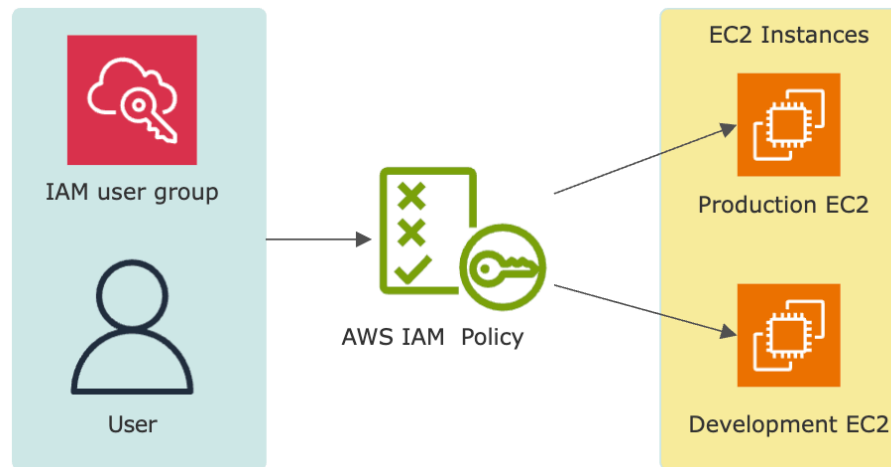


New Employee's Dev-Env Access with AWS IAM

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 closet 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

[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](#)

Q Name X

Q network-prod-dhruval X

Select resource types ▼

Remove

Instances X

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Q Env X

Q 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

Q Search our full catalog including 1000s of application and OS images

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

Free tier eligible ▼

ami-0ce45259f491c3d4f (64-bit (x86), uefi-preferred) / ami-0e26b1cd66cd6665c (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

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

Boot mode

AMI ID

Publish Date

Username [i](#)

Verified provider

64-bit (x86) ▼

uefi-preferred

ami-0ce45259f491c3d4f

2025-04-11

ec2-user

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).

▼
Key pair (login)
Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended)
Default value ▼
Create new key pair

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

Name and tags
Info

Name

network-dev-dhruval
Add additional tags

▼
Name and tags
Info

Key
Info

Value
Info

Resource types
Info

Name
X

network-dev-dhruval
X

Select resource types
▼

Remove

Instances
X

Key
Info

Value
Info

Resource types
Info

Env
X

network-dev-dhruval
X

Select resource types
▼

Remove

Instances
X

Add new tag

You can add up to 48 more tags.

You should have successfully created the 2 new EC2 instances

Instances (2/3) Info									
Find Instance by attribute or tag (case-sensitive)				All states ▼	Last updated less than a minute ago				
	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	t2.micro	-	View alarms +	us-west-1c	-	-
<input checked="" type="checkbox"/>	network-dev-...	i-0445c5fbae77d2ab9	Running	t2.micro	2/2 checks passec	View alarms +	us-west-1c	ec2-54-183-117-102.us...	54.183.11
<input checked="" type="checkbox"/>	network-prod-...	i-0f6625cc137d757ef	Running	t2.micro	2/2 checks passec	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-0445c5fb77d2ab9 (network-dev-dhruval)

Details	Status and alarms	Monitoring	Security	Networking	Storage	Tags
---------	-------------------	------------	----------	------------	---------	------

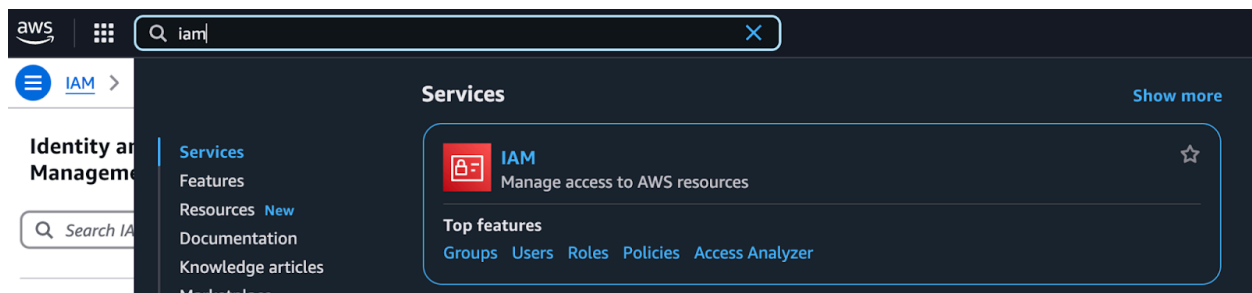
Tags

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.



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.

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



IAM Dashboard [Info](#)

Security recommendations 1

 **Add MFA for root user**
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

 **Root user has no active access keys**
Using access keys attached to an IAM user instead of the root user improves security.

[Add MFA](#)

AWS Account
Account ID
 471744311739
Account Alias
[Create](#)
Sign-in URL for IAM
 https://471744311739.signin.aws.amazon.com/console

Name the alias and create.

Create alias for AWS account 471744311739 ×


Preferred alias

network-alias-dhruval

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

https://network-alias-dhruval.signin.aws.amazon.com/console

 IAM users will still be able to use the default URL containing the AWS account ID.

[Cancel](#) [Create alias](#)

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.

1. From the IAM Dashboard select user groups on the left navigation section and create groups.
2. 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.

< 1 >

☐ User name
▲ Groups
Last activity ▼
Creation time ▼

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
All types ▼
1 match
< 1 >

<input type="checkbox"/>	Policy name	▲ Type	Used as ▼	Description
<input type="checkbox"/>	NextWorkDevEnvironmentPolicy	Customer managed	None	IAM Policy for NextWorks developmen...

Cancel
Create user group

- Next select users on the left navigation section and create user.
- 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 Keyspaces, 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.

Info If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.

[Learn more](#)

- 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

☐ Attached policies

☐ Created

<input checked="" type="checkbox"/>	network-dev-group	0	-	2025-04-18 (8 minutes ago)
-------------------------------------	-------------------	---	---	----------------------------

► 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 [Email sign-in instructions](#)

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

User name
network-dev-dhruval

Console password
***** [Show](#)

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.

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

IAM user sign in

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

☐ Remember this account

IAM username
network-dev-dhruval

Password

☐ Show Password [Having trouble?](#)

Sign in

2. 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

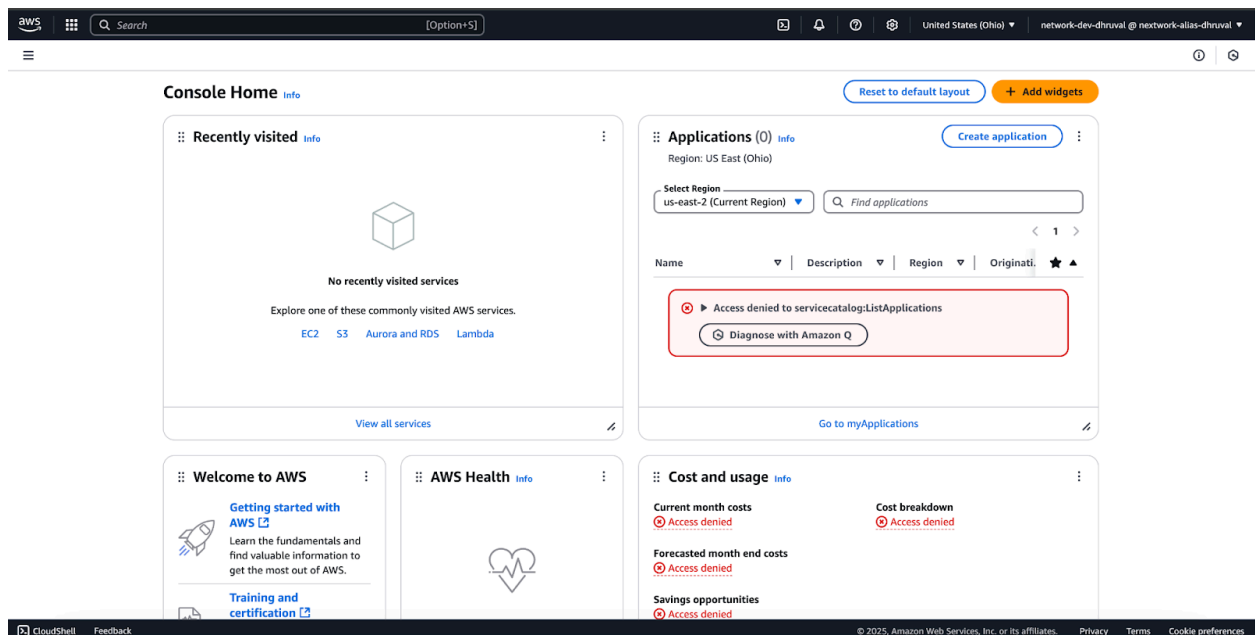
New Password

Confirm New Password

☐ Show Password

Confirm Password Change

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



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