14:23 UTC+0200

[Permissions](#)[Groups \(1\)](#)[Security credentials](#)[Access Advisor](#)[Add user to groups](#)

Group name ▼	Attached permissions
admin	AdministratorAccess

 Services ▾ Resource Groups ▾ 

Search IAM

Dashboard

Groups

Users

Roles

Policies


Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management












IAM users sign-in link:
<https://387124123361.signin.aws.amazon.com/console>  [Customize](#)


IAM Resources

Users: 1	Roles: 2
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

4 out of 5 complete.

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


Click Here

Dashboard

[Groups](#)[Users](#)[Roles](#)[Policies](#)[Identity providers](#)[Account settings](#)[Credential report](#)[Encryption keys](#)

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console>

[Customize](#)

IAM Resources

Users: 1

Roles: 2

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0

Security Status

4 out of 5 complete.

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

Use a password policy to require your IAM users to create strong passwords and to rotate their passwords regularly. [Learn More](#)

[Manage Password Policy](#)

Click Here

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with links to Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings (highlighted), Credential report, and Encryption keys. The main content area is titled 'Password Policy'. It contains a description of password policies and a list of configuration options. A yellow arrow points to the 'Enable password expiration' checkbox, which is labeled 'Click Here'.

Search IAM

Account settings

Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

- ☐ Require at least one uppercase letter ⓘ
- ☐ Require at least one lowercase letter ⓘ
- ☐ Require at least one number ⓘ
- ☐ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☐ Enable password expiration ⓘ

Click Here

Password expiration period (in days):

☐ Password reuse ⓘ

Number of passwords to remember:

☐ Password expiration requires administrator reset ⓘ

Apply password policy **Delete password policy**

Security Token Service Regions

You can enable additional regions from which you can request temporary credentials. Activate only the r

Feedback **English (US)**

The screenshot shows the AWS IAM console interface. On the left, the navigation menu includes 'Search IAM', 'Dashboard', 'Groups', 'Roles', 'Policies', 'Identity providers', 'Account settings' (highlighted with an orange box and 'Click Here' text), 'Credential report', and 'Encryption keys'. The main content area is titled 'Password Policy'. A yellow banner at the top of this section states 'You have unsaved changes to your password policy.' Below this, a paragraph explains that a password policy defines rules for IAM users and refers to 'Managing Passwords' in the 'Using IAM' guide. It then states that the current AWS account does not have a password policy and prompts the user to specify one. The configuration options include: 'Minimum password length' (set to 6), a list of requirements (Require at least one uppercase letter, lowercase letter, number, non-alphanumeric character, Allow users to change their own password, Enable password expiration, Prevent password reuse, and Password expiration requires administrator reset), 'Password expiration period (in days)' (set to 90), and 'Number of passwords to remember'. The 'Apply password policy' button is highlighted with an orange box and 'Click Here' text. The bottom of the page features a 'Feedback' link and 'English (US)' language selection.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Click Here

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

▼ Password Policy

You have unsaved changes to your password policy.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

- ☐ Require at least one uppercase letter ⓘ
- ☐ Require at least one lowercase letter ⓘ
- ☐ Require at least one number ⓘ
- ☐ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☒ Enable password expiration ⓘ



Password expiration period (in days):

- ☐ Prevent password reuse ⓘ
-
- Number of passwords to remember:
- ☐ Password expiration requires administrator reset ⓘ

Apply password policy **Delete password policy**

Click Here


Feedback English (US)

 Services ▾ Resource Groups ▾ 

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

Encryption keys

Welcome to Identity and Access Management




IAM users sign-in link:
<https://387124123361.signin.aws.amazon.com/console>  [Customize](#)

IAM Resources

Users: 1	Roles: 2
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

5 out of 5 complete.

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

Now copy past the IAM user sign-in link and login with IAM User.

You can also create an alias to the link by clicking on "Customize"

Welcome to Identity and Access Management

IAM users sign-in link:

<https://387124123361.signin.aws.amazon.com/console>

[Customize](#)

IAM Resources

Users: 1

Roles: 2

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0

Security Status

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

Create Account Alias

Account Alias

Cancel

Yes, Create

Click Here

Dashboard

[Groups](#)[Users](#)[Roles](#)[Policies](#)[Identity providers](#)[Account settings](#)[Credential report](#)[Encryption keys](#)

Welcome to Identity and Access Management

IAM users sign-in link:

<https://datacumulus-courses.signin.aws.amazon.com/console>

[Customize](#)

IAM Resources

Users: 1

Roles: 2

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0


Security Status

5 out of 5 complete.

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

IAM Management Console x Amazon Web Services Sign-In x +

← → ↻ https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-S



Account ID or alias

IAM user name

Password

Sign In

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



Account ID or alias

datacumulus-courses



IAM user name

stephane



Password



Sign In

[Sign-in using root credentials](#)

Click Here



You must change your password to continue

AWS account 387124123361



IAM user name stephane

Old password



New password



Retype new password



Confirm password change

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

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2018, Amazon Web Services, Inc. or its affiliates.

AWS account 387124123361



IAM user name stephane

Old password



New password



Retype new password



Confirm password change

Sign-in using

Click Here

State

English



Services
Resource Groups

stephane @ datacumulus-cour...
Paris
Support

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

IAM

EC2

VPC

CloudFormation

Billing

> All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
~2-3 minutes

Build a web app
With Elastic Beanstalk
~8 minutes

Build using virtual servers
With Lightsail
~1-2 minutes

Connect an IoT device
With AWS IoT
~5 minutes

Start a development project
With CodeStar
~5 minutes

Register a domain
With Route 53
~3 minutes

See more

Learn to build

Learn to deploy your solutions through step-by-step guides, labs, and videos.

Websites

DevOps

Backup and recovery

See all

Helpful tips

Manage your costs
Monitor your AWS costs, usage, and reservations using AWS Budgets. [Start now](#)

Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. [Start now](#)

Explore AWS

Machine Learning with Amazon SageMaker
The fastest way to build, train, and deploy machine learning models. [Learn more.](#)

Amazon Relational Database Service (RDS)
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. [Learn more.](#)

AWS Fargate Runs Containers for You
AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you need, scale quickly, and run any size application. [Learn more.](#)

Click Here

[Services](#)
[Resource Groups](#)

stephane @ datacumulus-cour...

Paris

Support

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

IAM

EC2

VPC

Billing

Click Here

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
 With EC2
 ~2-3 minutes

Build a web app
 With Elastic Beanstalk
 ~8 minutes

Build using virtual servers
 With Lightsail
 ~1-2 minutes

Connect an IoT device
 With AWS IoT
 ~5 minutes

Start a development project
 With CodeStar
 ~5 minutes

Register a domain
 With Route 53
 ~3 minutes

See more

Helpful tips

Manage your account
 Monitor your reservations

Create and manage IAM users
 Use AWS IAM console to manage your users

IAM User:
stephane

Account:
datacumulus-courses

My Account

My Organization

My Billing Dashboard

My Security Credentials

Switch Role

Sign Out

Explore AWS

Machine Learning with Amazon SageMaker
 The fastest way to build, train, and deploy machine learning models. [Learn more.](#)

Amazon Relational Database Service (RDS)
 RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. [Learn more.](#)

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a star icon. A search bar labeled 'Search IAM' is on the left. Below it, a sidebar lists navigation options: Dashboard (highlighted), Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management'. It features a section for 'IAM users sign-in link' with the URL 'https://datacumulus-courses.signin.aws.amazon.com/console' and a 'Customize' link. Below this is the 'IAM Resources' section, which displays counts for Users (1), Groups (1), Roles (2), and Identity Providers (0). The 'Security Status' section shows a progress bar at '5 out of 5 complete' and a list of five security checks, all of which are marked as complete with green checkmarks: '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'.

aws Services Resource Groups

Search IAM

Dashboard

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

<https://datacumulus-courses.signin.aws.amazon.com/console> [Customize](#)

IAM Resources

Users: 1 Roles: 2

Groups: 1 Identity Providers: 0

Customer Managed Policies: 0

Security Status

5 out of 5 complete.

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

Exercise

Alice is an intern who has joined your organization as an intern System Administrator. Since your infrastructure is hosted in AWS, you need to give access to Alice to view the AWS console.

Thank You