# CLOUD SECURITY WITH AWS IAM

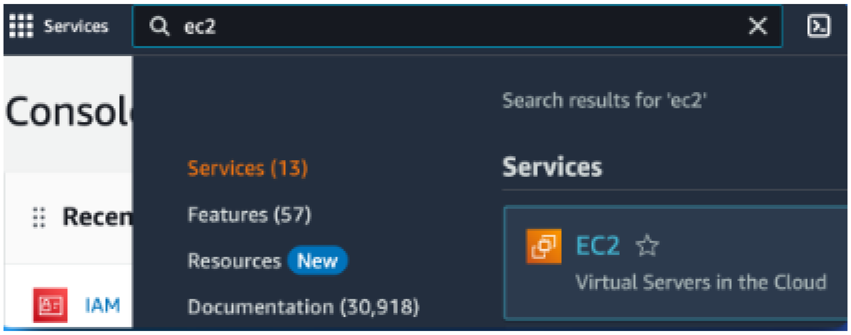
IAM means Identity and Access Management. AWS IAM is a service that enables you to securely control access to AWS services and resources. It helps you control who can do what in your AWS Account. It is useful as it enables efficient access management for users and services and also improves security practices. IAM makes use of Users, Groups, Roles, Policies and MFA. Strong IAM policies help protect sensitive data, prevent unauthorized access and reduce security risks. Key aspects of Cloud Security with IAM include

**USERS**: his is the individual accounts for people. Users are individuals or applications that need access to AWS. They have unique identities and can have specific permissions assigned to them.
**GROUPS**: This is a collection of users with the same permission
**ROLES**: This is used for AWS services or external users to access AWS without a password.
**POLICIES**: These are rules that define what users, groups can do
**MFA (Multi-Factor Authentication):** This adds security e.g password.

➢ **LAUNCH EC2 INSTANCE**

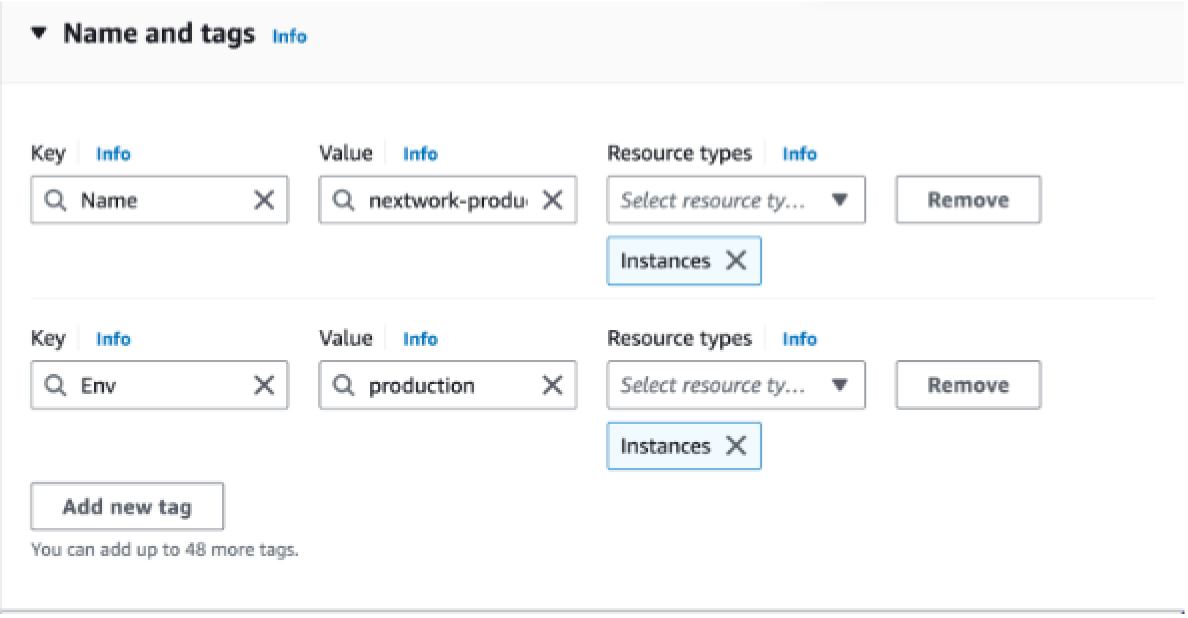
- Log in to your AWS Management Console.
- Head to **EC2**.

EC2 = **Elastic Compute Cloud.**
Amazon EC2 is a service that lets you rent and use virtual computers in the cloud. They're like your personal computers, but they exist on the internet instead of being physically in front of you. You can create, customize, and use these computers for all different reasons, from running applications to hosting websites.



- In your EC2 console, choose **Launch instances**.
- In **Name**, enter the value nextwork-production-ekom.
  Every EC2 instance must have a unique name in its AWS Region.
- Choose **Add additional tags**, which is right next to your **Name** field.
- Choose **Add new tag**.
- For the next tag, use this information:
  - Key: Env
  - Value: production

  Tags are like labels you can attach to AWS resources for organization. In this case, we're creating a tag called "Env" with a value of "production" or "development" to label the instances used in production vs development environments. This tagging helps us with identifying all resources with the same tag at once



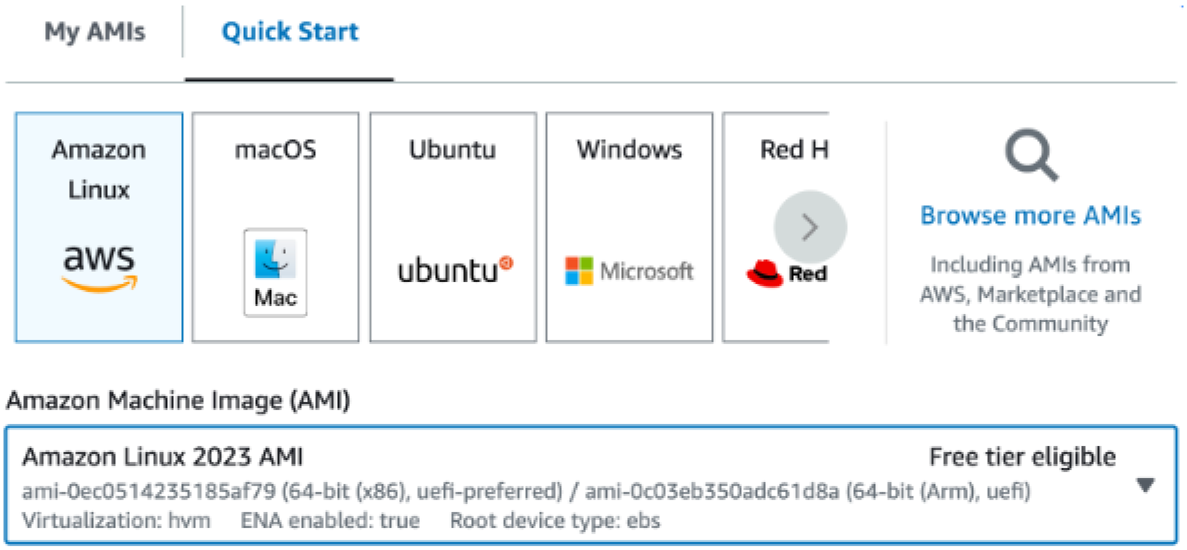
▼ Name and tags Info

| Key | Value | Resource types | |
|---|---|---|---|
| Name | nextwork-produ | Select resource ty...<br>Instances ✕ | Remove |
| Env | production | Select resource ty...<br>Instances ✕ | Remove |

Add new tag

You can add up to 48 more tags.

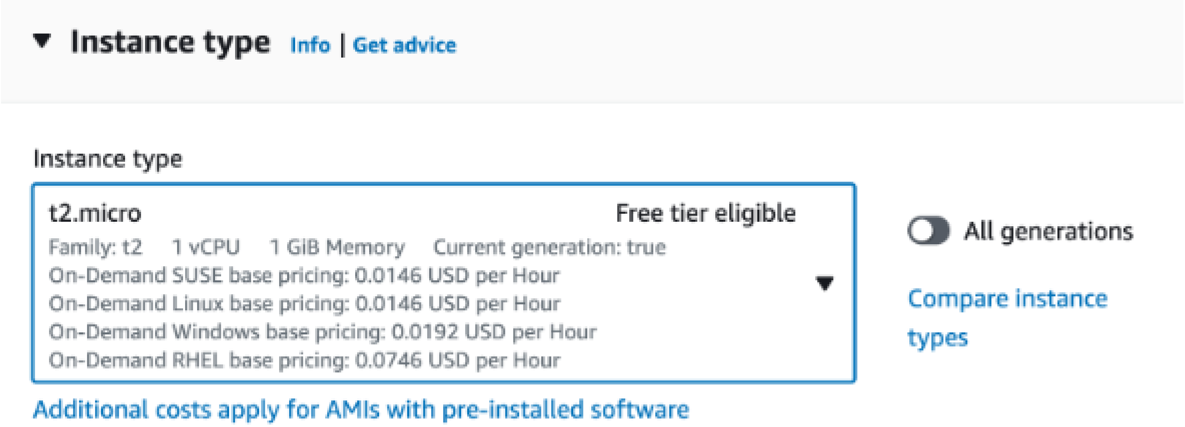
- Head on down to see your EC2 settings and make sure the **Amazon Machine Image (AMI)** is using a **Free tier eligible** option.
  AMI stands for Amazon Machine Image, and it's very similar to those pre-built computers. An AMI is a template or blueprint used to create EC2 instances and contains the operating system along with the applications needed to launch the instance.
  **Free tier eligible** AMIs are those that qualify for the AWS Free Tier, so you won't get charged for using it.



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-0ec0514235185af79 (64-bit (x86), uefi-preferred) / ami-0c03eb350adc61d8a (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

- For the instance type, also make sure you're using a **Free tier eligible** option!
  AMI decides what operating system your server runs, the instance type determines how fast and powerful it performs.

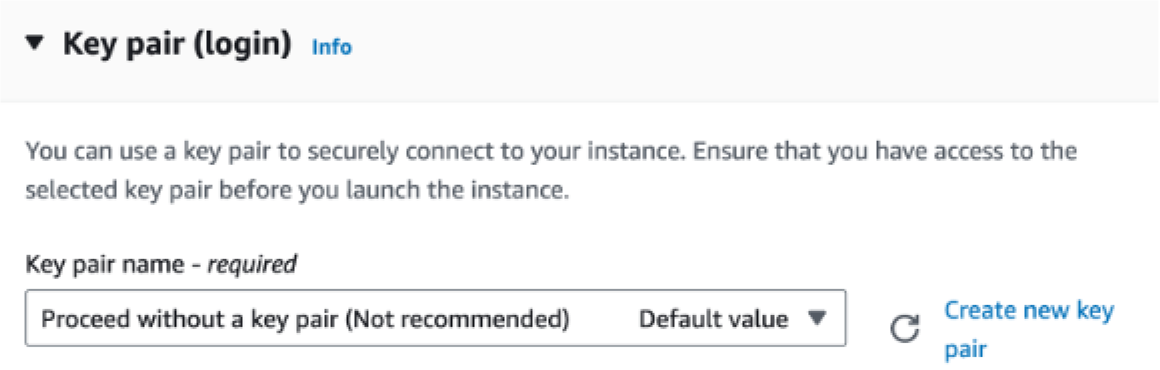

▼ Instance type Info | Get advice
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0146 USD per Hour
On-Demand Linux base pricing: 0.0146 USD per Hour
On-Demand Windows base pricing: 0.0192 USD per Hour
On-Demand RHEL base pricing: 0.0746 USD per Hour

- For **Key pair (login)**, select **Proceed without a key pair**.

A key pair is primarily used for accessing your EC2 instance securely **without going through the AWS Management Console**. Instead of the Management Console, you're using SSH (Secure Shell) Access with your key pairs. Proceeding without a key pair means you won't have SSH (Secure Shell) access to your instance, which is generally not recommended because it limits your ability to troubleshoot or manage your EC2 instance through a secure way outside of the Console.



▼ **Key pair (login)** Info

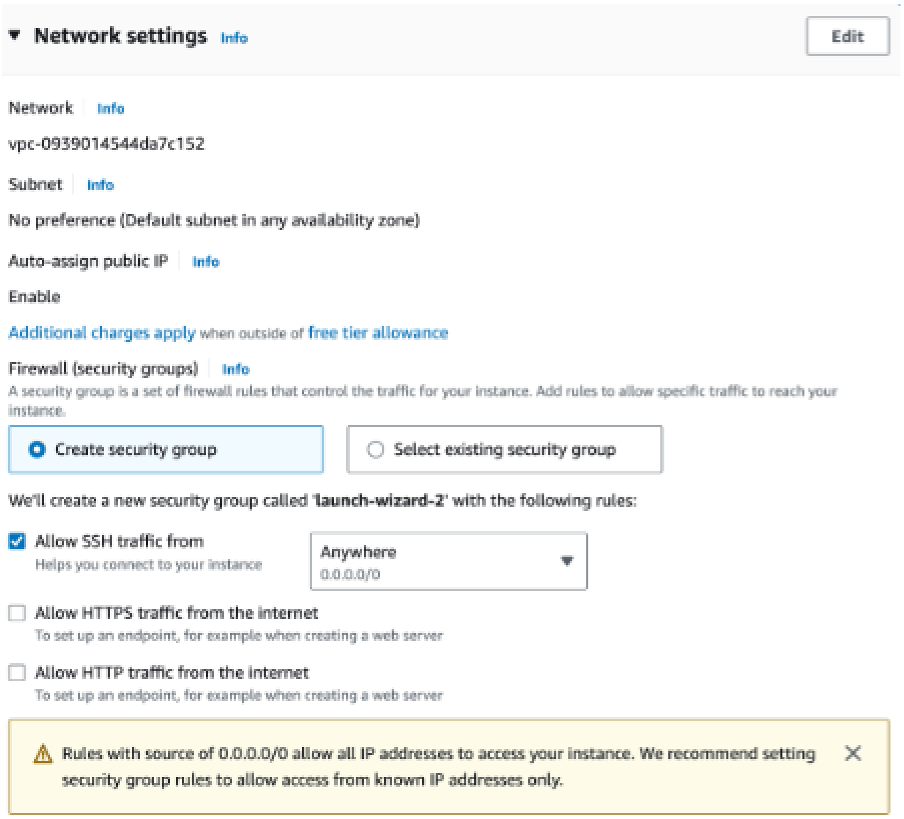
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

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

Create new key pair

- Configure your network settings



▼ **Network settings** Info

Edit

Network Info

vpc-0939014544da7c152

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-2**' with the following rules:

☑ Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0

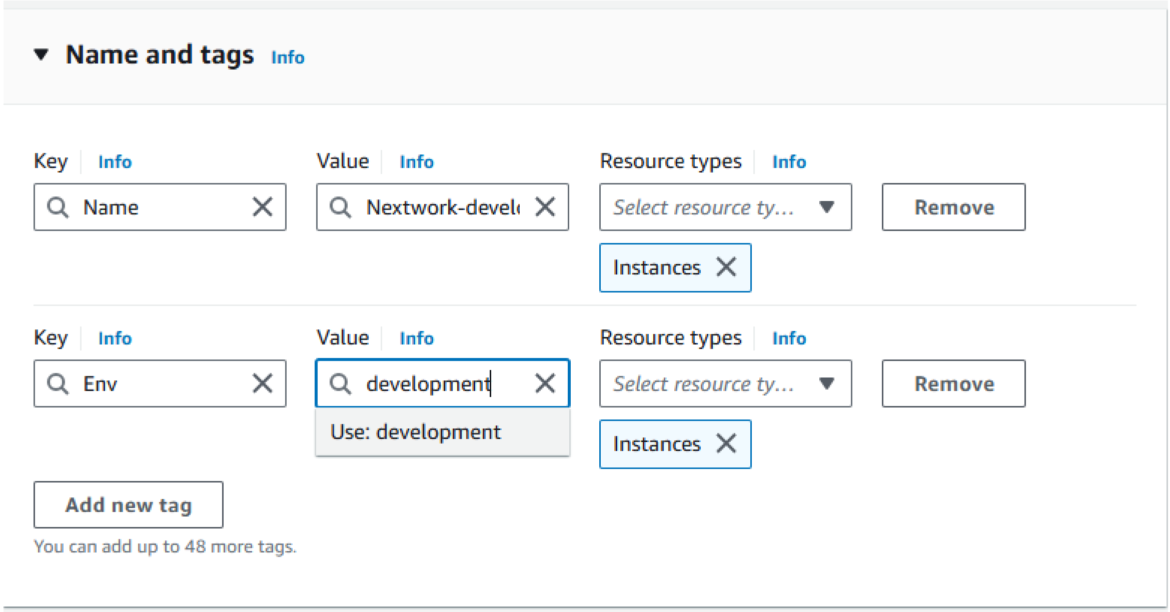
□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

- Click **Launch instance**.
- Now let's create one more EC2 instance for the **development environment**. Development and production environments refer to different stages in the software development lifecycle. The **development** environment is where developers write, test, and debug code before it's deployed to **production**, which is the live environment that your end users can use!

- Repeat the same flow, but this time using these tags:
- Name: nextwork-development-ekom
- Env: development



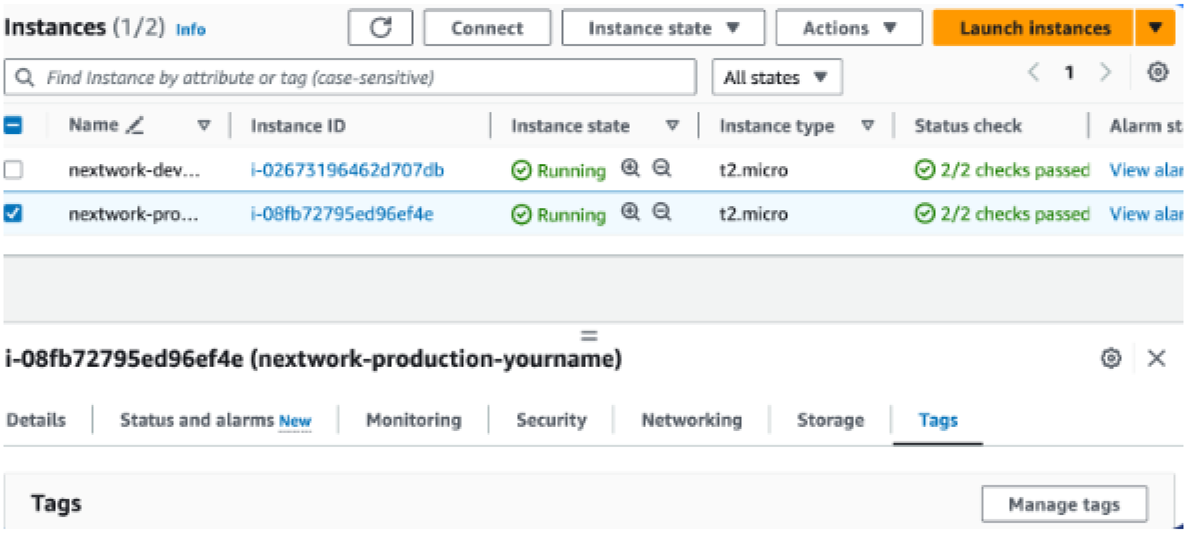
Name and tags

| Key | Value | Resource types |
|---|---|---|
| Name | Nextwork-devel‹ | Instances |
| Env | development | Instances |

Use: development

You can add up to 48 more tags.

- Select the checkbox next to one of your instances, and a popup window of information pops up!
- Select the **Tags** tab.



Instances (1/2)

Find Instance by attribute or tag (case-sensitive)

All states

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm st |
|---|---|---|---|---|---|---|
| □ | nextwork-dev... | i-02673196462d707db | ✓ Running | t2.micro | ✓ 2/2 checks passed | View alar |
| ☑ | nextwork-pro... | i-08fb72795ed96ef4e | ✓ Running | t2.micro | ✓ 2/2 checks passed | View alar |

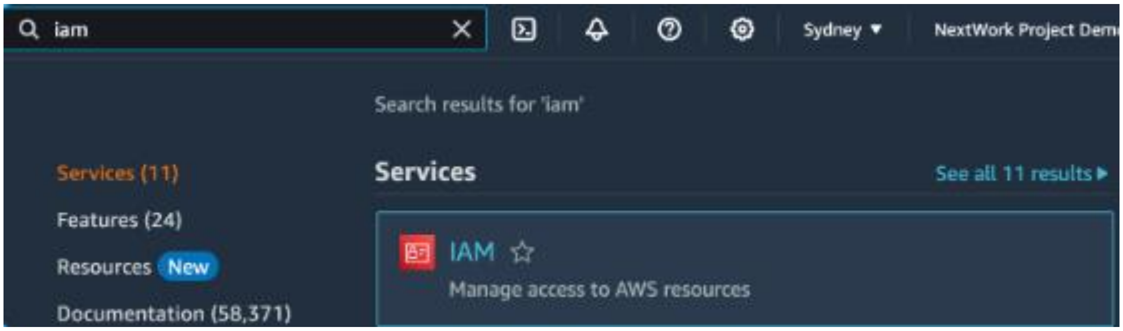
i-08fb72795ed96ef4e (nextwork-production-yourname)

Tags

## ➢ CREATE AN IAM POLICY

You've deployed two EC2 instances, one for your production environment and one for your development environment. It's time to onboard the team's new intern and **set up permission policies.**

- Head to your **IAM** console.

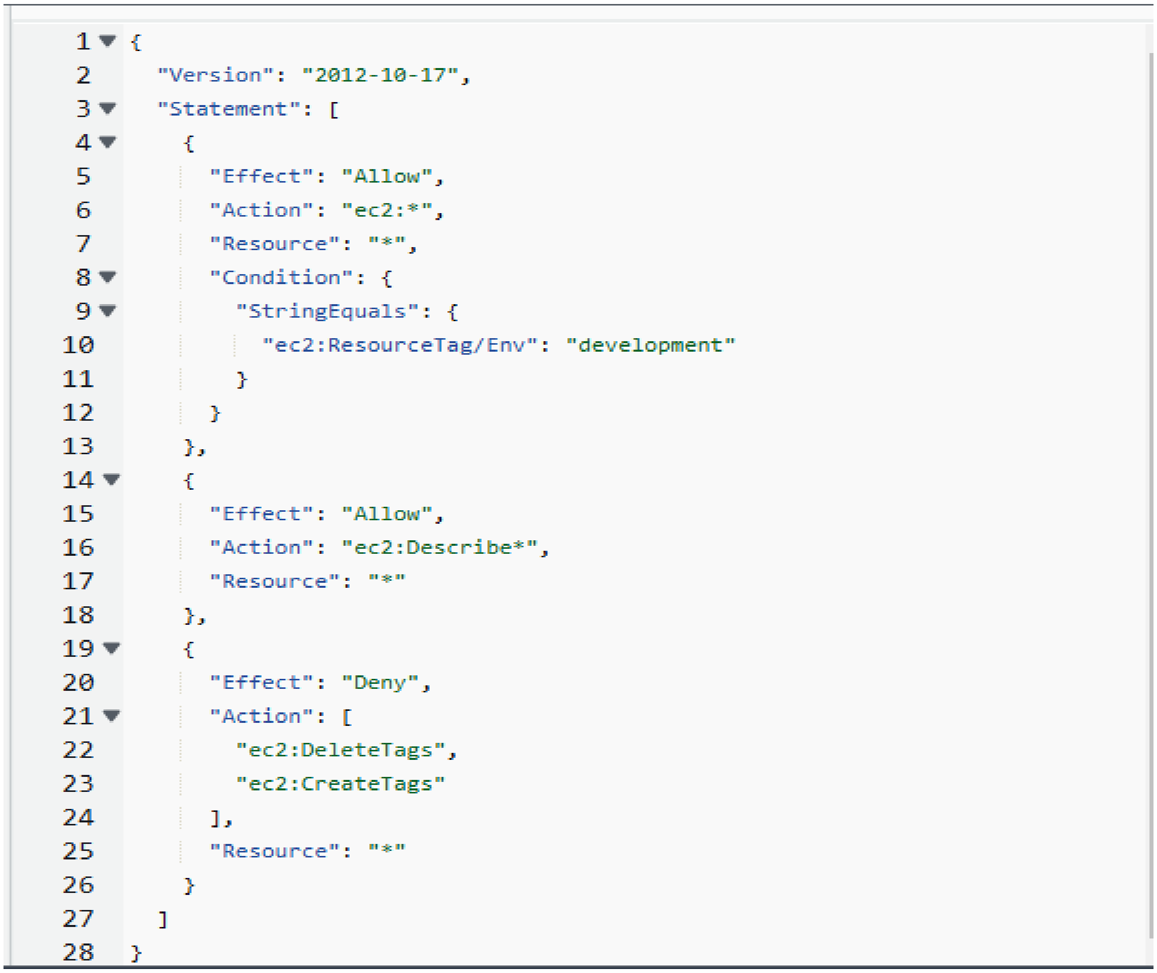


IAM stands for Identity and Access Management. You'll use AWS IAM to manage the access level that other users and services have to your resources.

- Now on the left-hand navigation panel of your IAM console, choose **Policies**.
  An IAM policy is a rule for who can do what with your AWS resources. It's all about giving permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources, and when those rules kick in.
- Choose **Create policy**.
- Switch your Policy editor tab to JSON.
- Paste this policy into your editor - replace ALL of the existing code in your editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
     "Effect": "Allow",
     "Action": "ec2:*",
     "Resource": "*",
     "Condition": {
       "StringEquals": {
         "ec2:ResourceTag/Env": "development"
       }
     }
   },
   {
     "Effect": "Allow",
     "Action": "ec2:Describe*",
     "Resource": "*"
   },
     "Effect": "Deny",
     "Action": [
       "ec2:DeleteTags",
       "ec2:CreateTags"
     ],
     "Resource": "*"
   }
 ]
}
```

This policy allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances.

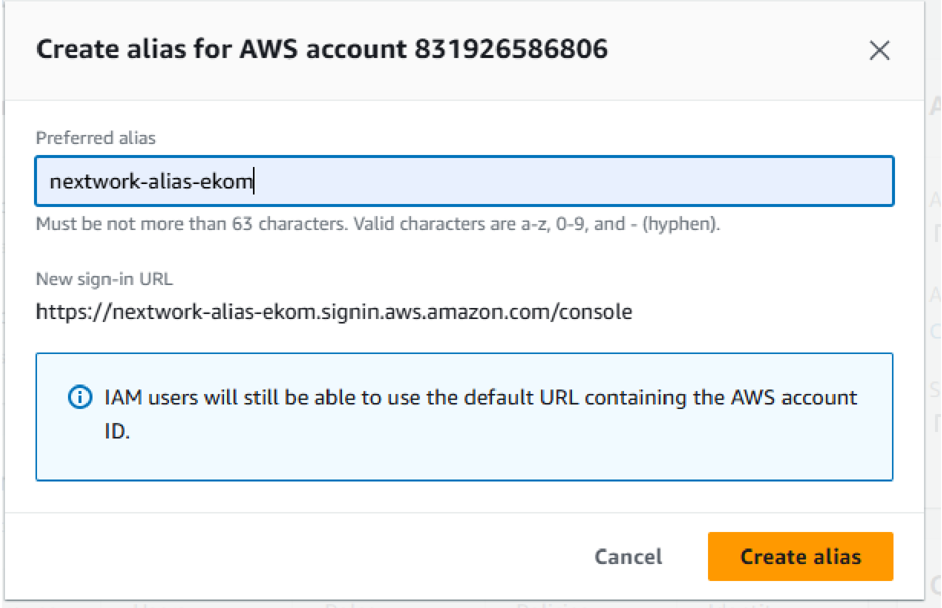


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    }
  ]
}
```

- Select **Next** when you're ready.
- Fill in your policy's details:
  - Name: NextWorkDevEnvironmentPolicy
  - Description: IAM Policy for NextWork's development environment
- Choose **Create policy**.

## CREATE AN AWS ACCOUNT ALIAS

- Head to your IAM dashboard.
- In the right-hand side of the dashboard, choose **Create** under **Account Alias**.
  An Account Alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.
  Your AWS account's sign-in page has this URL by default:
  https://**Your_Account_ID**.signin.aws.amazon.com/console/
  If you create an AWS account alias for your AWS account ID, your sign-in page URL looks more like:
  https://**Your_Account_Alias**.signin.aws.amazon.com/console/
- In the **Preferred alias** field, enter **nextwork-alias-ekom**



Create alias for AWS account 831926586806

Preferred alias

nextwork-alias-ekom

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

New sign-in URL

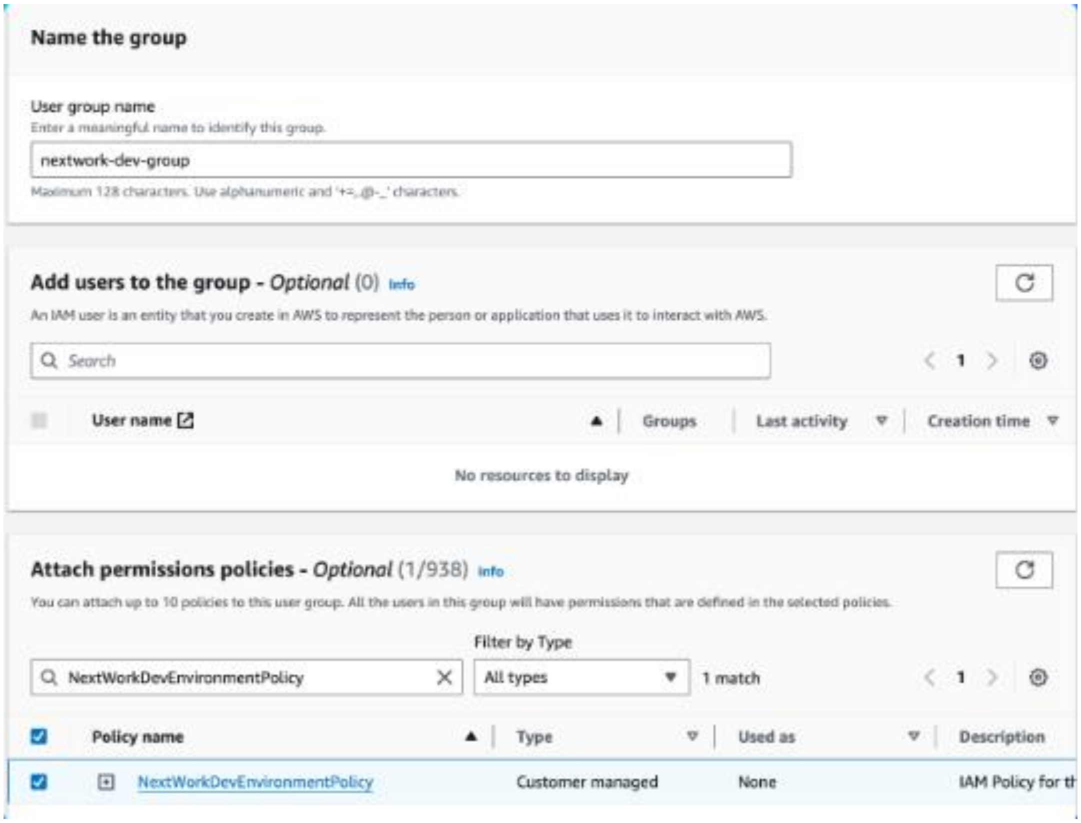
https://nextwork-alias-ekom.signin.aws.amazon.com/console

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

- Choose **Create alias**.

## ➢ CREATE IAM USERS AND USER GROUP

- Choose **User groups** in your left-hand navigation panel.
- Choose **Create group**.
- Let's create your first user group
  An IAM user group is a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.
- To set up your user group:
  - Name: nextwork-dev-group
  - Attach permission policies: NextWorkDevEnvironmentPolicy



Name the group

User group name
Enter a meaningful name to identify this group.
nextwork-dev-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.

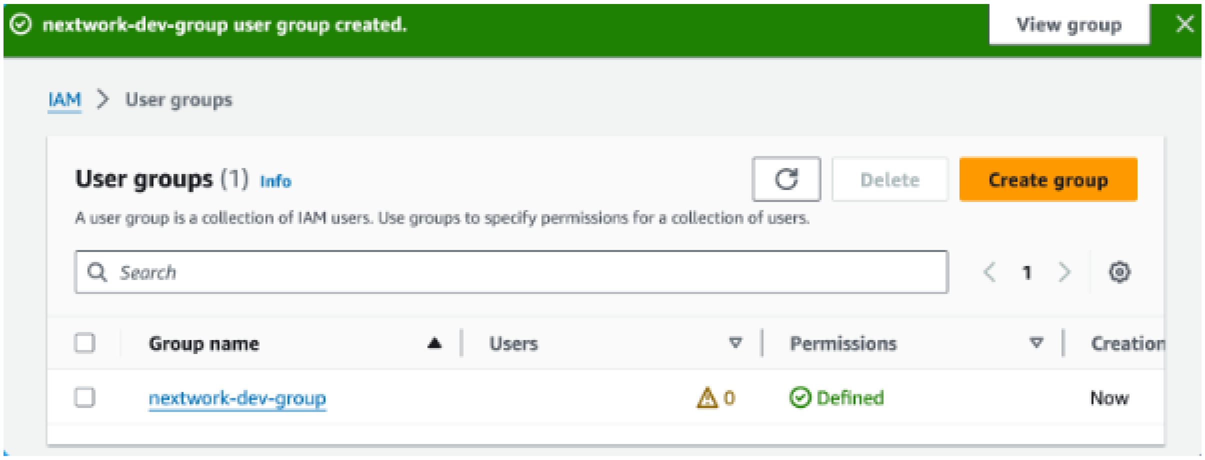
| □ | User name | Groups | Last activity | Creation time |
|---|---|---|---|---|
| No resources to display | | | | |

Attach permissions policies - *Optional* (1/938) 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
NextWorkDevEnvironmentPolicy | All types | 1 match

| ☑ | Policy name | Type | Used as | Description |
|---|---|---|---|---|
| ☑ | NextWorkDevEnvironmentPolicy | Customer managed | None | IAM Policy for th |

- Select **Create user group**.



nextwork-dev-group user group created.

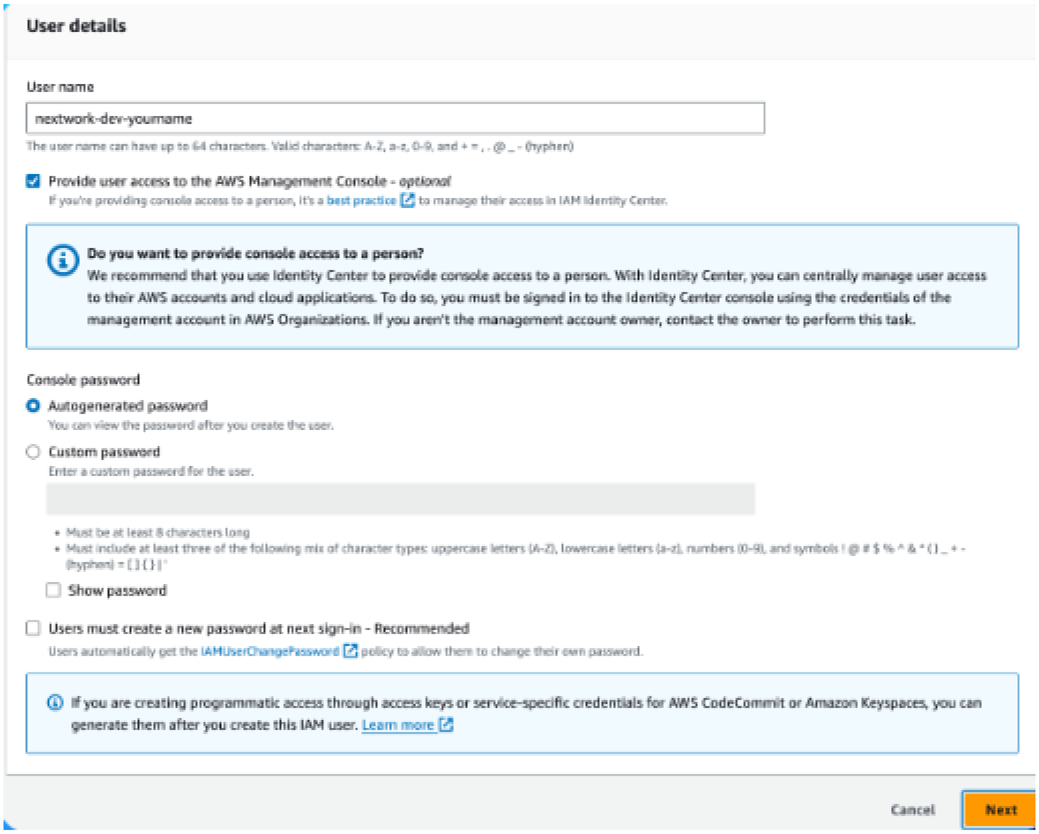
User groups (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

| Group name | Users | Permissions | Creation |
|---|---|---|---|
| nextwork-dev-group | ⚠ 0 | ✓ Defined | Now |

Now let's add Users to your user group.
IAM users are the people that will get access to your resources/AWS account, whereas user groups are the collections/folders of users for easier user management.
We're adding users to **nextwork-dev-group** to grant them the permissions associated with that group.

- Choose **Users** from the left-hand navigation panel.
- Choose **Create user**.
- Let's set up this user! Under **User name**, enter nextwork-dev-ekom
- Tick the checkbox for **Provide user access to the AWS Management Console**.
  If you don't tick this box, your new user won't get to sign in and access AWS services through the Console. They'll have to access AWS services through other, more advanced methods
- Uncheck the box for **Users must create a new password at next sign-in - Recommended**.



User details

User name

nextwork-dev-yourname

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.

**Do you want to provide console access to a person?**
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. To do so, you must be signed in to the Identity Center console using the credentials of the management account in AWS Organizations. If you aren't the management account owner, contact the owner to perform this task.

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) = [ ] { } | '

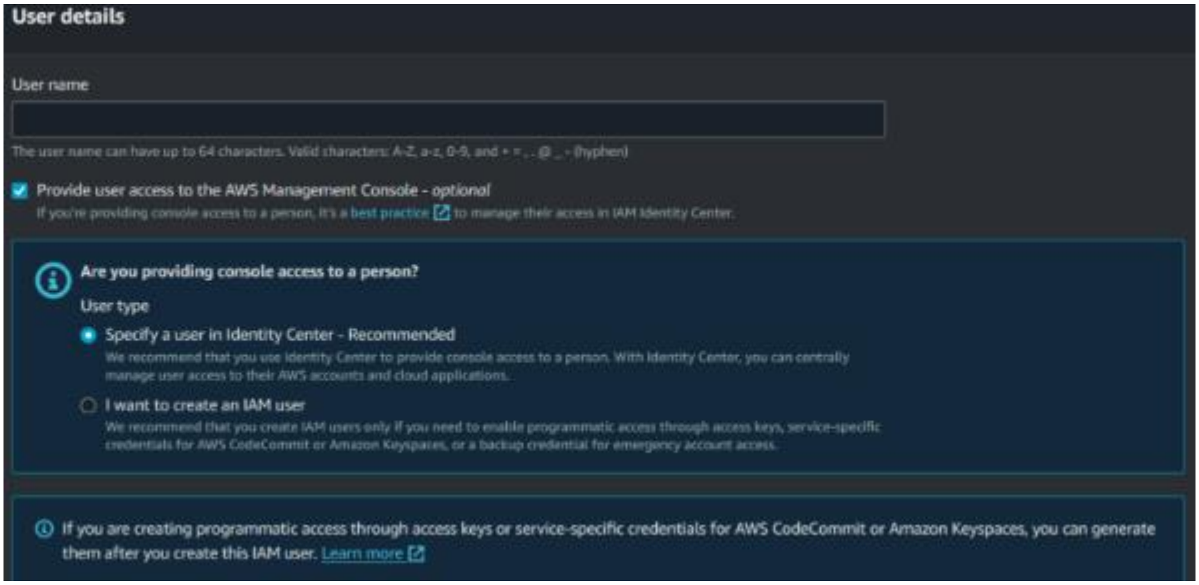
□ Show password

□ 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 Keyspaces, you can generate them after you create this IAM user. Learn more

**Note**: This does not show up for every AWS Account, but if you see a highlighted pop-up that asks "**Are you providing console access to a person?**" - select **I want to create an IAM user**.



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

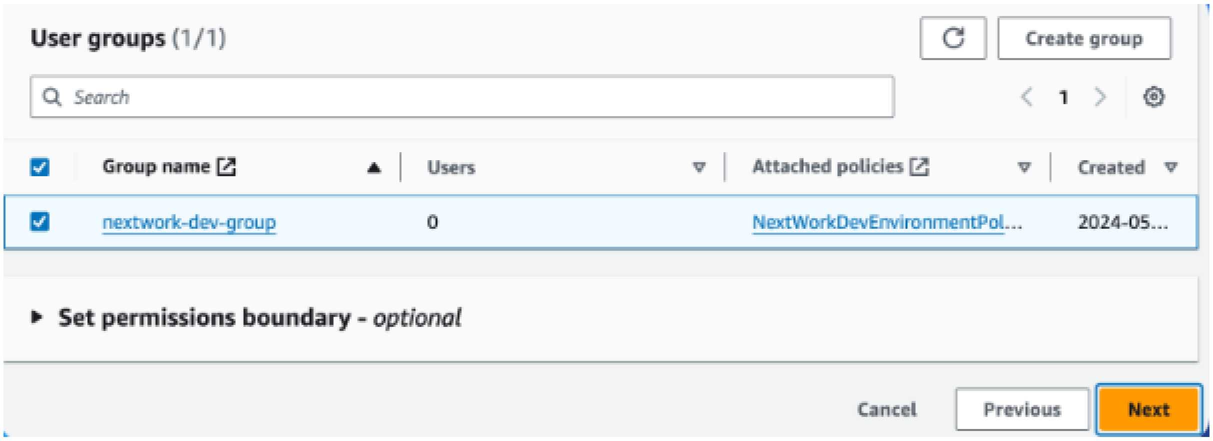
● Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

○ 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.

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

- Select **Next** when you're ready!

- To set permissions for your user, we'll simply add it to the user group you've created. Select the checkbox next to **nextwork-dev-group**.
- Select **Next**.
- Select **Create user**!

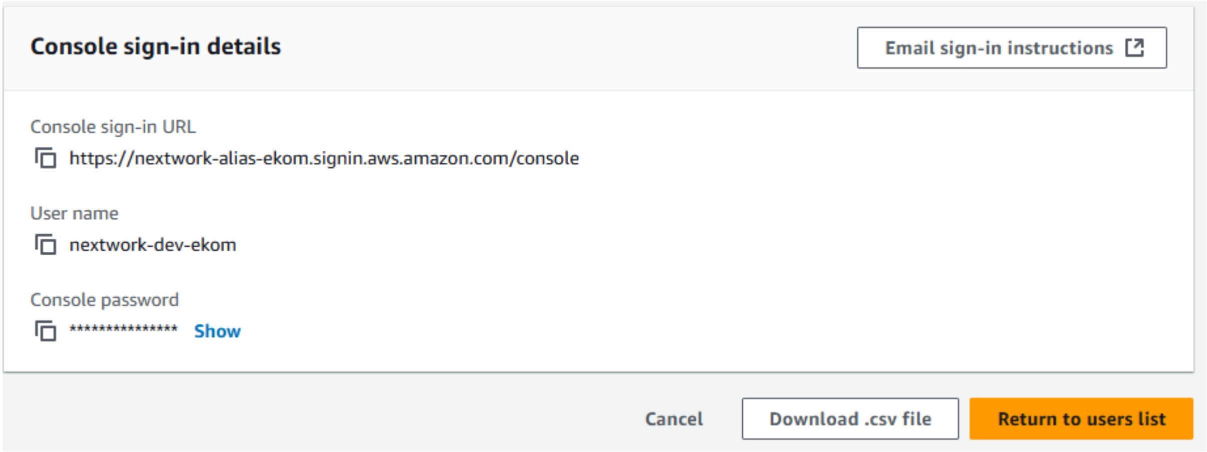


**User groups** (1/1)

| ☑ | Group name | Users | Attached policies | Created |
|---|---|---|---|---|
| ☑ | nextwork-dev-group | 0 | NextWorkDevEnvironmentPol... | 2024-05... |

▸ **Set permissions boundary** - *optional*

- It's a success - now you're seeing some specific sign-in details for your new user.



**Console sign-in details**

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

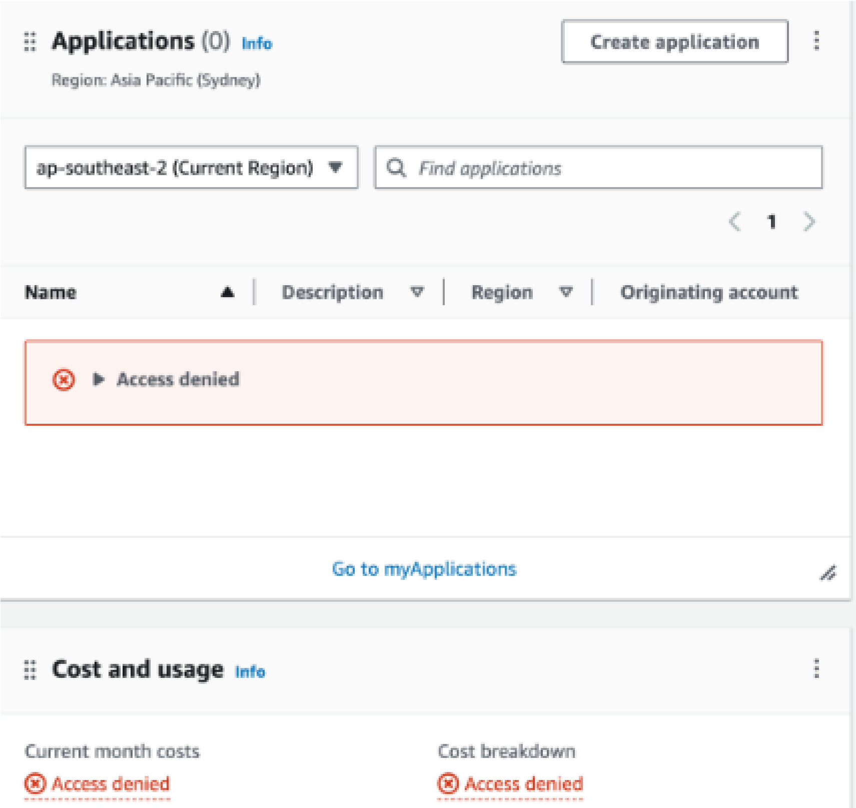
User name
nextwork-dev-ekom

Console password
*************** Show

➢ **TEST YOUR ACCESS**

- Log into AWS using the intern's IAM user.
- Test the intern's access to your production and development instance.
- Copy the **Console sign-in URL**. Do not close this tab!
- Open a new **incognito window** on your browser.
- Open the new console sign-in URL in your incognito window.
- Using the **User name** and **Console password** given in your IAM tab, let's log in!

- As a new user, you'll notice that some of your dashboard panels are showing **Access denied** already.



Region: Asia Pacific (Sydney)

ap-southeast-2 (Current Region)

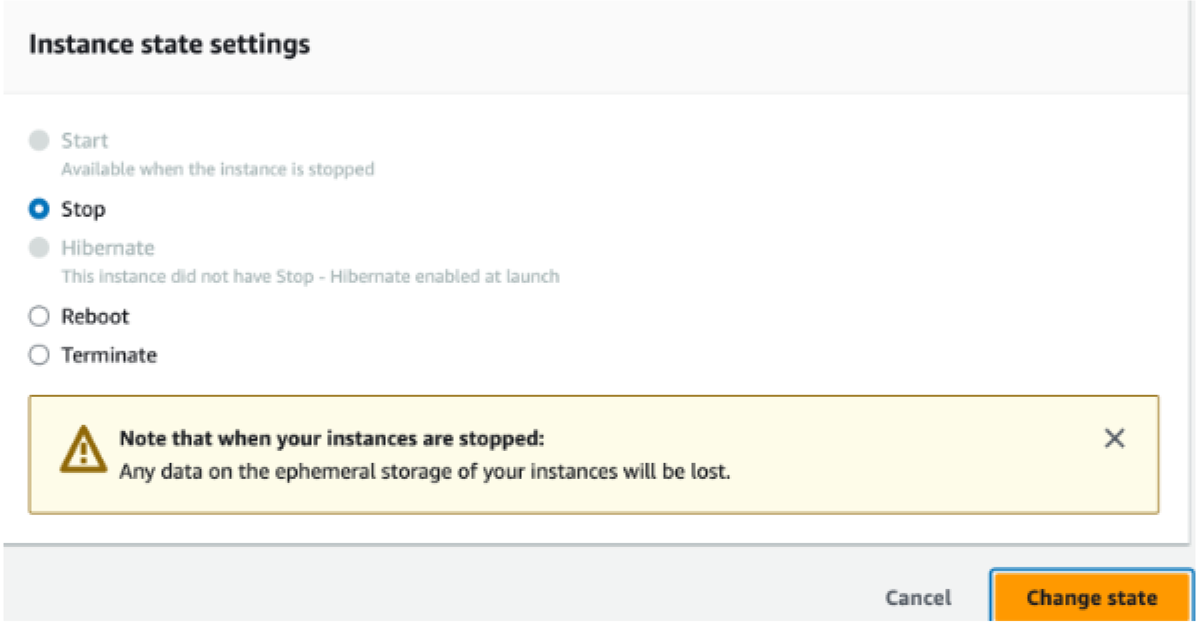
| Name | Description | Region | Originating account |
|---|---|---|---|

Access denied

Current month costs
Access denied

Cost breakdown
Access denied

- Head to your **EC2** console, and make sure you're in the same **Region** as the one where you deployed your two production and development instances.
- Head to **Instances**.
- Select your **production** instance, and in the **Actions** dropdown, select **Manage instance state**.
- Select the **Stop option**, then **Change state**.



**Instance state settings**

○ Start
Available when the instance is stopped

● Stop

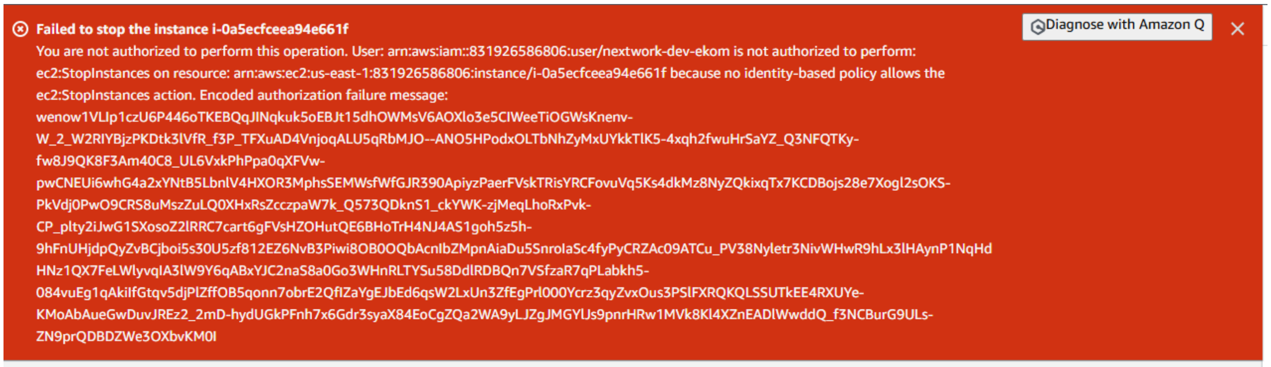
○ Hibernate
This instance did not have Stop - Hibernate enabled at launch

○ Reboot

○ Terminate

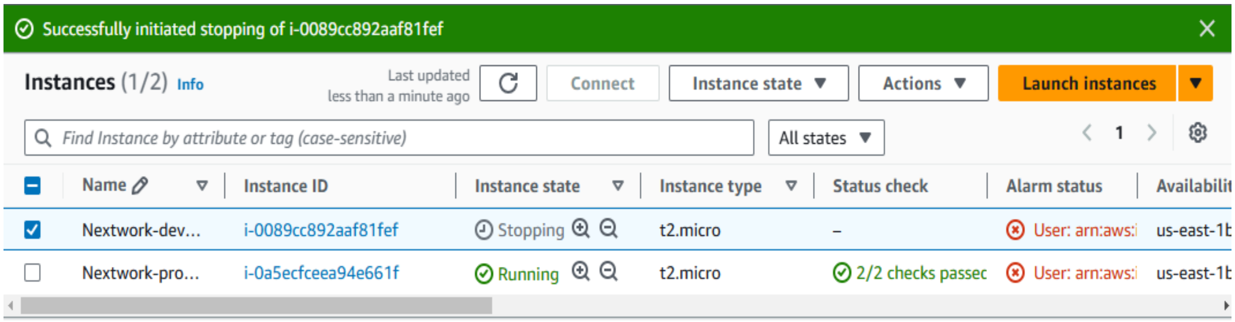
⚠ **Note that when your instances are stopped:**
Any data on the ephemeral storage of your instances will be lost.

Select **Stop**.
At the top of your page, an angry-looking banner tells us we've failed to stop this instance. The banner tells us it's because we're not authorized! We don't have permission to stop any instance with the production tag.



```
Failed to stop the instance i-0a5ecfceea94e661f
You are not authorized to perform this operation. User: arn:aws:iam::831926586806:user/nextwork-dev-ekom is not authorized to perform:
ec2:StopInstances on resource: arn:aws:ec2:us-east-1:831926586806:instance/i-0a5ecfceea94e661f because no identity-based policy allows the
ec2:StopInstances action. Encoded authorization failure message:
wenow1VLIp1czU6P446oTKEBQqJINqkuk5oEBJt15dhOWMsV6AOXlo3e5CIWeeTiOGWsKnenv-
W_2_W2RIYBjzPKDtk3lVfR_f3P_TFXuAD4VnjoqALU5qRbMJO--ANO5HPodxOLTbNhZyMxUYkkTlK5-4xqh2fwuHrSaYZ_Q3NFQTKy-
fw8J9QK8F3Am40C8_UL6VxkPhPpa0qXFVw-
pwCNEUi6whG4a2xYNtB5LbnlV4HXOR3MphsSEMWsfWfGJR390ApiyzPaerFVskTRisYRCFovuVq5Ks4dkMz8NyZQkixqTx7KCDBojs28e7Xogl2sOKS-
PkVdj0PwO9CRS8uMszZuLQ0XHxRsZcczpaW7k_Q573QDknS1_ckYWK-zjMeqLhoRxPvk-
CP_plty2iJwG1SXosoZ2lRRC7cart6gFVsHZOHutQE6BHoTrH4NJ4AS1goh5z5h-
9hFnUHjdpQyZvBCjboi5s30U5zf812EZ6NvB3Piwi8OB0OQbAcnIbZMpnAiaDu5SnrolaSc4fyPyCRZAc09ATCu_PV38Nyletr3NivWHwR9hLx3lHAynP1NqHd
HNz1QX7FeLWlyvqIA3lW9Y6qABxYJC2naS8a0Go3WHnRLTYSu58DdlRDBQn7VSfzaR7qPLabkh5-
084vuEg1qAkiIfGtqv5djPlZffOB5qonn7obrE2QflZaYgEJbEd6qsW2LxUn3ZfEgPrl000Ycrz3qyZvxOus3PSlFXRQKQLSSUTkEE4RXUYe-
KMoAbAueGwDuvJREz2_2mD-hydUGkPFnh7x6Gdr3syaX84EoCgZQa2WA9yLJZgJMGYlJs9pnrHRw1MVk8Kl4XZnEADlWwddQ_f3NCBurG9ULs-
ZN9prQDBDZWe3OXbvKM0I
```

- Now let's try to stop the development instance.
- Head back to the **Instances** page, and select the checkbox next to **nextwork-development-ekom**.
- Under the **Actions drop-down**, select **Manage instance state**.
- Select **Stop**, then **Change state**. Select **Stop**.
- Success!



Successfully initiated stopping of i-0089cc892aaf81fef

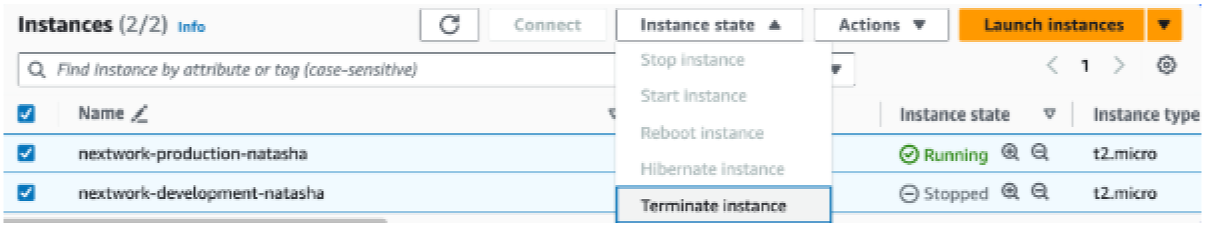
Instances (1/2) Info

Last updated less than a minute ago

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availabilit |
|---|---|---|---|---|---|---|---|
| ☑ | Nextwork-dev... | i-0089cc892aaf81fef | Stopping | t2.micro | – | User: arn:aws:i | us-east-1b |
| ☐ | Nextwork-pro... | i-0a5ecfceea94e661f | Running | t2.micro | 2/2 checks passec | User: arn:aws:i | us-east-1b |

➢ **DELETE YOUR RESOURCES**

- In your **EC2 console**, terminate your development and production instances.
- Select the x next to the **Instance state = running** box to reveal your development instance too

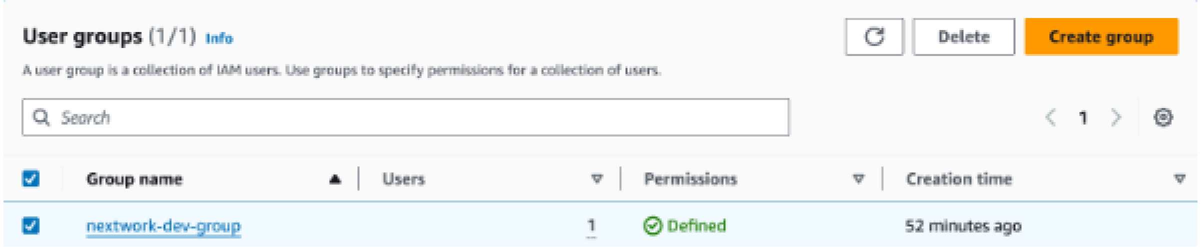


Instances (2/2) Info

| | Name | Instance state | Instance type |
|---|---|---|---|
| ☑ | nextwork-production-natasha | Running | t2.micro |
| ☑ | nextwork-development-natasha | Stopped | t2.micro |

In your **IAM console**, delete your:

- User group i.e. nextwork-dev-group

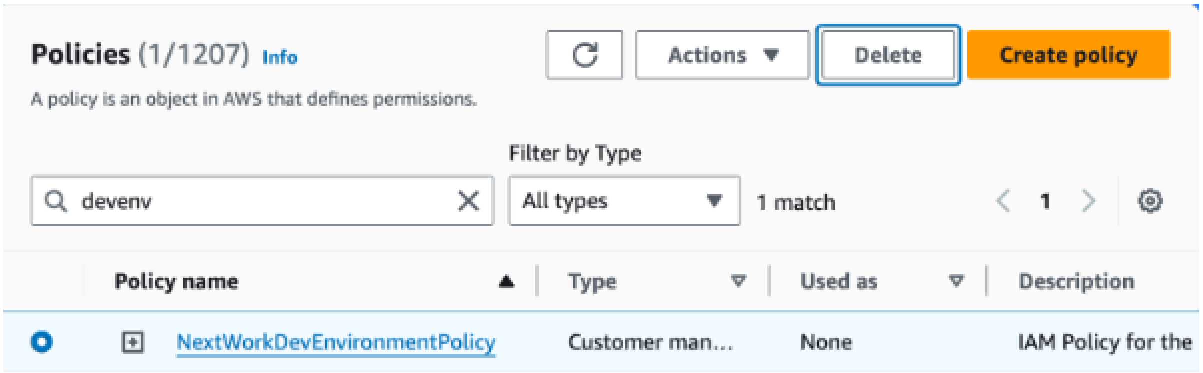


User groups (1/1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

| | Group name | Users | Permissions | Creation time |
|---|---|---|---|---|
| ☑ | nextwork-dev-group | 1 | Defined | 52 minutes ago |

- User i.e. nextwork-dev-ekom
- Policy i.e. NextWorkDevEnvironmentPolicy



Policies (1/1207) Info

A policy is an object in AWS that defines permissions.

Filter by Type

devenv

All types

1 match

| | Policy name | Type | Used as | Description |
|---|---|---|---|---|
| ● | NextWorkDevEnvironmentPolicy | Customer man... | None | IAM Policy for the |