DevOps
AIDE501 – M2 – 3 Credits
2026/2027

Course Contents

- **Chapter 1: Cloud Computing**
- **Chapter 2: Containerization**
- **Chapter 3: Shell Scripting**
- **Chapter 4: DevOps**
- **Chapter 5: Orchestration**
- **Chapter 6: GitLab CI/CD**

Chapter 1:

Cloud Computing

Amazon Web Services (AWS) Cloud

AWS account setup

- Prerequisites: to set up and secure your new AWS account, you will need the following:
- A web browser with access to AWS
- Credit card to set up AWS account (only for verification, access is free for many resources.)
- Email and Phone number to verify your account setup

- Create an AWS account
- https://aws.amazon.com/free/offers/

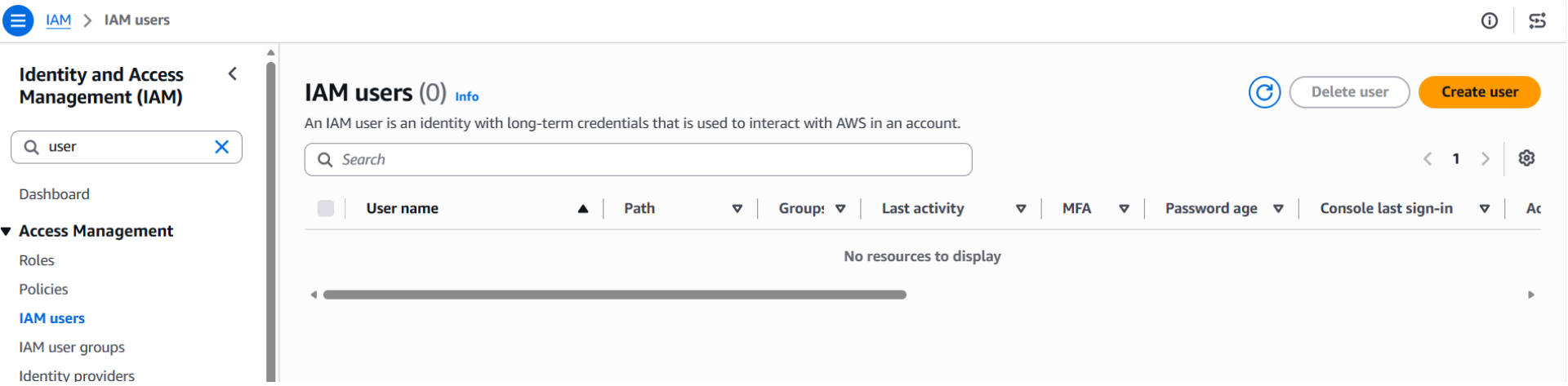
AWS account setup

- Secure the Root user: Add MFA and Remove API Access Key
- AWS best practices include some immediate changes to protect the default root user.
- These protections are located under the IAM (Identity and Access Management) service in AWS, which allows you to manage access to AWS services in your account.



AWS account setup

- For AWS IAM include not using the root account but instead setting up a new user and then using separate user accounts for normal operations. Lock away the root account access in a safe manner.
- Navigate to IAM page in AWS Console.
- Type IAM in the search box and click on IAM link.
- Click on Users on the left and click create user at the top right of the screen.



AWS account setup

User details

User name

M2_AIDE_User_2026-2027

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*

In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

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

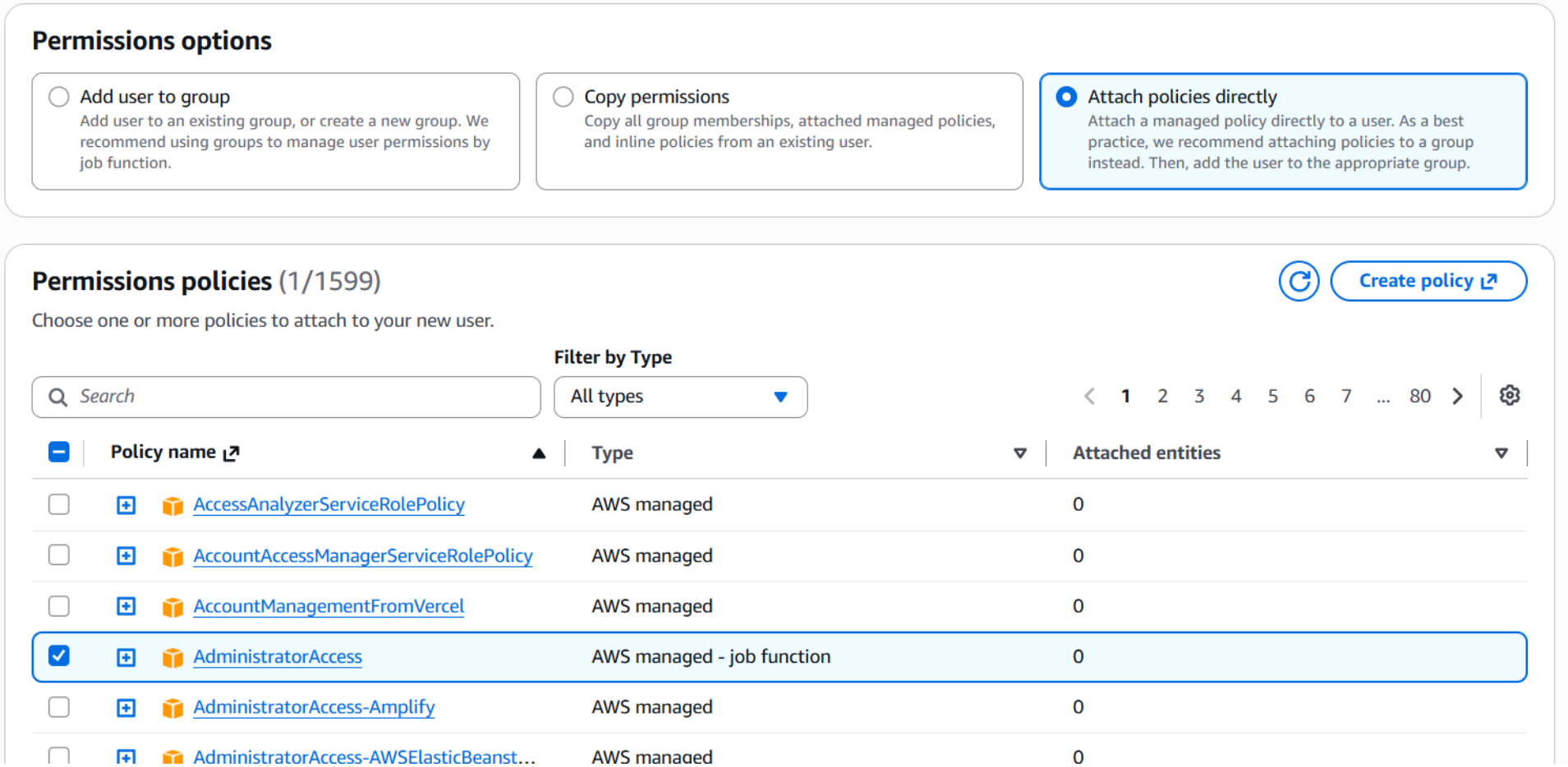
☐ Users must create a new password at next sign-in - Recommended

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

Cancel Next

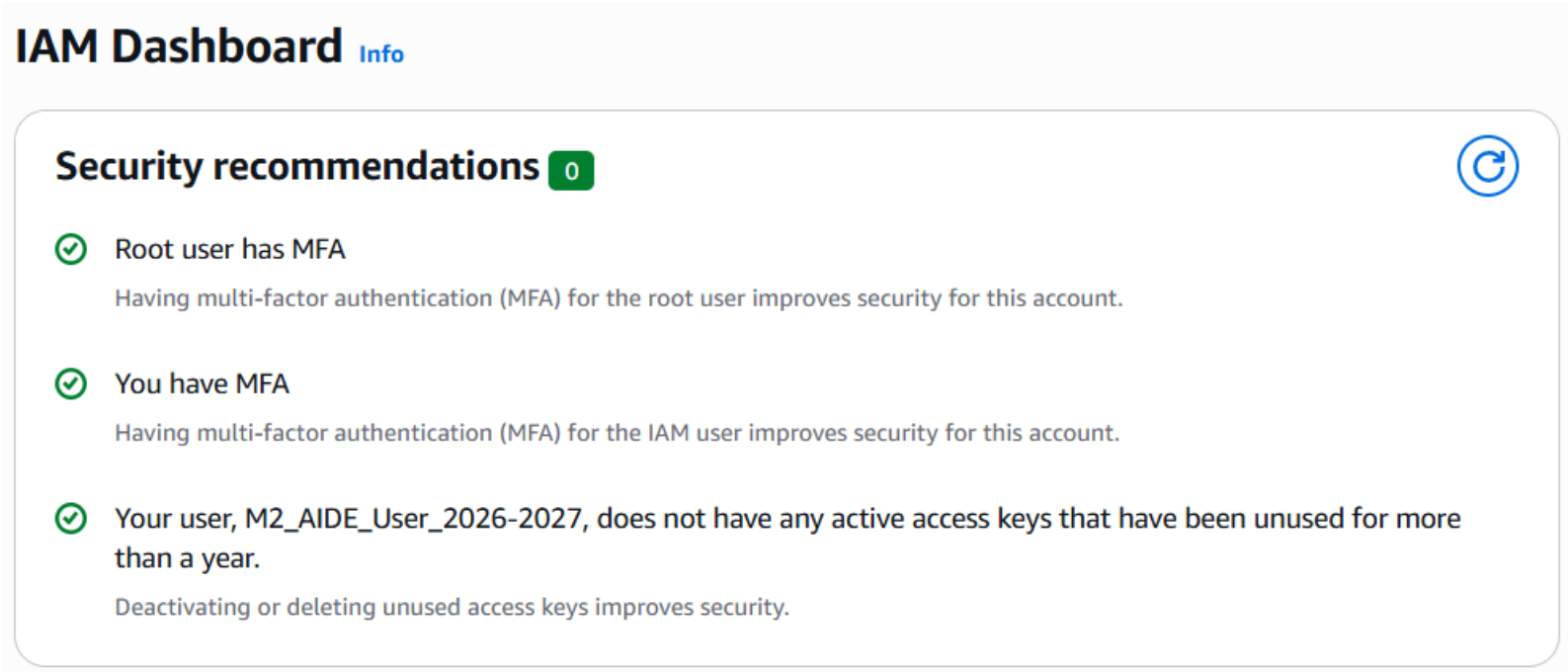
AWS account setup



After you click create user, download the csv file and keep it save in your laptop.

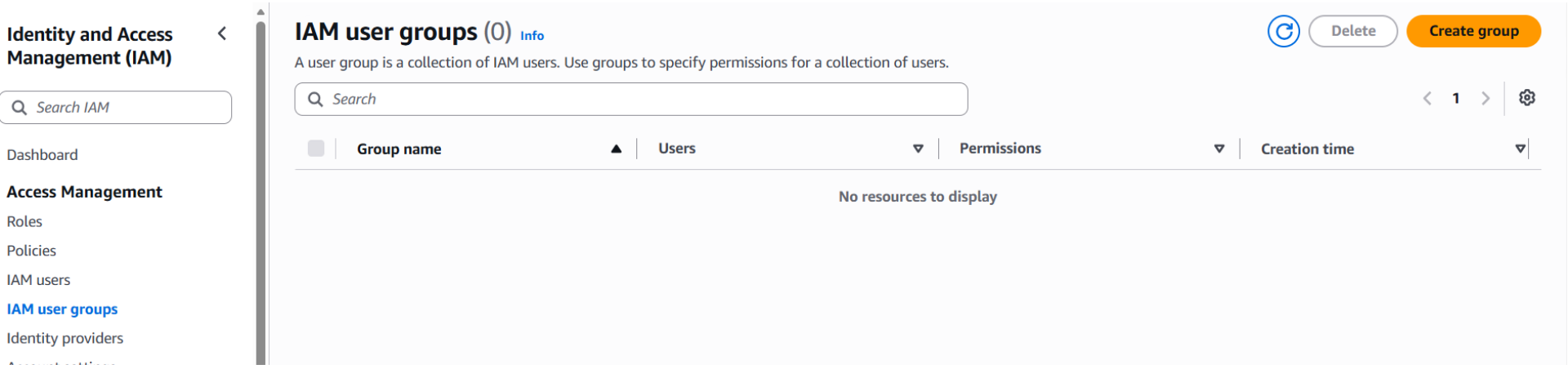
AWS account setup

- Copy the console sign in URL link to your browser and login as the new user
- Sign out from your root account
- Loging as the newly create user with the new URL
- Enable MFA to the new user



AWS account setup

- Create new Group and add a user to the group
- Click user Groups on the left menu or in the dashboard on number 0 in center of the screen.
- Click the “Create group” button and enter “user group name”
- Add users to the group – select the new user id you create
- Select the "AdministratorAccess" policy and click “Create user group”.



AWS account setup

AIDE501_Group

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1/1) 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.

Search

1

User name	Groups	Last activity	Creation time
M2_AIDE_User_2026-2027	0	16 minutes ago	23 minutes ago

Attach permissions policies - *Optional* (1/1232) 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

Search

All types

1 2 3 4 5 6 7 ... 62

Policy name	Type	Used as	Description
AccountManagementFr...	AWS managed	None	
AdministratorAccess	AWS managed - job function	Permissions policy (1)	

AWS account setup

- Set up user access key for AWS CLI
- Click on the Users in left menu and go to “create Access Key 1” to generate a key for AWS CLI access.
- Select “Command Line Interface (CLI)” and tick the confirmation box. The key is now created. Download the CSV file.
- Configure AWS CLI with your key. Choose Zone as the default one of your account.

```
PS C:\> cat ~/Downloads/LUMASTER_accesskeys.csv
Access key ID,Secret access key
AKIAXKPUZ4YPHAJHCZXL,zq/04ZOMCyy/JeJPyrzBTIf8NMs6RDMjccIFRdWJ
PS C:\> aws configure
AWS Access Key ID [None]: AKIAXKPUZ4YPHAJHCZXL
AWS Secret Access Key [None]: zq/04ZOMCyy/JeJPyrzBTIf8NMs6RDMjccIFRdWJ
Default region name [us-east-1]: eu-west-2
Default output format [json]: json
```

AWS account setup

- Validate your AWS CLI is correctly configured by running the following commands:
- aws iam get-account-summary
  - You see a json file like the summaryMap file.
- aws iam list-users --output yaml

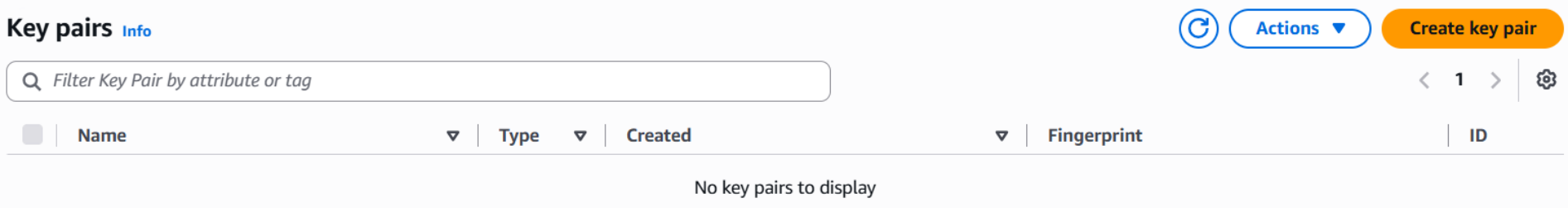
```
PS C:\> aws iam list-users --output yaml
Users:
- Arn: arn:aws:iam::503561446942:user/LUMASTER
  CreateDate: '2025-02-08T17:08:10+00:00'
  PasswordLastUsed: '2025-02-08T17:14:52+00:00'
  Path: /
  UserId: AIDAXKPUZ4YPPY6CBED74
  UserName: LUMASTER
```


```
{
    "SummaryMap": {
        "GroupPolicySizeQuota": 5120,
        "InstanceProfilesQuota": 1000,
        "Policies": 0,
        "GroupsPerUserQuota": 10,
        "InstanceProfiles": 0,
        "AttachedPoliciesPerUserQuota": 10,
        "Users": 1,
        "PoliciesQuota": 1500,
        "Providers": 0,
        "AccountMFAEnabled": 1,
        "AccessKeysPerUserQuota": 2,
        "AssumeRolePolicySizeQuota": 2048,
        "PolicyVersionsInUseQuota": 10000,
        "GlobalEndpointTokenVersion": 1,
        "VersionsPerPolicyQuota": 5,
        "AttachedPoliciesPerGroupQuota": 10,
        "PolicySizeQuota": 6144,
        "Groups": 1,
        "AccountSigningCertificatesPresent": 0,
        "UsersQuota": 5000,
        "ServerCertificatesQuota": 20,
        "MFADevices": 2,
        "UserPolicySizeQuota": 2048,
        "PolicyVersionsInUse": 3,
        "ServerCertificates": 0,
        "Roles": 2,
```

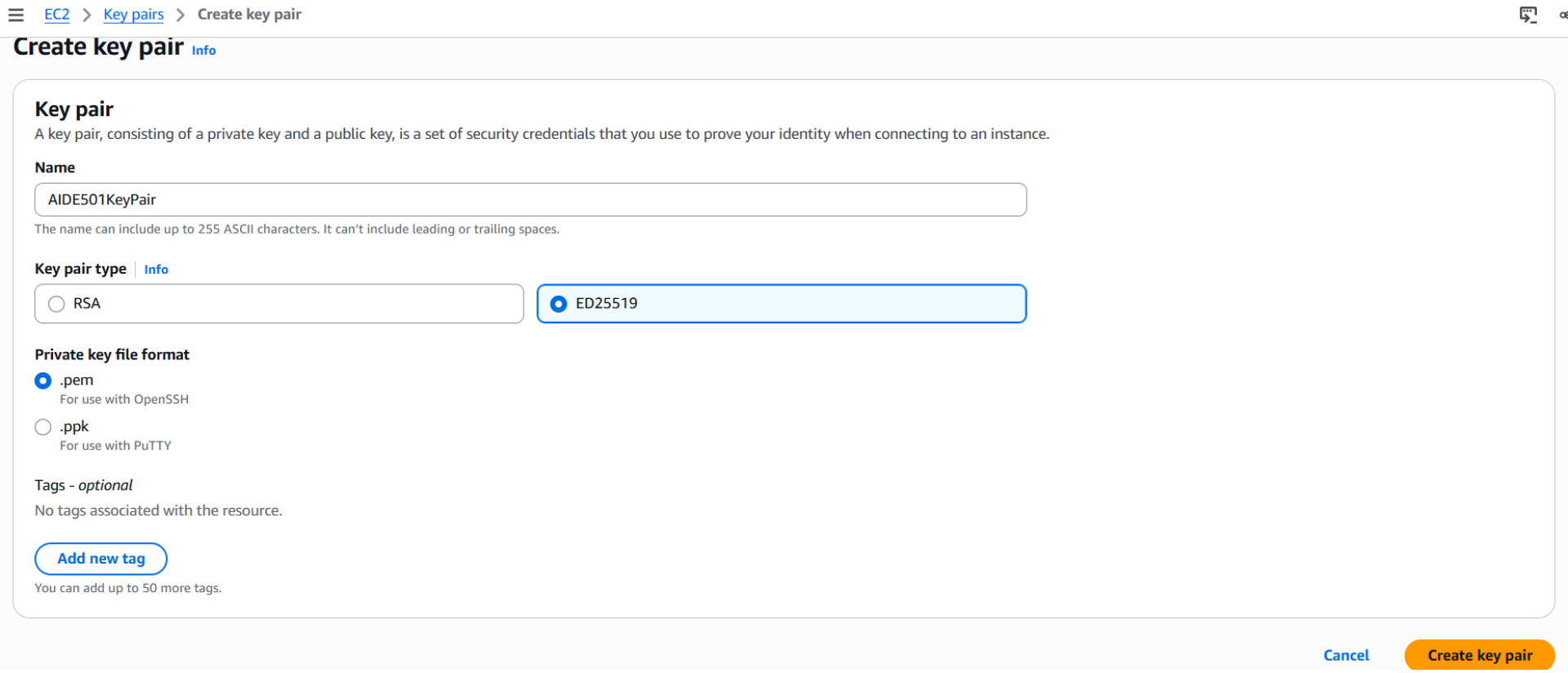
AWS account setup

- Generate and Configure SSH Key
- AWS allows you to deploy Linux hosts (called EC2 instances) in your account. You can then access these instances remotely with SSH using an SSH key (called an EC2 keypair). Each time you create a new Linux EC2 instance, you are given the option to choose an existing keypair or create new one.

- Navigate to “Key Pairs”



AWS account setup



AWS account setup

- Prerequisites: to set up and secure your new AWS account, you will need the following:
- A web browser with access to AWS
- Credit card to set up AWS account (only for verification, access is free for many resources.)
- Email and Phone number to verify your account setup

- Create an AWS account
- https://aws.amazon.com/free/offers/