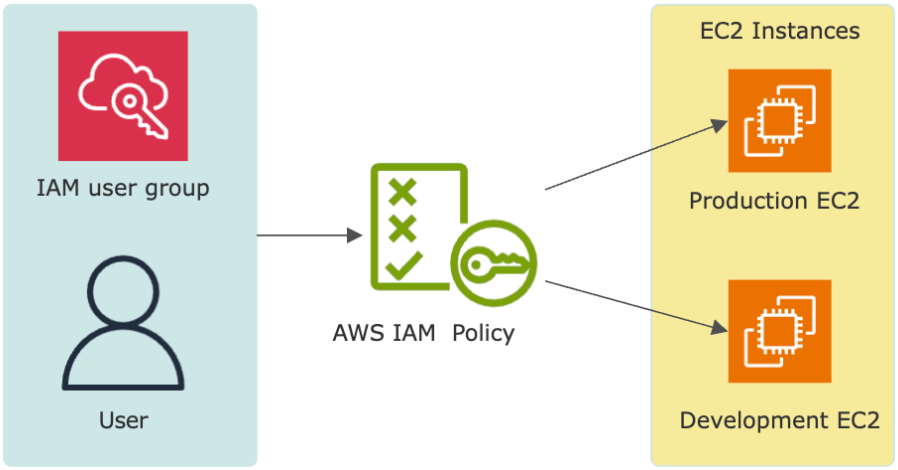
New Employee's Dev-Env Access with AWS IAM

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.

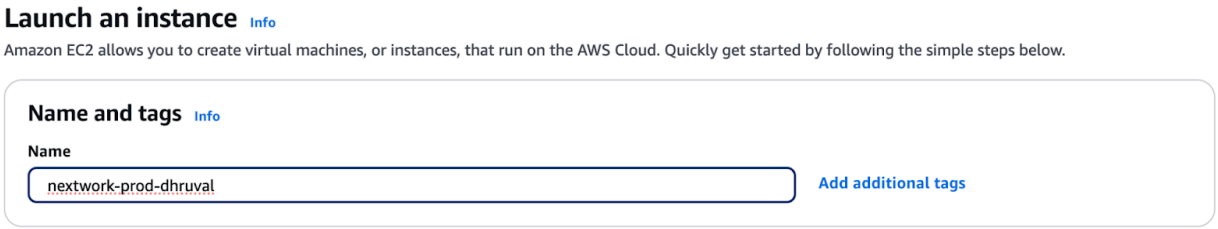


Note: make sure you select the closet region before starting for better performance.

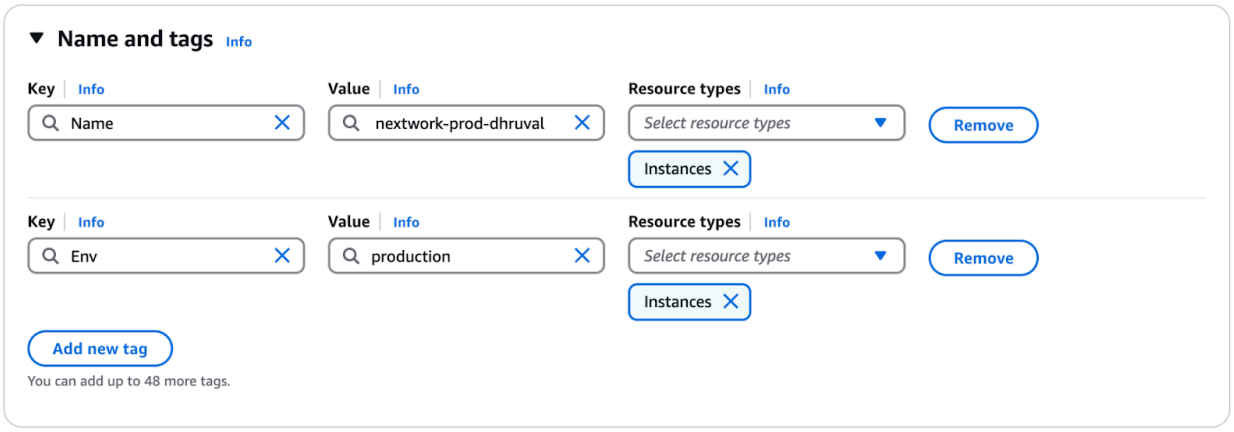
Launch EC2 instances:

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

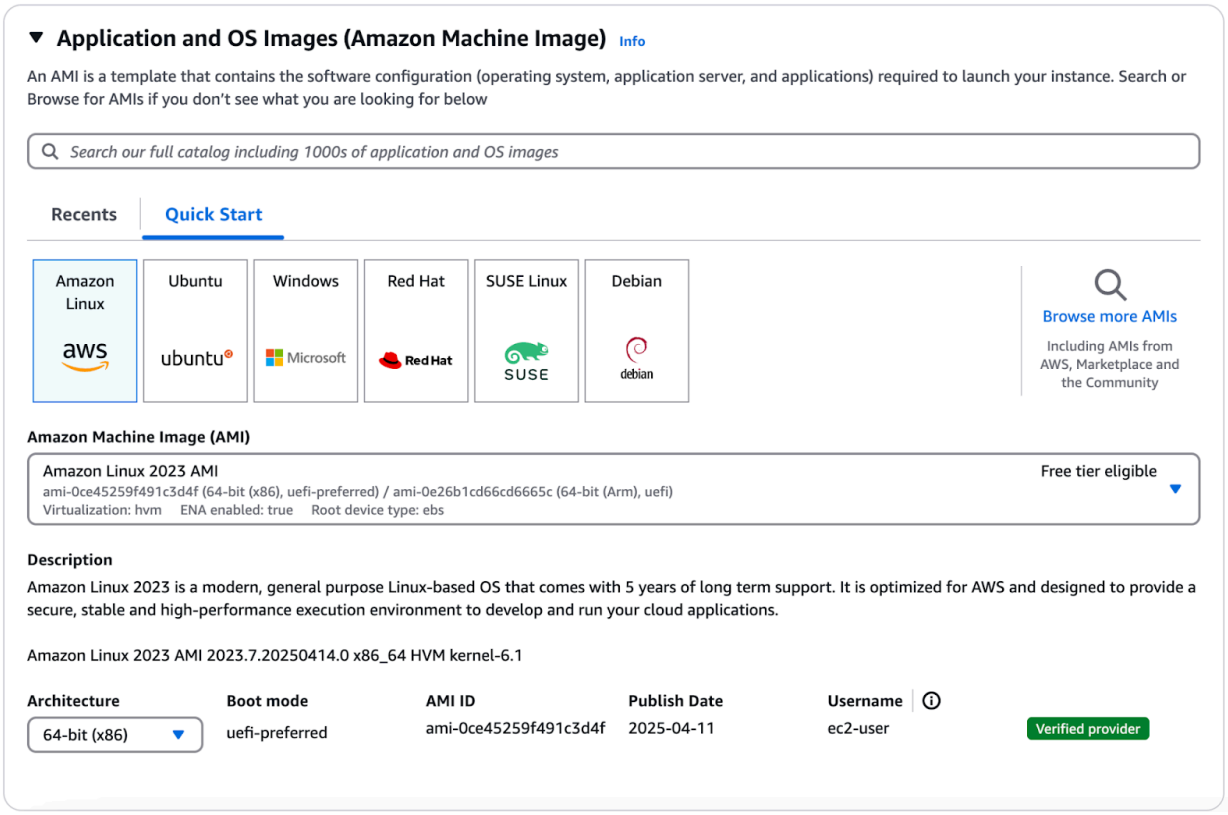
1. Launch an instance for prod.



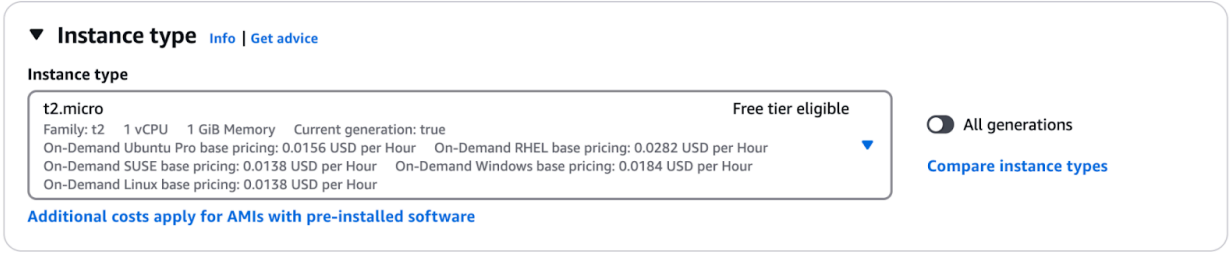
2. Choose Add additional tags, which is right next to the Name field.
    a. Choose Add new tag.
    b. For the next tag, use this information:
        i. Key: Env
        ii. Value: production



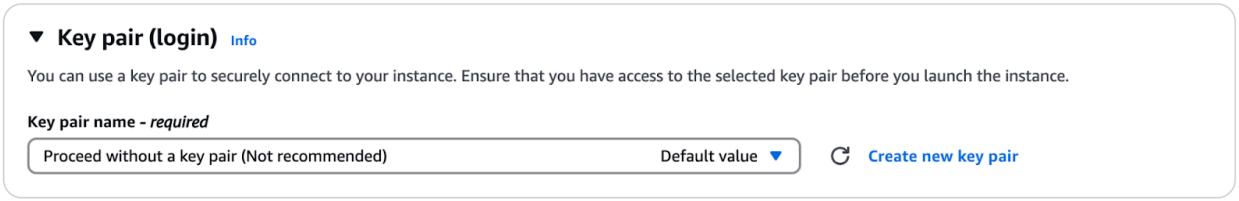
3. Select free tier Amazon Machine Image (AMI).



4. Select default free tier instance type.

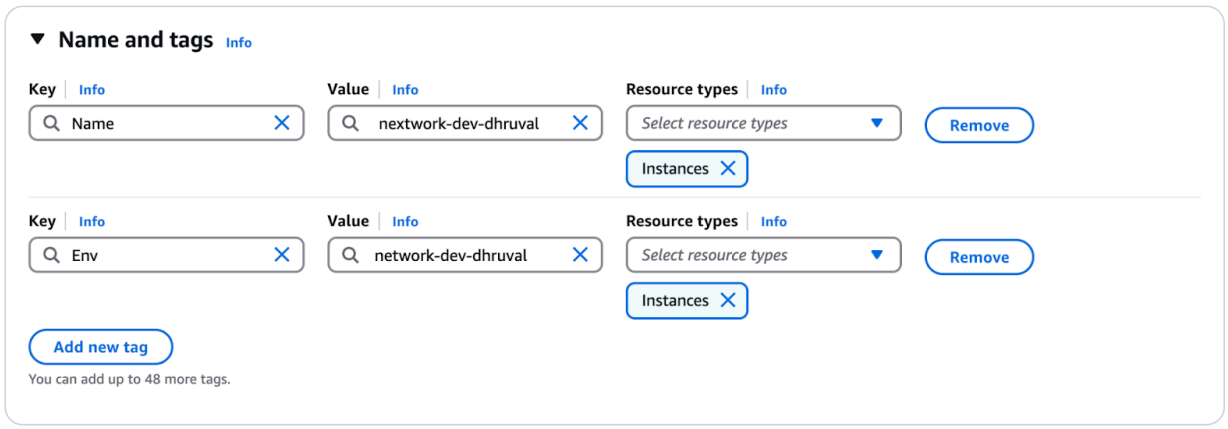


5. For the key pair select, proceed without keypair (not recommended but for this project no need for SSH).

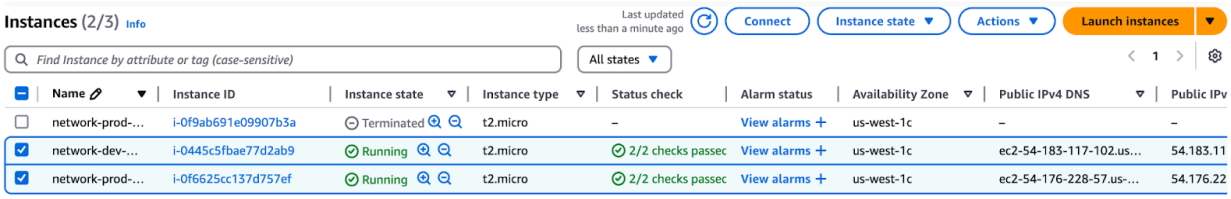


6. Leave network settings and Configure storage default and then click Launch Instance.

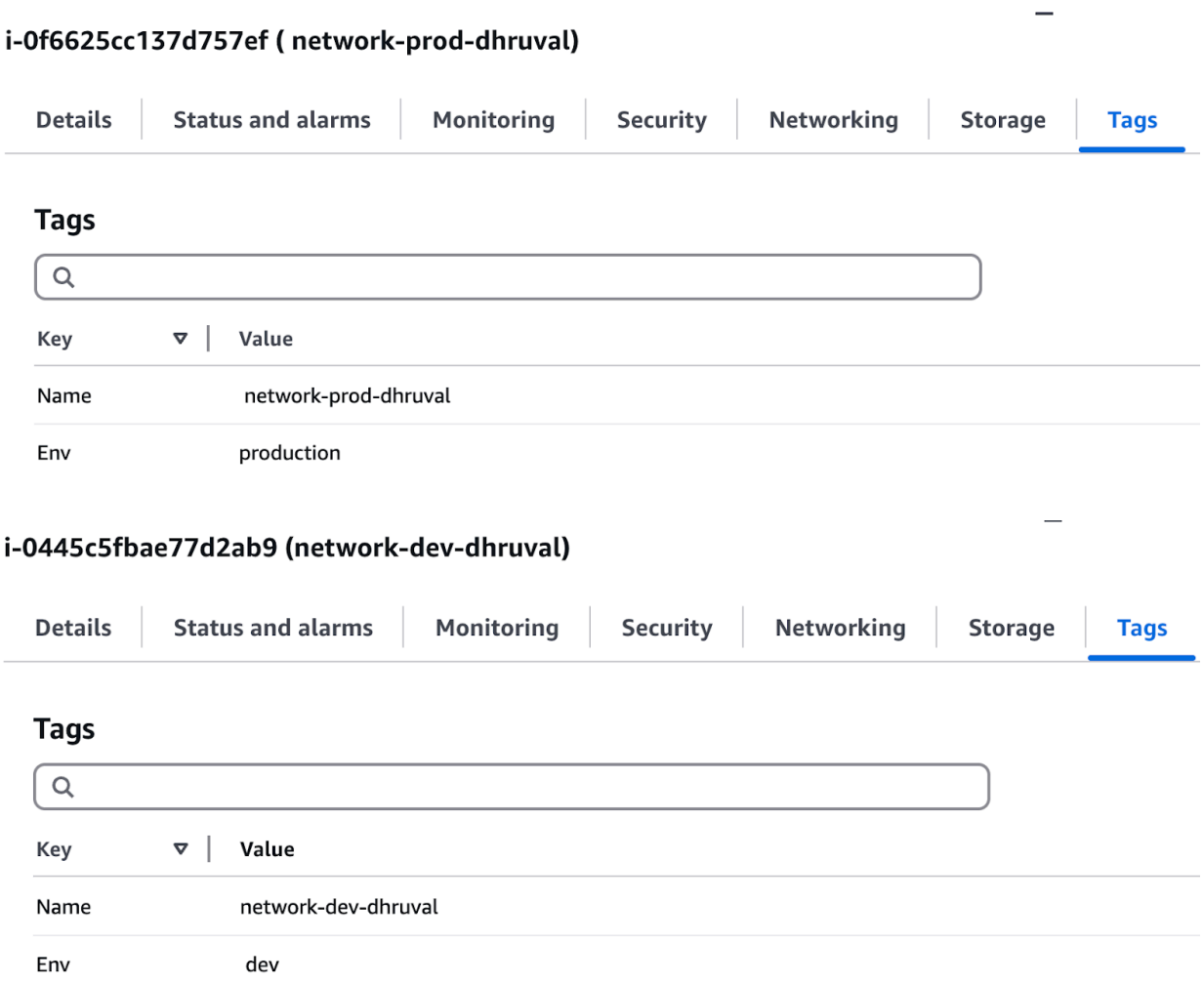
7. Repeat the same steps for creating the dev EC2 instance. Keep Amazon Machine Image (AMI), instance type, and key pair same Just change the EC2 instance name and the env value to development in tags. EC2 See screenshots below



You should have successfully created the 2 new EC2 instances



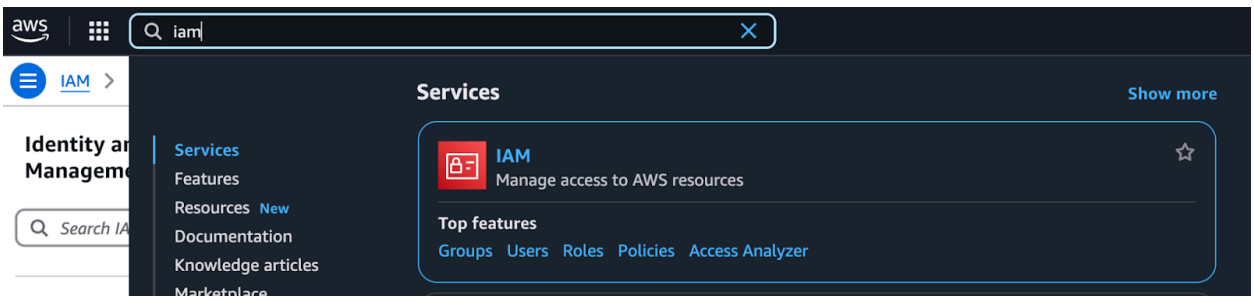
Note: double check tags for both instances



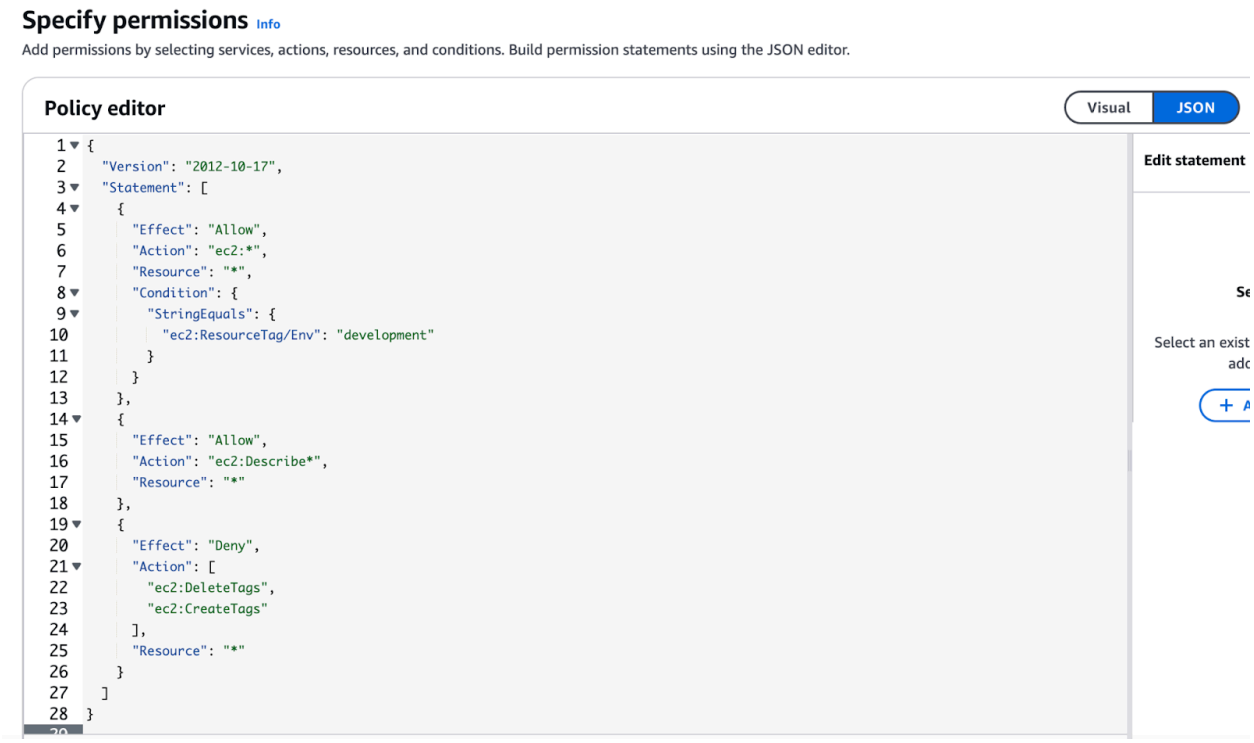
Create an IAM Policy:

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.

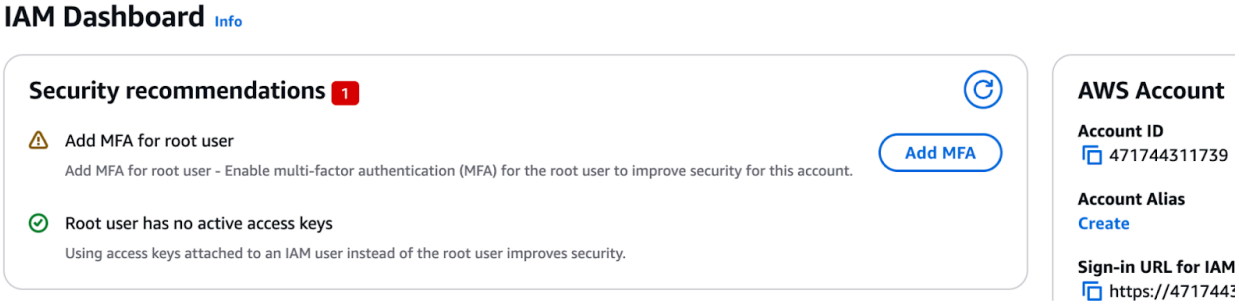


4. Fill in policy's details:
    - Name: NextWorkDevEnvironmentPolicy
    - Description: IAM Policy for NextWork's development environment
    - And then select “Create policy”

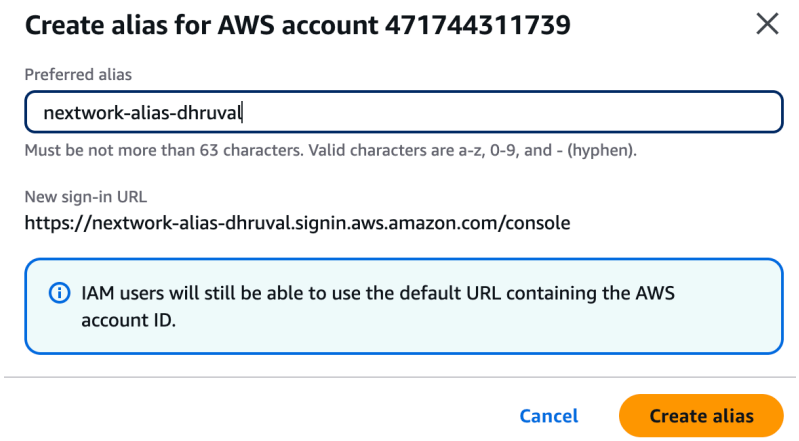
Create an AWS Account Alias:

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.



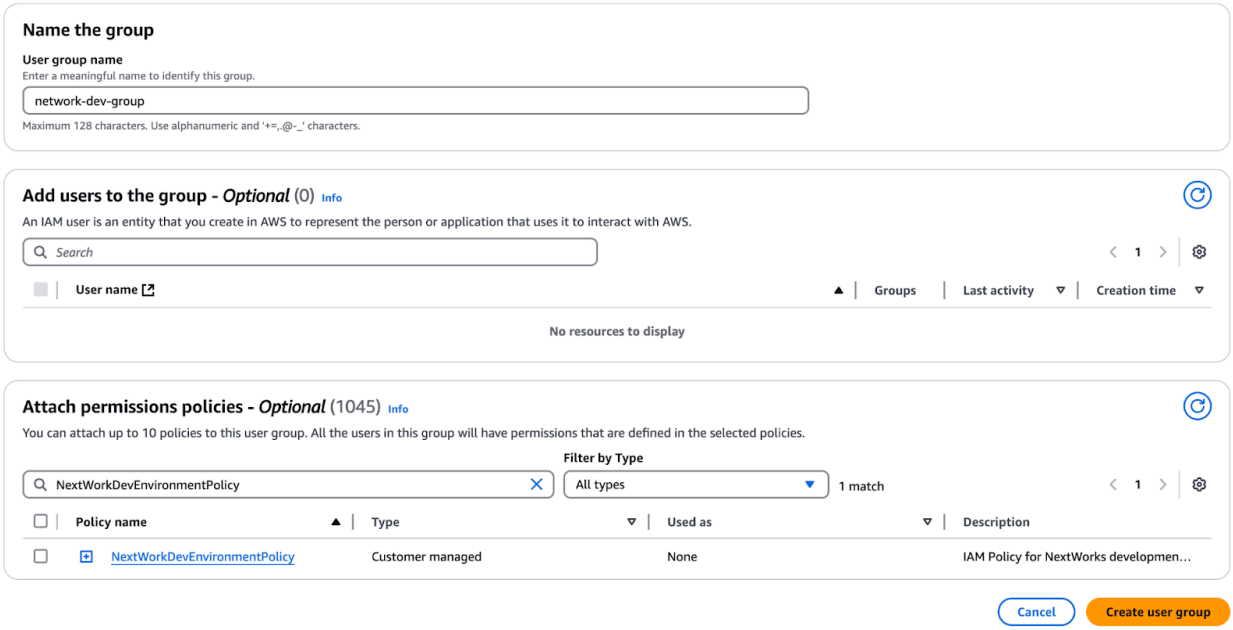
Name the alias and create.



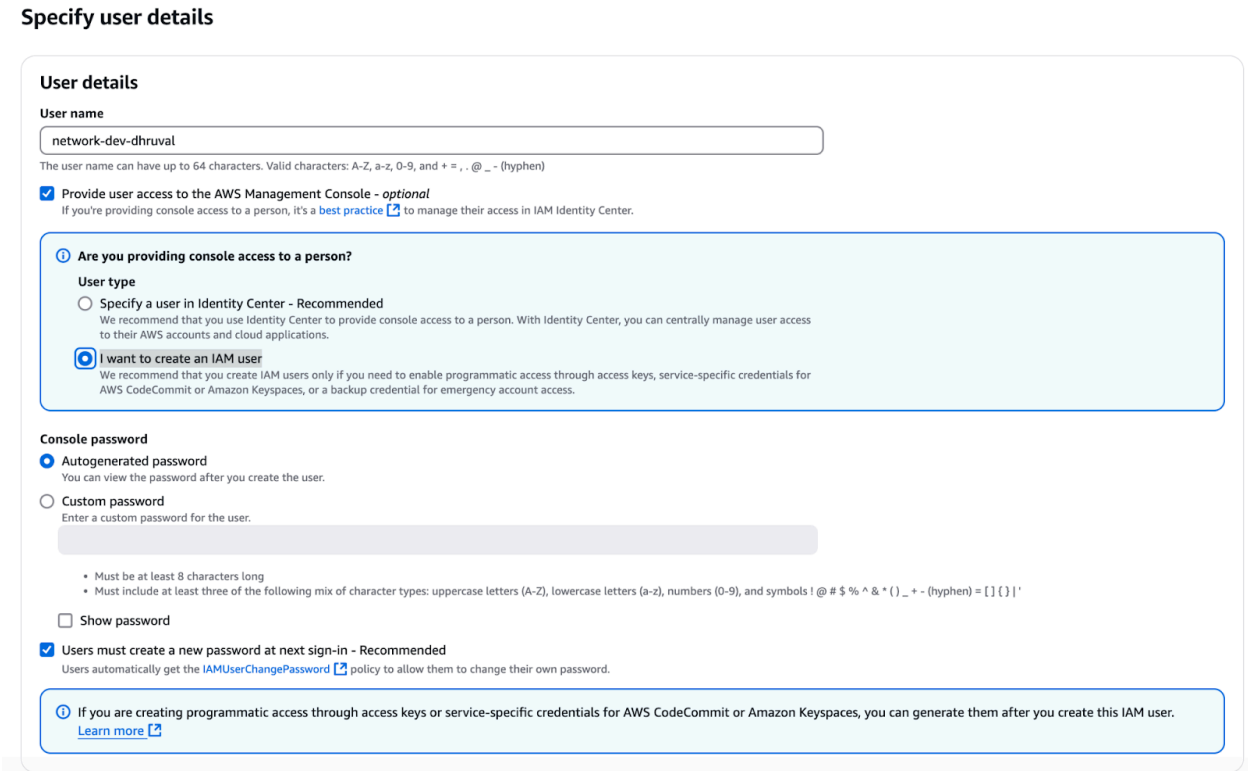
Create IAM Users and User Groups:

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

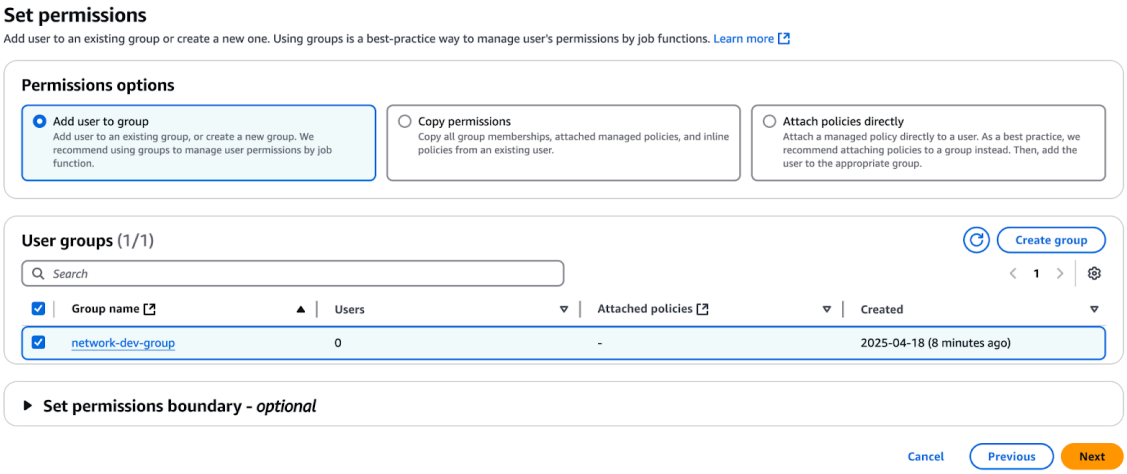
1. From the IAM Dashboard select user groups on the left navigation section and create groups.
2. To set up the user group:
    - Name: network-dev-group
    - Attach permission policies: NextWorkDevEnvironmentPolicy
    - Then create user group



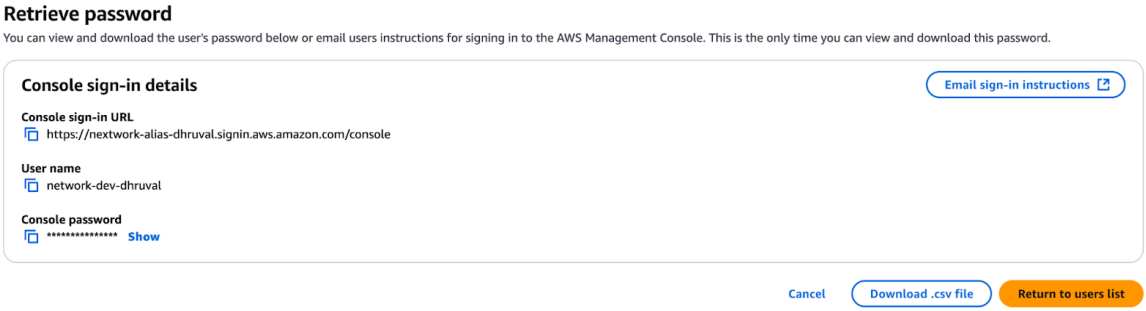
3. Next select users on the left navigation section and create user.
4. Name the user, for user type select “I want to create an IAM user” for sign in and access and then select next.



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



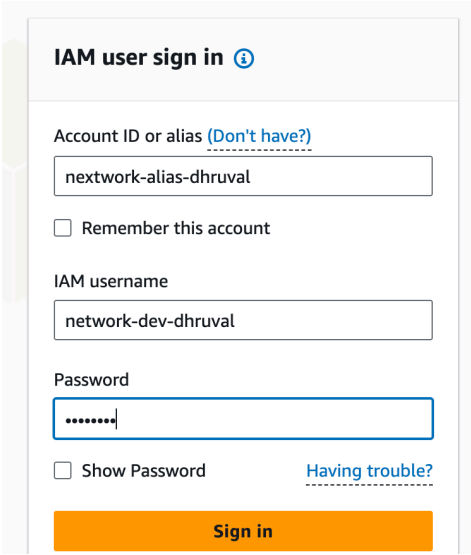
Note: there will be a console sign in details after review and create.



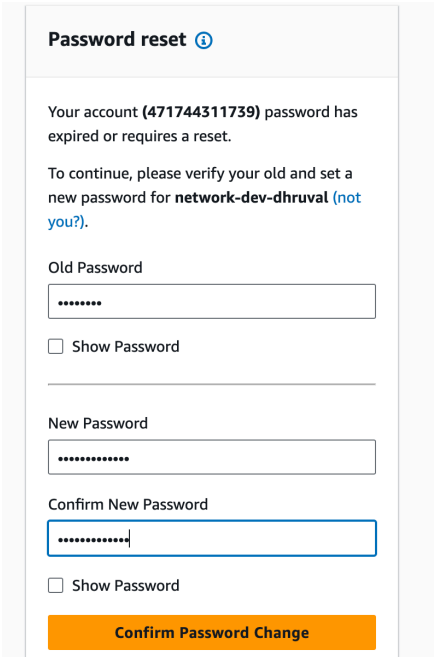
Test the employee’s login access:

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

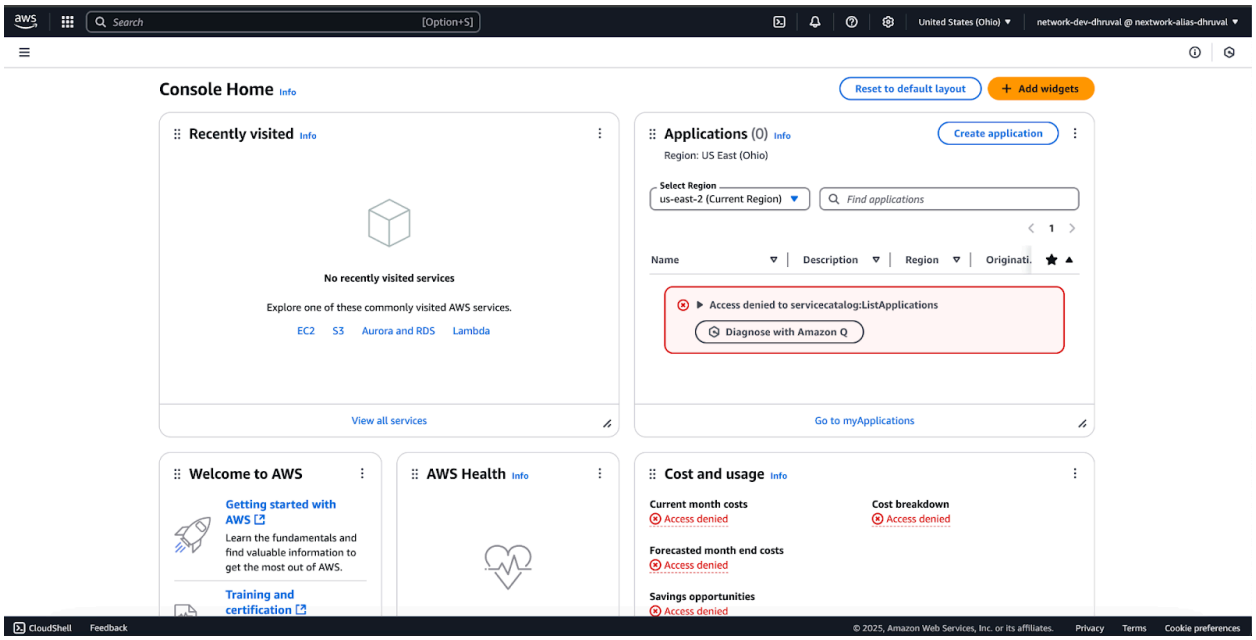
1. Copy console sign-in URL, paste in a new incognito window and login with the given username and password.



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



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



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