

Imran Teli | Create IAM User.

→ Login to AWS account => Services => IAM

The screenshot shows the AWS IAM Management Console home page. On the left, there's a sidebar with links like Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area has a "Welcome to Identity and Access Management" section with a sign-in link. It also displays IAM Resources (Users: 1, Groups: 0, Roles: 2, Customer Managed Policies: 0) and a Security Status checklist with five items, three of which are checked (Delete your root access keys, Activate MFA on your root account, Create individual IAM users). To the right, there's a "Feature Spotlight" section with a video player showing an "Introduction to AWS IAM" video, and an "Additional Information" section with links to IAM documentation, Web Identity Federation Playground, Policy Simulator, and Videos, IAM release history and additional resources.

The screenshot shows the AWS IAM Management Console users page. The sidebar includes links for Dashboard, Groups, **Users**, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area features a search bar and a table titled "Showing 1 result". The table has columns for User name, Groups, Password, Last sign-in, Access keys, and Creation time. One user, "kops", is listed with 0 groups, N/A password, 1 active access key, and a creation time of 2017-03-26 13:01 UTC+0530.



IAM Management Console - Chromium

IAM Management Services Resource Groups Imran Global Support

Add user

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.

* Required

Cancel Next: Permissions



IAM Management Console - Chromium

IAM Management Services Resource Groups Imran Global Support

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

 Show password

Require password reset User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel Next: Permissions



Imran Teli

→ Attach Policy to the User.

The screenshot shows the AWS IAM Management Console interface. At the top, there are three options: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. The third option is highlighted with a blue background. Below this, a section titled 'Attach one or more existing policies directly to the user or create a new policy.' includes a 'Create policy' button and a 'Refresh' button. A search bar labeled 'Search' and a filter dropdown 'Filter: Policy type' are also present. The main area displays a list of 254 results, with the first few items being: 'AdministratorAccess' (selected), 'AmazonAPIGatewayAdministrator', 'AmazonAPIGatewayInvokeFullAccess', 'AmazonAPIGatewayPushToCloudWatchLogs', 'AmazonAppStreamFullAccess', 'AmazonAppStreamReadOnlyAccess', 'AmazonAppStreamServiceAccess', 'AmazonAthenaFullAccess', 'AmazonCloudDirectoryFullAccess', and 'AmazonCloudFrontReadonlyAccess'. Each item has a checkbox, a policy icon, a name, a type (e.g., 'Job function', 'AWS managed'), and a brief description. At the bottom of the page, there are links for 'Feedback', 'English', 'Cancel', 'Previous', 'Next', 'Review', and copyright information.

The screenshot shows the 'Review' step of creating a new user. The title 'Visualpath Imran Teli' is displayed prominently at the top. The interface includes a 'Details' step (blue circle), a 'Permissions' step (blue circle), a 'Review' step (blue circle, currently active), and a 'Complete' step (grey circle). The 'Review' section contains a 'Review' heading and a note: 'Review your choices. After you create the user, you can view and download the autogenerated password and access key.' Below this is a 'User details' section with fields: 'User name' (devopsadmin), 'AWS access type' (AWS Management Console access - with a password), 'Console password type' (Custom), and 'Require password reset' (No). The 'Permissions summary' section indicates that the 'AdministratorAccess' policy will be attached. At the bottom, there are 'Cancel', 'Previous', 'Create user' (highlighted in blue), and 'Complete' buttons.

The screenshot shows the completion of the user creation process. The title 'Visualpath Imran Teli' is displayed. The 'Create user' button is highlighted in blue. Below it, the 'Cancel', 'Previous', and 'Complete' buttons are visible. The footer includes standard links: 'Feedback', 'English', 'Cancel', 'Previous', 'Create user', 'Next', 'Review', 'Complete', 'Privacy Policy', and 'Terms of Use'. The copyright notice '© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.' is also present.

Imran Teli

The screenshot shows the AWS IAM Management Console interface. At the top, there's a navigation bar with tabs for Services and Resource Groups. Below the navigation is a progress bar with four steps: Details (step 1), Permissions (step 2), Review (step 3), and Complete (step 4, highlighted in blue). A success message box is displayed, stating: "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." It includes a link to "Email login instructions" and a "Send email" button. A "Download .csv" button is also present. The main table lists one user: "User" devopsadmin. At the bottom right of the table is a "Close" button. The footer of the page includes links for Feedback, English, Privacy Policy, and Terms of Use.

The screenshot shows the AWS IAM Management Console interface. The left sidebar has a navigation menu with options like Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, and Credential report. Below this is an "Encryption keys" section. The main content area shows a table of users. The table has columns for User name, Groups, Password, Last sign-in, Access keys, and Creation time. Two users are listed: "devopsadmin" and "kops". The "devopsadmin" row is currently selected, indicated by a cursor icon over its "User name" field. The table shows 0 groups, N/A password, N/A last sign-in, and None access keys. The creation times are 2017-04-11 21:55 UTC+0530 and 2017-03-26 13:01 UTC+0530 respectively. The footer of the page includes links for Feedback, English, Privacy Policy, and Terms of Use.

Imran Teli

→ Click on Assigned MFA device.

The screenshot shows the AWS IAM Management Console for the user 'devopsadmin'. The 'Security credentials' tab is selected. Under 'Sign-in credentials', the 'Assigned MFA device' field is set to 'No' with a pencil icon, which is highlighted with a red box. Other fields shown include 'Console password' (Enabled), 'Console login link' (https://[REDACTED]signin.aws.amazon.com/console), and 'Last login' (Never). The 'Access keys' section shows no results. The 'SSH keys for AWS CodeCommit' section also shows no results.



The screenshot shows the 'Manage MFA Device' dialog box open over the IAM console. The dialog box asks to 'Select the type of MFA device to activate:' with two options: 'A virtual MFA device' (selected) and 'A hardware MFA device'. Below the dialog, a note says 'For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)'. The background shows the IAM console for the user 'devopsadmin' with the 'Security credentials' tab selected. The 'Assigned MFA device' field still shows 'No'.

Imran Teli

Imran Teli

Download google authenticator in your smartphone => Open google authenticator => Click plus symbol => Scan the barcode => Enter Auth code1 => Enter second auth code.

The screenshot shows the AWS IAM Management Console for a user named 'devopsadmin'. A modal window titled 'Manage MFA Device' is open. It contains instructions to scan a QR code with a smartphone's camera. Below the QR code are two input fields labeled 'Authentication Code 1' and 'Authentication Code 2'. At the bottom right of the modal are 'Cancel', 'Previous', and 'Activate Virtual MFA' buttons.

→ Use the highlighted URL for your user to login to aws account with IAM user.

The screenshot shows the AWS IAM Management Console for a user named 'devopsadmin'. The 'Security credentials' tab is selected. Under the 'Sign-in credentials' section, there is a table with rows for 'Console password', 'Console login link' (which is highlighted with a red box), 'Last login', 'Assigned MFA device', and 'Signing certificates'. The 'Console login link' row contains the URL 'https://signin.aws.amazon.com/console'. At the bottom of the page, there is a table for 'Access keys' with one row listed: 'Access key ID' (highlighted with a red box), 'Created', and 'Last used'. The 'Status' column shows 'No results'.

Imran Teli

Imran Teli Creating Ec2 Instance.

Create 1 ec2 instance with centos 6 AMI.

Step 1: Choose an Amazon Machine Image (AMI)

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

Categories

All Categories

Software Infrastructure (155)

Developer Tools (7)

Business Software (5)

Operating System

All Linux/Unix

Amazon Linux (6)

CentOS (150)

CentOS 7 (x86_64) - with Updates HVM

★★★★★ (44) | 1602 | Sold by CentOS.org

\$0.00/hr for software + AWS usage fees

Linux/Unix, CentOS 7 | 64-bit Amazon Machine Image (AMI) | Updated: 2/26/16

This is the Official CentOS 7 x86_64 HVM image that has been built with a minimal profile, suitable for use in HVM instance types only. The image contains just enough packages to ...

More info

CentOS 6 (x86_64) - with Updates HVM

★★★★★ (32) | 1602 | Sold by CentOS.org

\$0.00/hr for software + AWS usage fees

Linux/Unix, CentOS 6 | 64-bit Amazon Machine Image (AMI) | Updated: 2/26/16

This is the Official CentOS 6 x86_64 HVM image that has been built with a minimal profile. The image contains just enough packages to run within AWS, bring up an SSH Server and ...

More info

CentOS 6.5 (x86_64) - Release Media

★★★★★ (55) | 6.5 - 2013-12-01 | Sold by CentOS.org

Select

Select

Select

Feedback English

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

EC2 Management

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 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)

Note: The vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
0	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
1	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
2	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
3	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
4	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
5	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
6	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
7	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Feedback English

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Visualpath

Imran Teli

Review and Launch Review and Edit

Imran Teli

EC2 Management x https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard:

Services Resource Groups

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

Number of instances 1 Launch into Auto Scaling Group

Purchasing option Request Spot Instances

Network vpc-9610c2f2 (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

IAM role None Create new IAM role

Shutdown behavior Stop

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring Additional charges apply.

Tenancy Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

► Advanced Details

Cancel Previous Review and Launch Next: Add Storage

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Imran Teli

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-f711c830	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use



Imran Teli

The screenshot shows the AWS EC2 Launch Instance Wizard at Step 5: Add Tags. The URL is <https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard>. The page title is "EC2 Management" and the sub-page title is "Launch instance". The navigation bar includes "Services", "Resource Groups", "Imran", "N. California", and "Support". The main content area shows a table for adding tags. A single tag is being added with the key "Name" and value "elbtestproj-web1". There is a button to "Add another tag" and a note stating "(Up to 50 tags maximum)". The top navigation bar also includes "Choose AMI", "Choose Instance Type", "Configure Instance", "Add Storage", "Configure Security Group", and "Review".

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)
Name		elbtestproj-web1	<input type="button" value="X"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

The screenshot shows the AWS EC2 Launch Instance Wizard at Step 6: Configure Security Group. The URL is <https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard>. The page title is "EC2 Management" and the sub-page title is "Launch instance". The navigation bar includes "Feedback", "English", "Services", "Resource Groups", "Imran", "N. California", and "Support". The main content area shows the "Assign a security group:" section. The user has selected "Create a new security group" and entered "elbtestproj-SG" as the name. Below this, there is a table for defining security rules. Two rules are listed: one for SSH (Protocol TCP, Port Range 22, Source My IP, 183.82.216.42/32) and one for HTTP (Protocol TCP, Port Range 80, Source Anywhere, 0.0.0.0/:/0). There is a "Description" field containing "elbtestproj-SG". At the bottom, there is a "Add Rule" button. The top navigation bar also includes "Choose AMI", "Choose Instance Type", "Configure Instance", "Add Storage", "Configure Security Group", and "Review".

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group

Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	My IP 183.82.216.42/32
HTTP	TCP	80	Anywhere 0.0.0.0/:/0

[Add Rule](#)

[Cancel](#) [Previous](#) [Review and Launch](#)

The screenshot shows the AWS EC2 Launch Instance Wizard at Step 6: Configure Security Group. The URL is <https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard>. The page title is "EC2 Management" and the sub-page title is "Launch instance". The navigation bar includes "Feedback", "English", "Services", "Resource Groups", "Imran", "N. California", and "Support". The main content area shows the "Review and Launch" section. It lists the instance configuration: AMI: Amazon Linux 2017.03, Instance Type: t2.micro, Volume Type: Standard, and Security Group: elbtestproj-SG. Below this, there is a "Launch instance" button. The top navigation bar also includes "Choose AMI", "Choose Instance Type", "Configure Instance", "Add Storage", "Configure Security Group", and "Review".

Visualpath
Imran Teli

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

CentOS 6 (x86_64) - with Updates HVM
Free tier eligible
CentOS Linux 6 x86_64 HVM EBS 1602
Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t2.micro instance (Additional taxes may apply.)
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement.

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name: elbtestproj-SG
Description: elbtestproj-SG

Type: Protocol: Port Range: Source: **Cancel Previous Launch**

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

CentOS 6 (x86_64) - with Updates HVM
Free tier eligible
CentOS Linux 6 x86_64 HVM EBS 1602
Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t2.micro instance (Additional taxes may apply.)
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement.

Instance Type

Instance Type	ECUs	vCPUs
t2.micro	Variable	1

Security Groups

Security group name: elbtestproj-SG
Description: elbtestproj-SG

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair
Key pair name: elbtestproj-ncalifornia
Download Key Pair

You have to download the **private key file (*.pem file)** before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Visualpath
Imran Teli