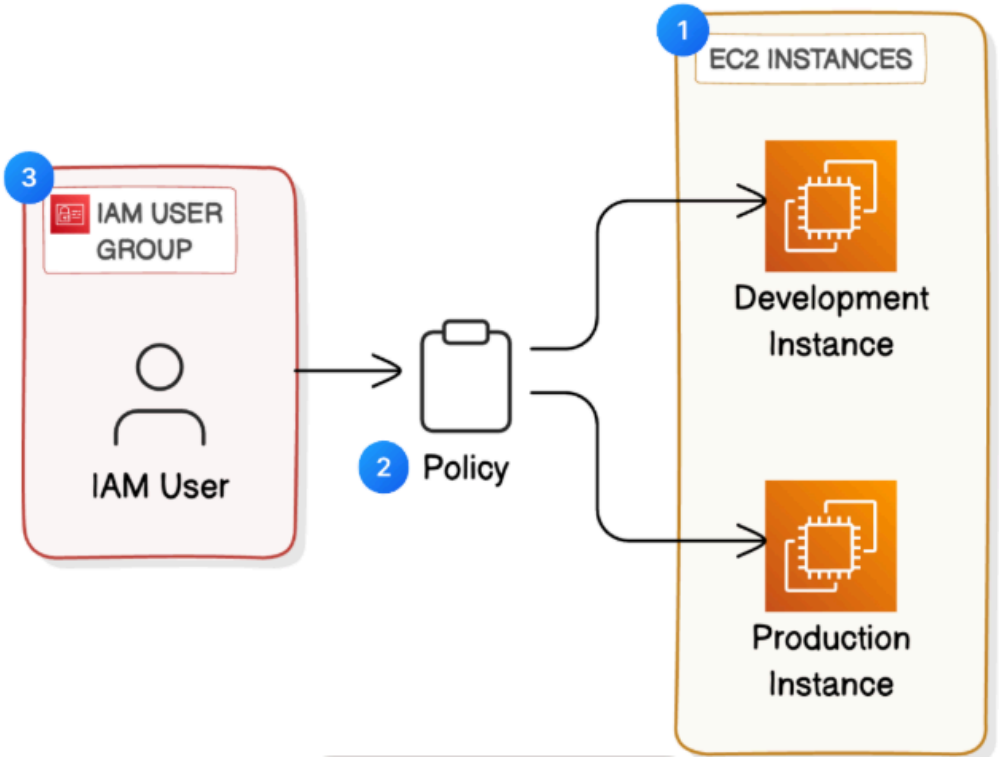
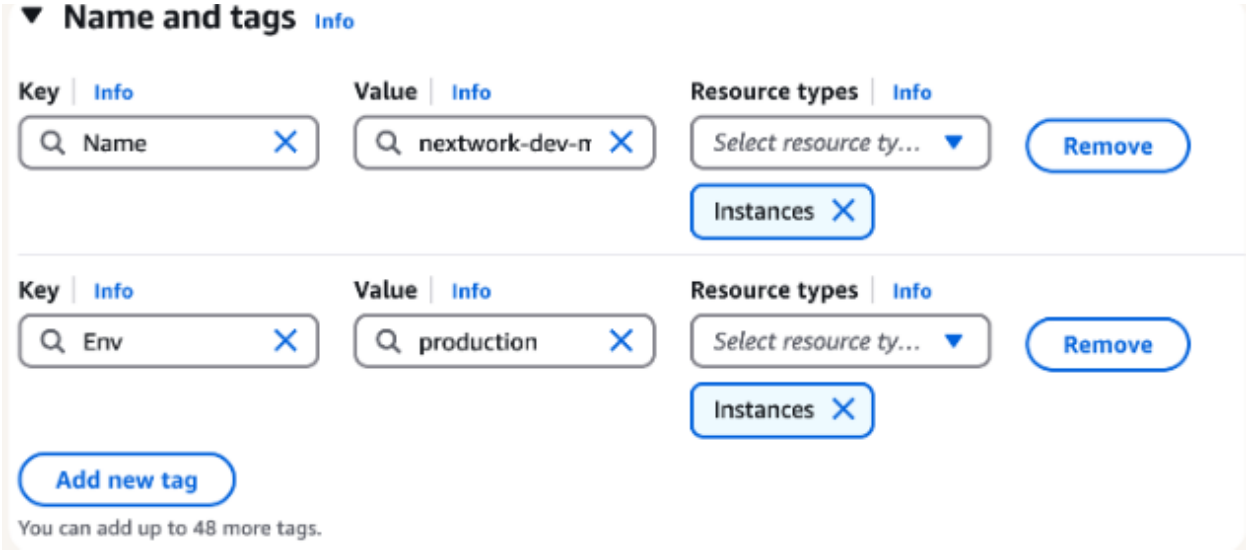
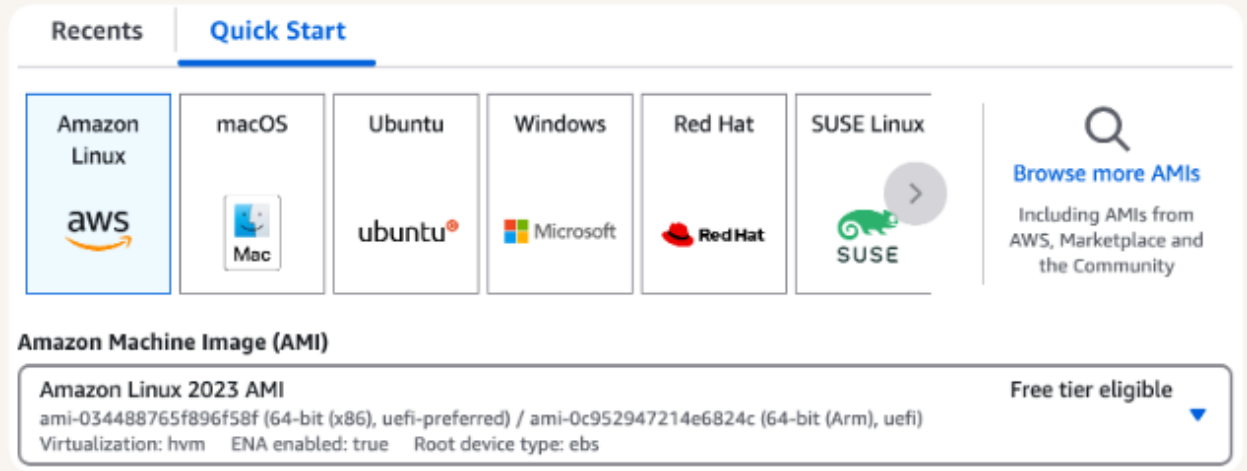
Setting up IAM in AWS EC2 instance



- [Log in to your AWS Management Console](#).
- Open your EC2 console - search for it at the search bar.
- Switch your **Region** to the one closest to you!
- In your EC2 console, choose **Launch instance**.
- In **Name**, enter the value.
    - nextwork-prod-Russell
- 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**.
- You're ready! Click **Launch instance**.

Now let's create one more EC2 instance for the **development environment**.

Repeat the same flow, but this time using these tags:

- Name: nextwork-dev-Russell
- Env: development
- Launch your second instance.
- Select **Instances** from your left hand navigation panel.
- If you only see one instance on your page, make sure to use that refresh button!
- Select the checkbox next to one of your instances, and a popup window of information pops up!
- Select the **Tags** tab.

Create an IAM Policy

🎉 WOOOOOOO! You've deployed two EC2 instances, one for your production environment and one for your development environment.

Now let's move into our second task as NextWork's engineer - it's time to onboard the team's new intern and set up permission policies.

Our intern should have permission to the development EC2 instance but not the production instance. We don't want them to accidentally shut down the platform or push their changes to the production environment while they're just testing things!

To start this task, we'll use AWS IAM to give our intern access to the development instance first.

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.

Here's the policy you'll be using! 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": "*"
   }
  ]
}
```

- 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** when you're done.

Create an AWS Account Alias

Alrighty, that was the permission policy all set up ✅

Now that we can give our intern access to the development instance, the intern can't wait to start. They'd love to jump into the team's AWS account right away!

Sounds great... where should they go to log in?

- Still in your IAM console, select Dashboard from the left hand navigation panel.
- In the right-hand side of the dashboard, choose **Create** under **Account Alias**.

In the **Preferred alias** field, enter

- nextwork-alias-Russell

Choose **Create alias**.

- 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**. Success!

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-Russell
- 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

- 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!
- Woah! Welcome back to your AWS console, but this time as the dev user that you've created for yourself.
- 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-dev-yourname**.
- Under the **Actions drop-down**, select **Manage instance state**.
- Select **Stop**, then **Change state**. Select **Stop**.
- Success!
-