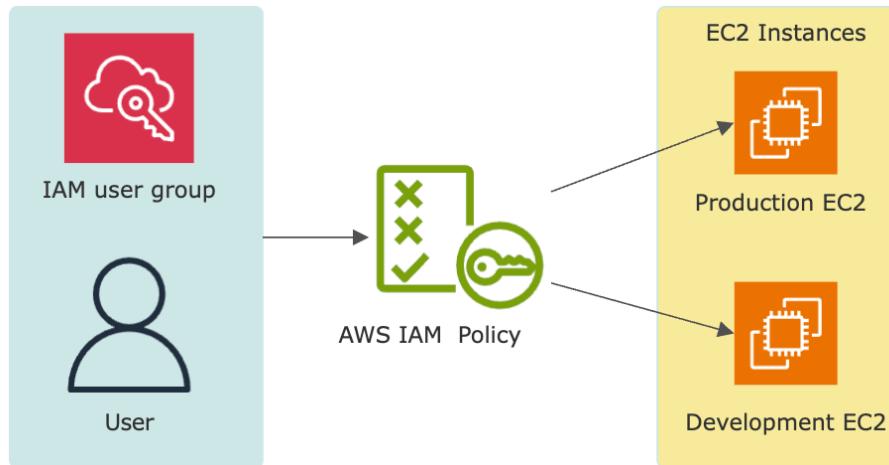


New Employee's Dev-Env Access with AWS IAM

I will be using the AWS Identity and Access Management (IAM) service to control who is authenticated (signed in) and authorized (has permissions) in your AWS console. In this scenario a new employee who just joined would need development environment access and I will show how to give that access with AWS IAM. See diagram below.



Note: make sure you select the closest region before starting for better performance.

Launch EC2 instances:

Note: Create two EC2 instances for production and development environments.

1. Launch an instance for prod.

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name	<input type="text" value="nextwork-prod-dhruval"/>	Add additional tags
------	--	-------------------------------------

2. Choose Add additional tags, which is right next to the Name field.

- a. Choose Add new tag.
- b. For the next tag, use this information:
 - i. Key: Env
 - ii. Value: production

Name and tags [Info](#)

Key Info	Value Info	Resource types Info
<input type="text" value="Name"/> X	<input type="text" value="nextwork-prod-dhruval"/> X	Select resource types ▼
Remove		
Instances X		
Key Info	Value Info	Resource types Info
<input type="text" value="Env"/> X	<input type="text" value="production"/> X	Select resource types ▼
Remove		
Instances X		
Add new tag		

You can add up to 48 more tags.

3. Select free tier Amazon Machine Image (AMI).

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

[Recents](#) [Quick Start](#)

 Amazon Linux	 Ubuntu	 Windows	 Red Hat	 SUSE Linux	 Debian
---	---	--	--	---	---

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-Oce45259f491c3d4f (64-bit (x86), uefi-preferred) / ami-0e26b1cd66cd6665c (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible ▼
---	--------------------------------------

Description
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.7.20250414.0 x86_64 HVM kernel-6.1

Architecture 64-bit (x86) ▼	Boot mode uefi-preferred	AMI ID ami-Oce45259f491c3d4f	Publish Date 2025-04-11	Username ① ec2-user	Verified provider
--	-----------------------------	---------------------------------	----------------------------	--	-----------------------------------

4. Select default free tier instance type.

Instance type [Info](#) | [Get advice](#)

Instance type

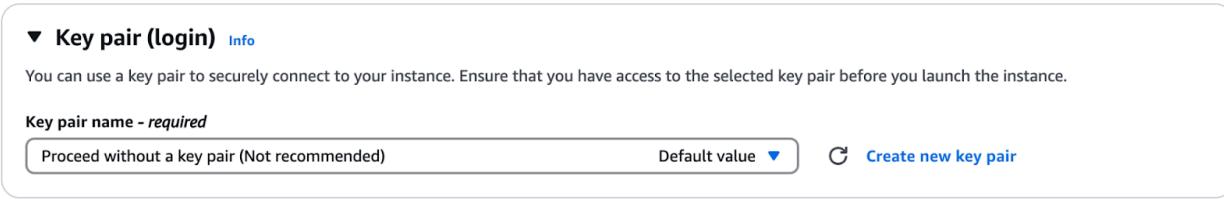
t2.micro	Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Ubuntu Pro base pricing: 0.0156 USD per Hour On-Demand RHEL base pricing: 0.0282 USD per Hour On-Demand SUSE base pricing: 0.0138 USD per Hour On-Demand Windows base pricing: 0.0184 USD per Hour On-Demand Linux base pricing: 0.0138 USD per Hour	▼

[All generations](#)

[Compare instance types](#)

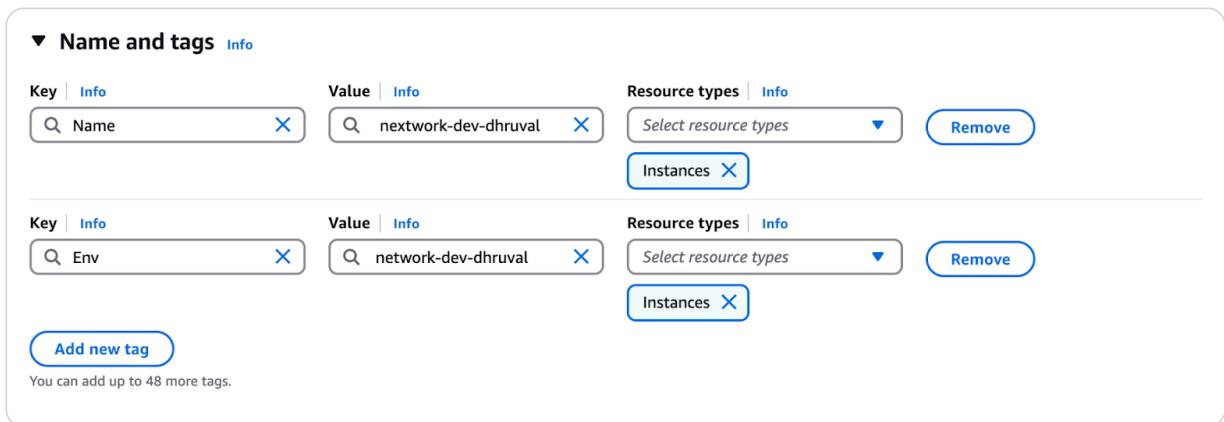
Additional costs apply for AMIs with pre-installed software

5. For the key pair select, proceed without keypair (not recommended but for this project no need for SSH).



6. Leave network settings and Configure storage default and then click Launch Instance.

7. Repeat the same steps for creating the dev EC2 instance. Keep Amazon Machine Image (AMI), instance type, and key pair same Just change the EC2 instance name and the env value to development in tags. EC2 See screenshots below



You should have successfully created the 2 new EC2 instances

Instances (2/3) Info									
Last updated less than a minute ago Connect Actions Launch instances									
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/> All states ▼									
	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼	Public IPv4 DNS ▼	Public IPv
<input type="checkbox"/>	network-prod-...	i-0f9ab691e09907b3a	Terminated Q Q	t2.micro	-	View alarms +	us-west-1c	-	-
<input checked="" type="checkbox"/>	network-dev-...	i-0445c5fbae77d2ab9	Running Q Q	t2.micro	2/2 checks passed Q Q	View alarms +	us-west-1c	ec2-54-183-117-102.us...	54.183.11
<input checked="" type="checkbox"/>	network-prod-...	i-0f6625cc137d757ef	Running Q Q	t2.micro	2/2 checks passed Q Q	View alarms +	us-west-1c	ec2-54-176-228-57.us...	54.176.22

Note: double check tags for both instances

i-0f6625cc137d757ef (network-prod-dhruval)

Details | Status and alarms | Monitoring | Security | Networking | Storage | **Tags**

Tags

Key	Value
Name	network-prod-dhruval
Env	production

i-0445c5fbea77d2ab9 (network-dev-dhruval)

Details | Status and alarms | Monitoring | Security | Networking | Storage | **Tags**

Tags

Key	Value
Name	network-dev-dhruval
Env	dev

Create an IAM Policy:

Now it's time to give permissions with appropriate policy to the employee who just joined.

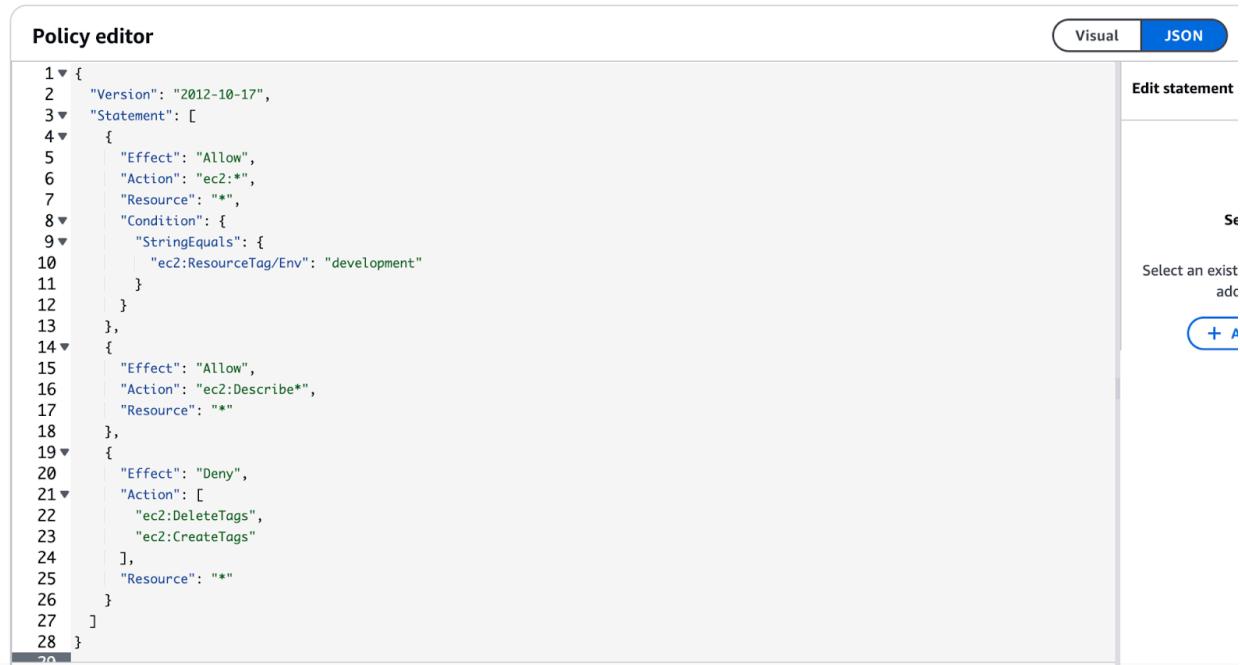
1. Head to AWS IAM.

The screenshot shows the AWS IAM service page. The search bar at the top has 'iam' typed into it. The main content area is titled 'Services' and features a prominent 'IAM' service card. The IAM card includes a red icon, the text 'Manage access to AWS resources', and a 'Top features' section with links for Groups, Users, Roles, Policies, and Access Analyzer. To the left, there's a sidebar with links for Identity and Management, Services, Features, Resources (New), Documentation, Knowledge articles, and Marketplace. The 'Identity and Management' link is currently selected.

2. Then from the left navigation section select “policies” and then top right select “Create Policy”.
3. Then Switch the Policy editor tab to JSON format. Create JSON format to allow EC2 instances with development tag and then select “Next”. See screenshot below.

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.



```

1 ▼ {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:*",
7       "Resource": "*",
8       "Condition": {
9         "StringEquals": {
10           "ec2:ResourceTag/Env": "development"
11         }
12       },
13     },
14     {
15       "Effect": "Allow",
16       "Action": "ec2:Describe*",
17       "Resource": "*"
18     },
19     {
20       "Effect": "Deny",
21       "Action": [
22         "ec2:DeleteTags",
23         "ec2>CreateTags"
24       ],
25       "Resource": "*"
26     }
27   ]
28 }

```

4. Fill in policy's details:

- Name: NextWorkDevEnvironmentPolicy
- Description: IAM Policy for NextWork's development environment
- And then select “Create policy”

Policy details

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+-=,@-_' characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+-=,@-_' characters.

Create an AWS Account Alias:

Since the permission policy is set up now an account alias would be needed. This is the name for the AWS account that can be used instead of the account ID to sign in to the AWS Management Console.

- From the IAM Dashboard select create account alias on the right.

IAM Dashboard Info

The screenshot shows the IAM Dashboard. On the left, under 'Security recommendations', there are two items: 'Add MFA for root user' (with a note about enabling MFA for the root user) and 'Root user has no active access keys' (with a note about using access keys attached to an IAM user). On the right, the 'AWS Account' section displays the 'Account ID' (471744311739), 'Account Alias' (Create), and the 'Sign-in URL for IAM' (https://471744311739.signin.aws.amazon.com/console).

Name the alias and create.

The dialog box is titled 'Create alias for AWS account 471744311739'. It contains fields for 'Preferred alias' (set to 'nextwork-alias-dhruval'), 'New sign-in URL' (set to 'https://nextwork-alias-dhruval.signin.aws.amazon.com/console'), and a note: 'IAM users will still be able to use the default URL containing the AWS account ID.' At the bottom are 'Cancel' and 'Create alias' buttons.

Create IAM Users and User Groups:

In this section the employee would be given a log in access and instructions by setting up an IAM group and IAM user.

- From the IAM Dashboard select user groups on the left navigation section and create groups.
- To set up the user group:
 - Name: network-dev-group
 - Attach permission policies: NextWorkDevEnvironmentPolicy
 - Then create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,.,@,_' characters.

Add users to the group - Optional (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search	Groups	Last activity	Creation time
<input type="text"/>	<input checked="" type="checkbox"/> User name <input type="checkbox"/>		
No resources to display			

Attach permissions policies - Optional (1045) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type		1 match	
<input type="text"/> NextWorkDevEnvironmentPolicy <input type="button" value="X"/>	All types		
<input type="checkbox"/> Policy name <input type="checkbox"/> NextWorkDevEnvironmentPolicy	Type	<input type="checkbox"/> Used as	Description
	Customer managed	None	IAM Policy for NextWorks developmen...

3. Next select users on the left navigation section and create user.
4. Name the user, for user type select “I want to create an IAM user” for sign in and access and then select next.

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keypairs, or a backup credential for emergency account access.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | '

Show password

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

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user.
[Learn more](#)

5. Set permissions to add user to the group and select the “network-dev-group” in user groups and select next.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)	
Group name	Users
<input checked="" type="checkbox"/> network-dev-group	0

Set permissions boundary - *optional*

Cancel Previous Next

Note: there will be a console sign in details after review and create.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
 <https://nextwork-alias-dhruval.signin.aws.amazon.com/console>

User name
 network-dev-dhruval

Console password
 [Show](#)

Email sign-in instructions [\[copy\]](#)

Cancel Download .csv file Return to users list

Test the employee's login access:

This is where to test the login with the credentials given.

1. Copy console sign-in URL, paste in a new incognito window and login with the given username and password.

IAM user sign in [\[i\]](#)

Account ID or alias ([Don't have?](#))
nextwork-alias-dhruval

Remember this account

IAM username
network-dev-dhruval

Password
.....

Show Password [Having trouble?](#)

Sign in

- Then use the password given to create a new password.

Password reset ⓘ

Your account (**471744311739**) password has expired or requires a reset.

To continue, please verify your old and set a new password for **network-dev-dhruval** (**not you?**).

Old Password
.....

Show Password

New Password
.....

Confirm New Password
.....

Show Password

Confirm Password Change

Note: User **network-dev-dhruval** will get logged in.

Console Home ⓘ

Recently visited ⓘ

No recently visited services

Explore one of these commonly visited AWS services.

EC2 **S3** **Aurora and RDS** **Lambda**

View all services

Applications (0) ⓘ

Region: US East (Ohio)

Create application

Select Region: us-east-2 (Current Region) Find applications

Name	Description	Region	Originati.
▶ Access denied to servicelogic>ListApplications			
Diagnose with Amazon Q			

Go to myApplications

Welcome to AWS

Getting started with AWS ⓘ

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification ⓘ

AWS Health ⓘ

Cost and usage ⓘ

Current month costs ⓘ Access denied

Forecasted month end costs ⓘ Access denied

Savings opportunities ⓘ Access denied

Cost breakdown ⓘ Access denied

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Successfully given the new employee access to the development environment with limited access!