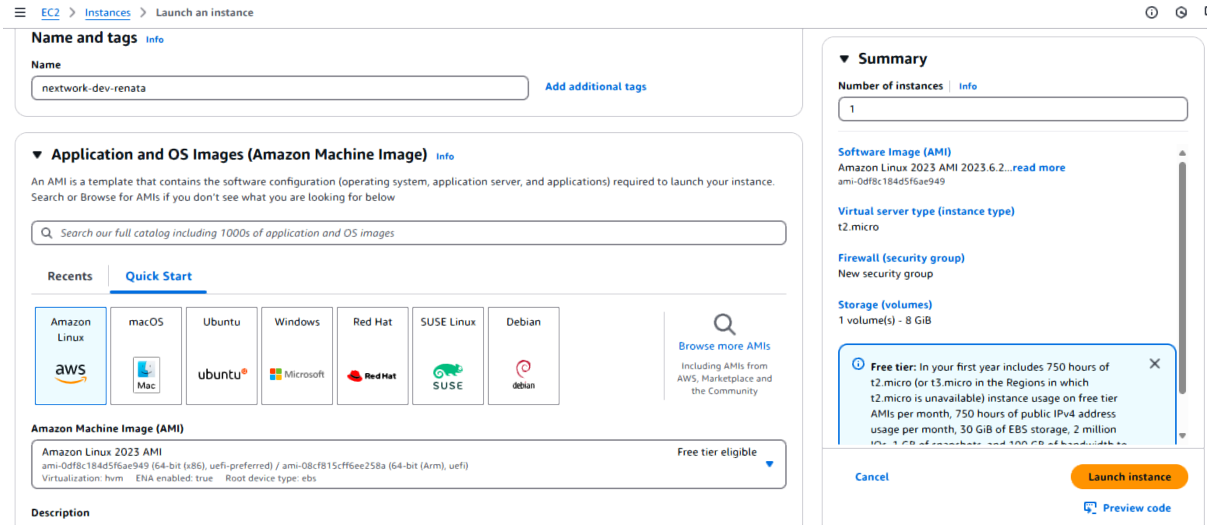
Using AWS Identity and Access Management (IAM) to control who is authenticated (signed in) and authorized (has permissions) to use your account's resources.

- Launch two Amazon EC2 instances.
- In your EC2 console, choose **Launch instances**.
- In **Name**, enter the value nextwork-production-yourname.
- 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
- Head on down to see your EC2 settings and make sure the **Amazon Machine Image (AMI)** is using a **Free tier eligible** option.
- For the instance type, also make sure you're using a **Free tier eligible** option
- For **Key pair (login)**, select **Proceed without a key pair**.
- Click **Launch instance**.



Name: nextwork-dev-renata

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

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

Amazon Machine Image (AMI)
Amazon Linux 2023 AMI — Free tier eligible
ami-0df8c184d5f6ae949 (64-bit (x86), uefi-preferred) / ami-08cf815cff6ee258a (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0df8c184d5f6ae949

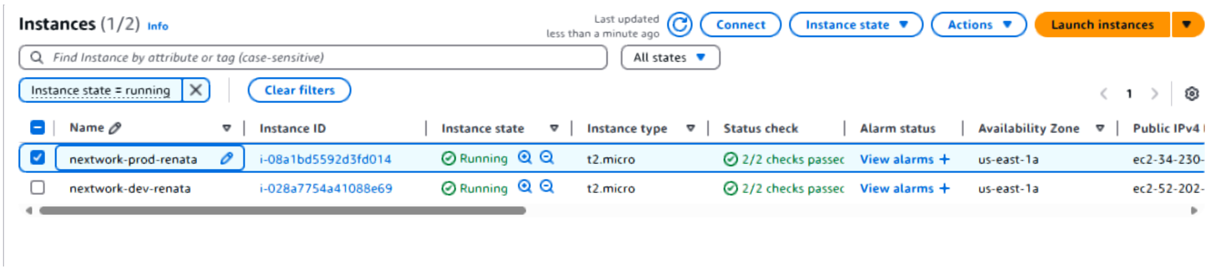
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million

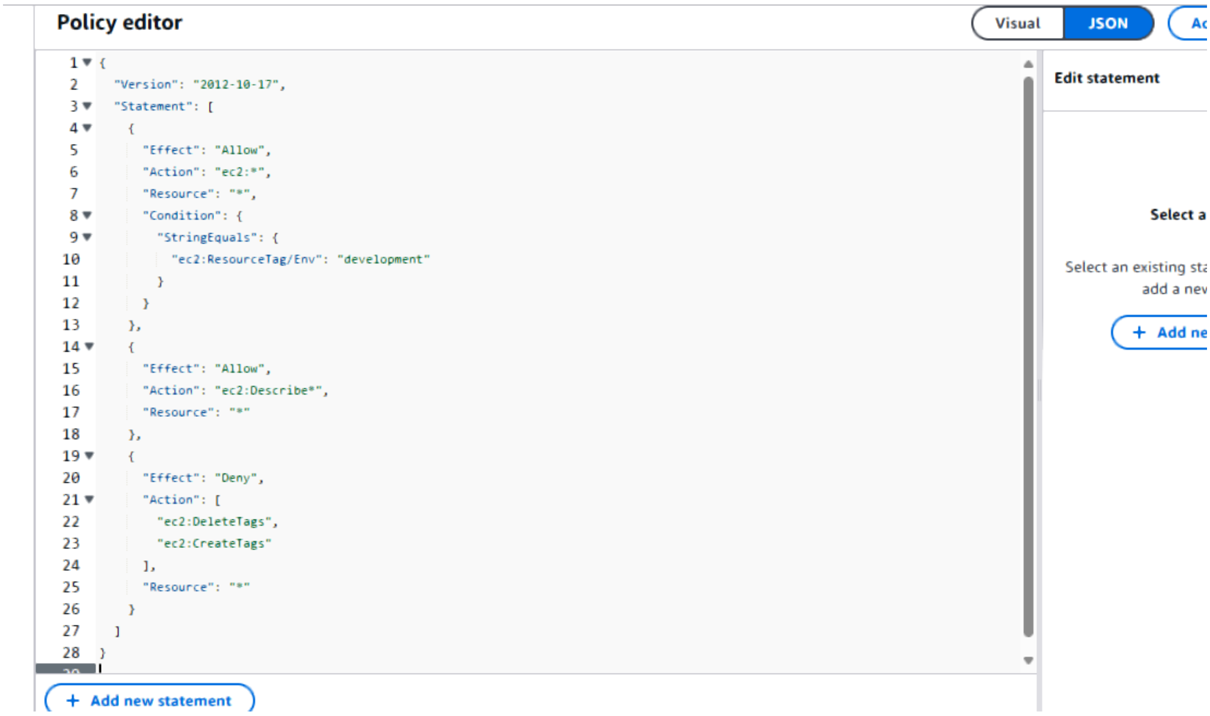
- Now let's create one more EC2 instance for the **development environment**.
- Repeat the same flow, but this time using these tags:
- Name: nextwork-development-yourname
- Env: development
- Launch your second instance.


Instances (1/2) Info
Last updated less than a minute ago
Connect
Instance state ▼
Actions ▼
Launch instances ▼
Find Instance by attribute or tag (case-sensitive)
All states ▼
Instance state = running ✕
Clear filters
1

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
☑	nextwork-prod-renata	i-08a1bd5592d3fd014	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	us-east-1a	ec2-34-230-
□	nextwork-dev-renata	i-028a7754a41088e69	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	us-east-1a	ec2-52-202-

Create an IAM Policy

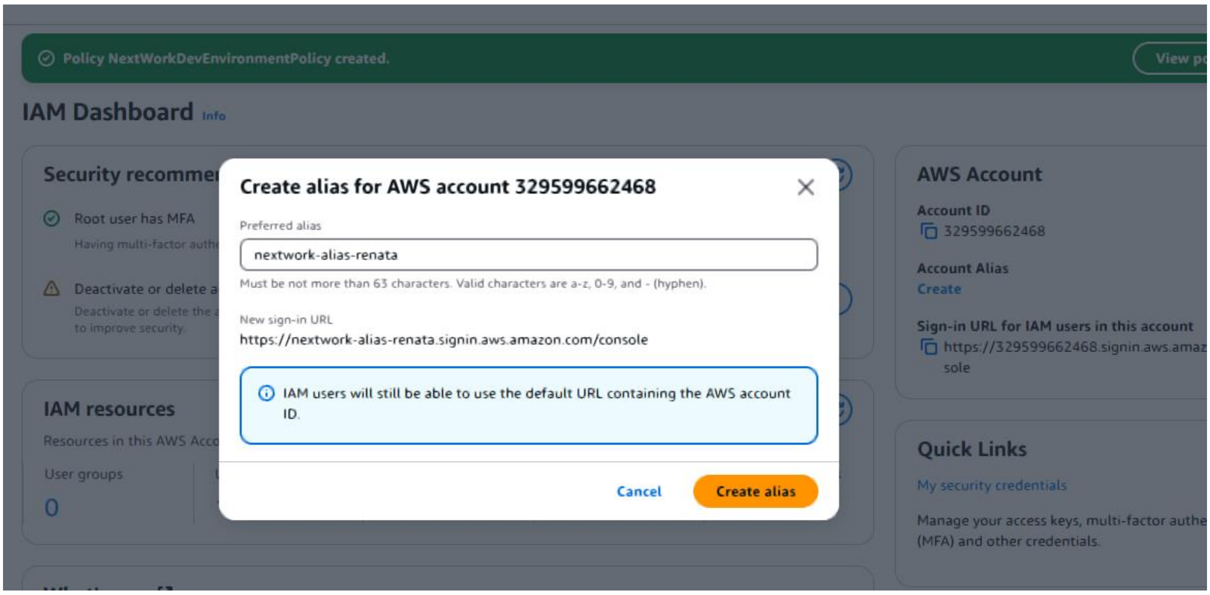
- Head to your **IAM** console.
- Now on the left-hand navigation panel of your IAM console, choose **Policies**.
- Choose **Create policy**.
- Switch your Policy editor tab to JSON. Copy code from separate file.



```
{
  "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**.
- Oh no! Turns out there's a rule for the characters allowed in your Policy description. Edit this description to get rid of that error (can you tell which character is not valid? There's a hint given to you right underneath the **Description's** text box).
- Choose **Create policy** again when you're done.
- Create an AWS Account Alias
- Head to your IAM dashboard.
- In the right-hand side of the dashboard, choose **Create** under **Account Alias**.

- In the **Preferred alias** field, enter **nextwork-alias-yourname**. Yup, replace **yourname** with your name!
- Choose **Create alias**.



Policy NextWorkDevEnvironmentPolicy created.

IAM Dashboard Info

Create alias for AWS account 329599662468

Preferred alias: nextwork-alias-renata

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

New sign-in URL
https://nextwork-alias-renata.signin.aws.amazon.com/console

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

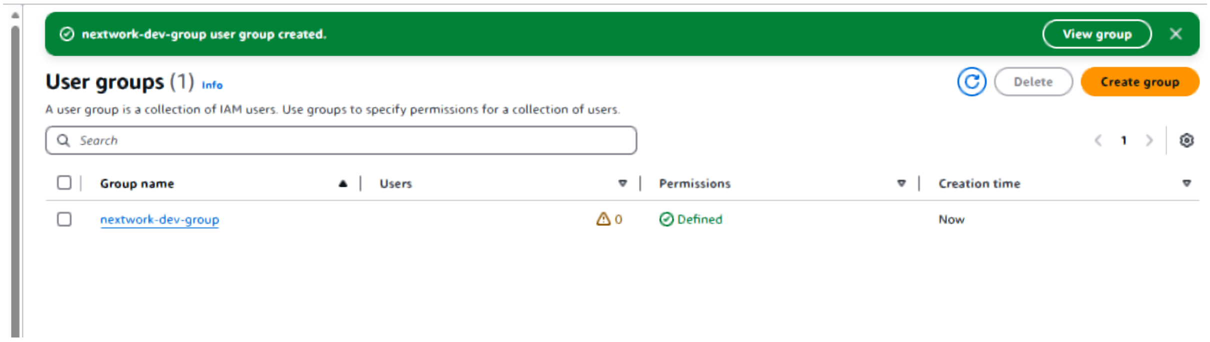
AWS Account

Account ID
329599662468

Account Alias
Create

Sign-in URL for IAM users in this account
https://329599662468.signin.aws.amaz sole

-
- Create IAM Users and User Groups
- **In this step, get ready to:**
- Set up a dedicated IAM **group** for all NextWork interns, so you can manage all interns' permissions from one place.
- Set up a dedicated IAM **user** for your new intern, so they have a way to log in.
-
- Choose **User groups** in your left-hand navigation panel.
- Choose **Create group**.
- Let's create your first user group!
- To set up your user group:
- Name: nextwork-dev-group
- Attach permission policies: NextWorkDevEnvironmentPolicy
- Select **Create user group**.



nextwork-dev-group user group created.

User groups (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	⚠ 0	✓ Defined	Now

-
- Now let's add Users to your user group.
- Choose **Users** from the left-hand navigation panel.
- Choose **Create user**.

- Let's set up this user! Under **User name**, enter nextwork-dev-yourname
- Tick the checkbox for **Provide user access to the AWS Management Console**.
- Uncheck the box for **Users must create a new password at next sign-in - Recommended**.
- 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**!
- Test your intern's access

- **In this step, get ready to:**

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