⚠ **Do not change the lab Region unless specifically instructed to do so**.

# Task 1: Create an account password policy

In this task, you create a custom password policy for your AWS account. This policy affects all the users associated with the account.

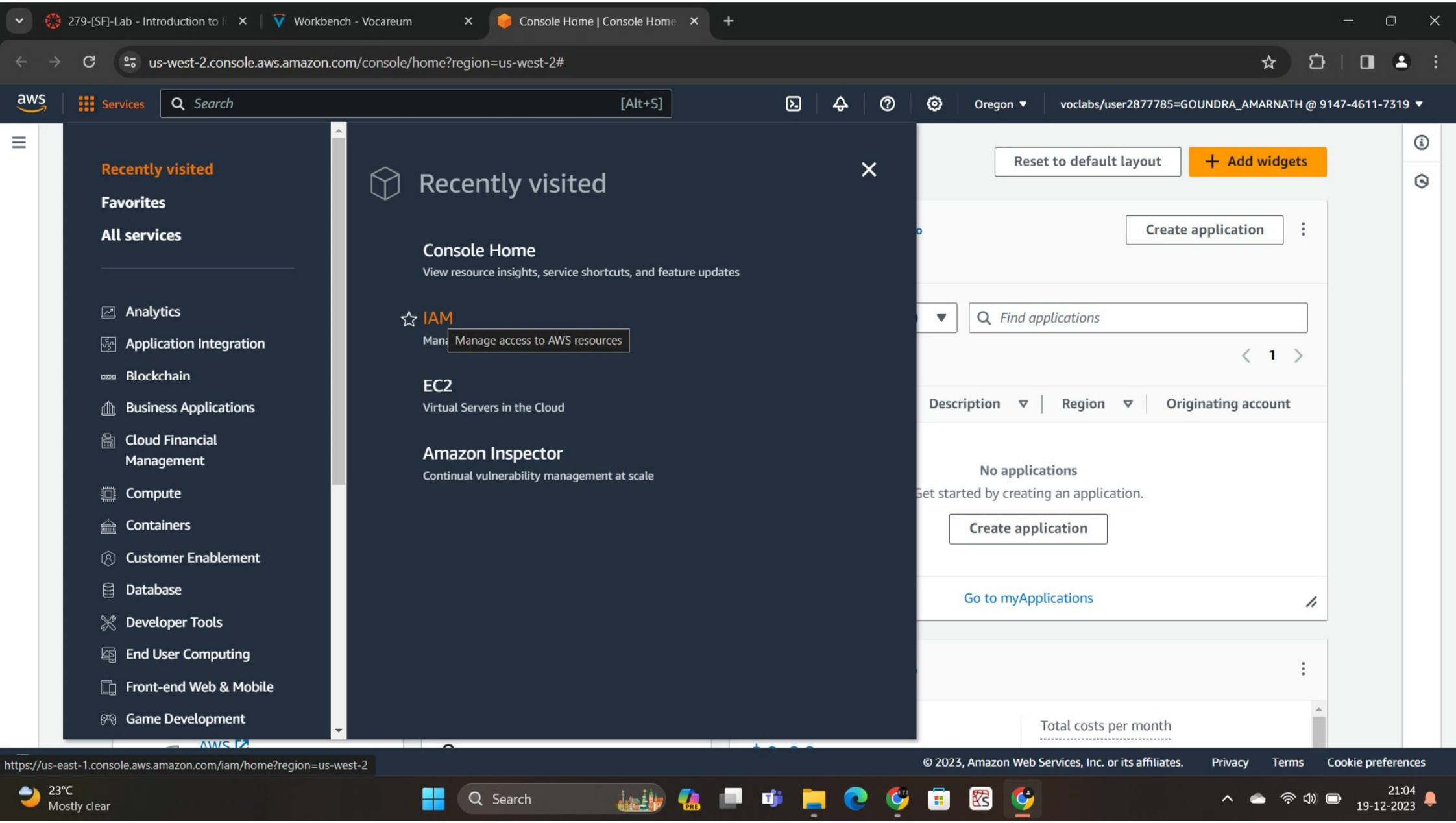
6. First, note the Region that you are in (for example, **Oregon**). The upper-right corner of the console page displays your Region.
7. In the AWS Management Console, in the search 🔍 box, enter `IAM` and select it.
8. In the left navigation pane, choose **Account settings**.

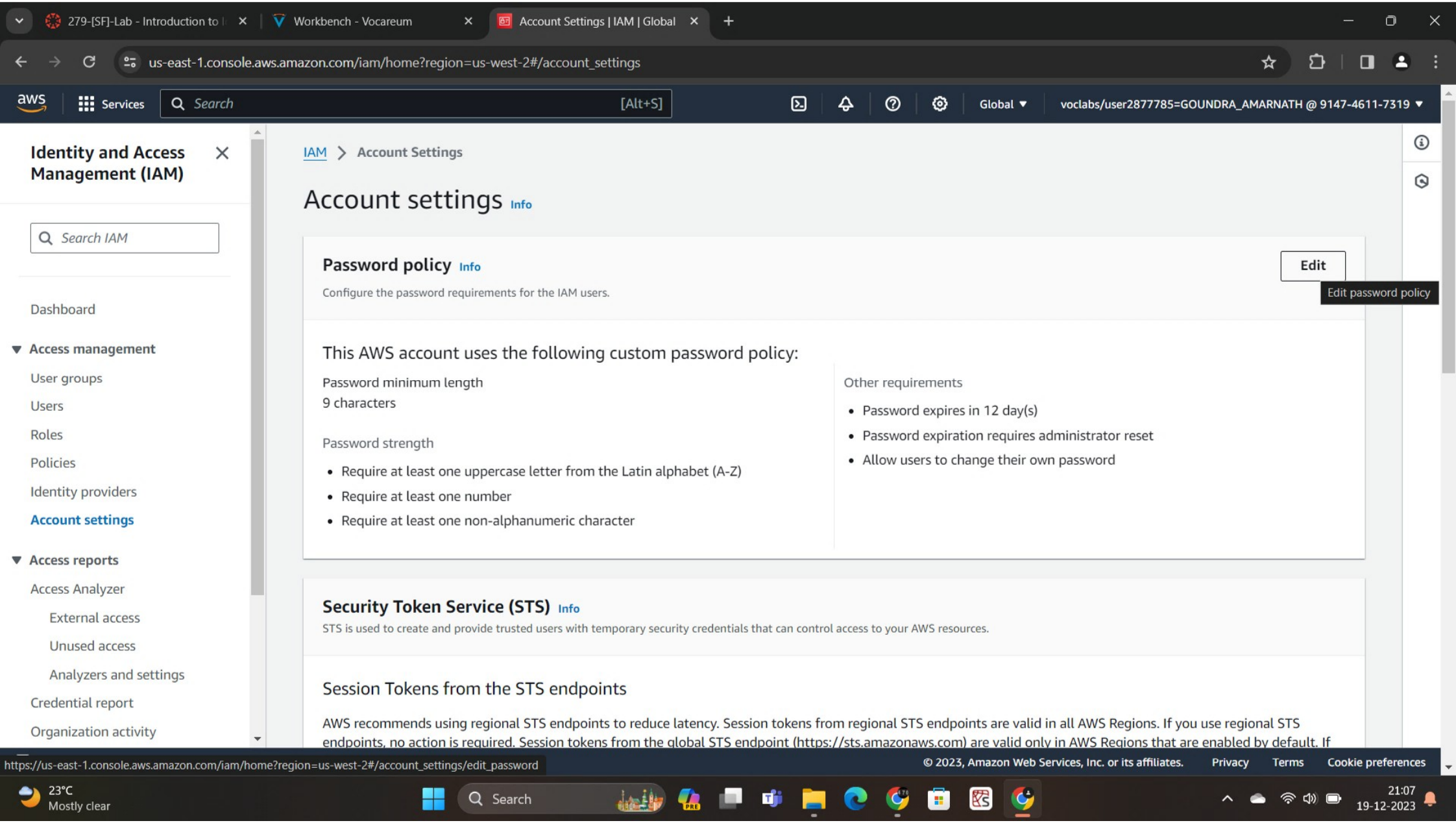
   Here you can see the default password policy that is currently in effect. The company that you are working for has much stricter requirements, and you need to update this policy.
9. Choose **Change password policy**.
10. Under **Select your account password policy requirements**, configure the following options:
    - For **Enforce minimum password length**, change `8` to `10` characters.
    - Select every check box except the check box for **Password expiration requires administrator reset**.
    - For **Enable password expiration**, leave the default option of **90** days.
    - For **Prevent password reuse**, leave the default option of **5** passwords.
11. Choose **Save changes**.

    These changes take affect at the AWS account level and apply to every user associated with the account.

## Summary of task 1

In this task, you strengthened the password requirements by creating a custom password policy. The various password options that you


279-[SF]-Lab - Introduction to
Workbench - Vocareum
Console Home | Console Home
us-west-2.console.aws.amazon.com/console/home?region=us-west-2#
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 9147-4611-7319
Recently visited
Favorites
All services
Analytics
Application Integration
Blockchain
Business Applications
Cloud Financial Management
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Recently visited
Console Home
View resource insights, service shortcuts, and feature updates
IAM
Manage access to AWS resources
EC2
Virtual Servers in the Cloud
Amazon Inspector
Continual vulnerability management at scale
Reset to default layout
Add widgets
Create application
Find applications
Description
Region
Originating account
No applications
Get started by creating an application.
Create application
Go to myApplications
Total costs per month
https://us-east-1.console.aws.amazon.com/iam/home?region=us-west-2
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
23°C
Mostly clear
Search
21:04
19-12-2023


279-[SF]-Lab - Introduction to
Workbench - Vocareum
Account Settings | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#/account_settings
aws
Services
Search
[Alt+S]
Global
voclabs/user2877785=GOUNDRA_AMARNATH @ 9147-4611-7319
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzers and settings
Credential report
Organization activity
IAM > Account Settings
Account settings Info
Password policy Info
Configure the password requirements for the IAM users.
Edit
Edit password policy
This AWS account uses the following custom password policy:
Password minimum length
9 characters
Password strength
Require at least one uppercase letter from the Latin alphabet (A-Z)
Require at least one number
Require at least one non-alphanumeric character
Other requirements
Password expires in 12 day(s)
Password expiration requires administrator reset
Allow users to change their own password
Security Token Service (STS) Info
STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.
Session Tokens from the STS endpoints
AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (https://sts.amazonaws.com) are valid only in AWS Regions that are enabled by default. If
https://us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#/account_settings/edit_password
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
23°C
Mostly clear
Search
21:07
19-12-2023

# Edit password policy Info

## Password policy

- ○ IAM default
  Apply default password requirements.
- ◉ Custom
  Apply customized password requirements.

Password minimum length.
Enforce a minimum length of characters.

3 characters

Needs to be between 6 and 128.

Password strength

- [x] Require at least one uppercase letter from the Latin alphabet (A-Z)
- [ ] Require at least one lowercase letter from the Latin alphabet (a-z)
- [x] Require at least one number
- [x] Require at least one non-alphanumeric character ( ! @ # $ % ^ & * ( ) _ + - = [ ] {} | ' )

Other requirements

- [x] Turn on password expiration

  Expire password in 12 day(s)

  Needs to be between 1 and 1095 days.
- [x] Password expiration requires administrator reset
- [x] Allow users to change their own password
- [ ] Prevent password reuse

Cancel | Save changes

# Edit password policy Info

## Password policy

- ○ IAM default
  Apply default password requirements.
- ◉ Custom
  Apply customized password requirements.

Password minimum length.
Enforce a minimum length of characters.

7 characters

Needs to be between 6 and 128.

Password strength

- [x] Require at least one uppercase letter from the Latin alphabet (A-Z)
- [ ] Require at least one lowercase letter from the Latin alphabet (a-z)
- [x] Require at least one number
- [x] Require at least one non-alphanumeric character ( ! @ # $ % ^ & * ( ) _ + - = [ ] {} | ' )

Other requirements

- [x] Turn on password expiration

  Expire password in 12 day(s)

  Needs to be between 1 and 1095 days.
- [x] Password expiration requires administrator reset
- [x] Allow users to change their own password
- [ ] Prevent password reuse

Cancel | Save changes

# Task 2: Explore users and user groups

In this task, you explore the users and user groups that have already been created for you in IAM.

12. In the left navigation pane, choose **Users**.

    The following IAM users have been created for you:

    - user-1
    - user-2
    - user-3

13. Choose **user-1**.

    This option bring you to a **Summary** page for **user-1**. The **Permissions** tab is displayed.

    Notice that user-1 does not have any permissions.

14. Choose the **Groups** tab.

    user-1 is also is not a member of any user groups.

    ℹ A user group consists of several users who need access to the same data. Privileges can be distributed to the entire group of users rather than to each individual. This option is much more efficient when applying permissions and provides greater overall control of access to resources than applying permissions to individuals.

15. Choose the **Security credentials** tab.

    user-1 is assigned a **Console password**.

16. In the left navigation pane, choose **User groups**.

67. Paste the **Sign-in URL for IAM users in this account** into your private window, and press Enter.

    If this link is not in your clipboard, retrieve it from the text editor where you pasted it earlier.

68. Sign in using the following credentials:

    - **IAM user name:** Enter `user-3`
    - **Password:** Enter `Lab-Password3`

69. Choose **Sign in**.

    If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.

70. From the **Services** menu, choose **EC2**.

71. In the left navigation pane, choose **Instances**.

    As an EC2 administrator, you should now have permissions to stop the EC2 instance.

    Your EC2 instance should be selected. If it is not, choose it.

    ⚠ If you cannot see an EC2 instance, then your Region may be incorrect. In the upper-right of the screen, choose the **Region** menu, and select the Region that you noted at the start of the lab (for example, **Oregon**).

72. From the **Instance state** dropdown list, choose **Stop instance**.

73. In the **Stop instance?** window, choose **Stop**.

    The instance should enter the **Stopping** state and will shut down.

74. Close your private window.

## Summary of task 4