168-[JAWS]-Activity - Install and Configure the AWS CLI

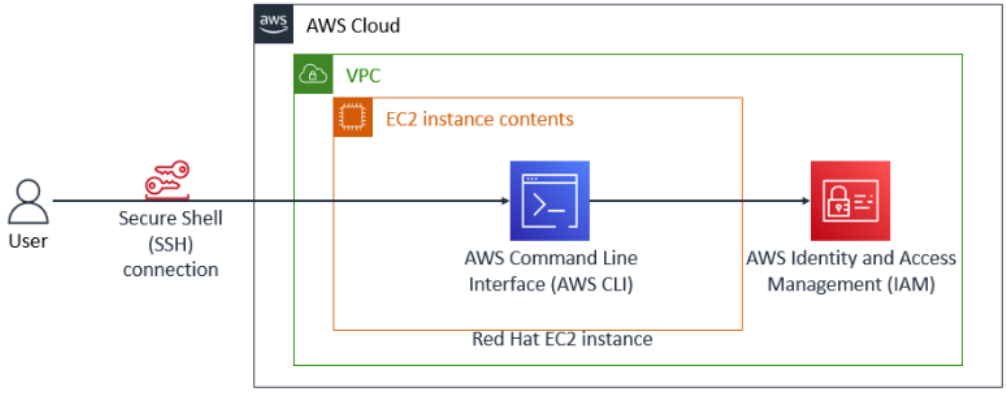
Install and Configure the AWS CLI

Umi Nur F | nurfatih365@gmail.com

A. Lab overview

The AWS Command Line Interface (AWS CLI) is a command line tool that provides an interface for interacting with products and services from Amazon Web Services (AWS). You can install the AWS CLI on your local machine or a virtual machine such as an Amazon Elastic Compute Cloud (Amazon EC2) instance. In this activity, you install and configure the AWS CLI on a Red Hat Linux instance because this instance type does not have the AWS CLI pre-installed. Some instance types, such as Amazon Linux, do come pre-installed with the AWS CLI. During this activity, you establish a Secure Shell (SSH) connection to the instance. You configure the installation with an access key that can connect to an AWS account. Finally, you practice using the AWS CLI to interact with AWS Identity and Access Management (IAM).

When you finish the activity, it will reflect the following diagram:



In the preceding diagram, you can access the AWS Cloud through an SSH connection. Within the AWS Cloud, a virtual private cloud (VPC) with a Red Hat EC2 instance is configured with the AWS CLI. IAM is configured, and you use the AWS CLI to interact with IAM.

Objectives

After completing this lab, you should be able to do the following:

- Install and configure the AWS CLI.

- Connect the AWS CLI to an AWS account.
- Access IAM by using the AWS CLI.

This activity requires approximately 45 minutes to complete.

B. Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch the lab.
2. Wait until the message "Lab status: ready" appears, and then choose X to close the Start Lab panel.
3. Next to Start Lab, choose AWS, which opens the AWS Management Console in a new browser tab. The system automatically signs you in.

   Tip If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose Allow pop-ups.
4. Arrange the AWS Management Console so that it appears alongside these instructions.

   Important: Do not change the lab Region unless specifically instructed to do so.

Task 1: Connect to the Red Hat EC2 instance by using SSH

In this task, you log in to an existing EC2 instance.

Windows users. These instructions are specifically for Windows users. If you are using macOS or Linux, skip to the next section.

5. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
6. Select the Download PPK button and save the labsuser.ppk file. *Typically your browser will save it to the Downloads directory.*
7. Make a note of the PublicIP address.
8. Then exit the Details panel by selecting the X.
9. Download PuTTY to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer, download it here.
10. Open putty.exe

11. Configure your PuTTY session by following the directions in the following link: Connect to your Linux instance using PuTTY
12. Windows Users: Select here to skip ahead to the next task.

macOS and Linux users

These instructions are specifically for Mac and Linux users. If you are a Windows user, skip to the next task.

13. At the top of the page, choose the Details dropdown menu, and then choose Show. A Credentials window opens.
14. Choose Download PEM, and save the labsuser.pem file.
15. Copy and paste the PublicIP into a text editor to use later. This IP address is the IPv4 server address that you have to connect to.
16. To exit the Details panel, choose the X.
17. Open a terminal window, and change the cd directory to the directory where you downloaded the labsuser.pem file. For example, run the following command if you saved the file to your Downloads directory:

```
cd ~/Downloads
```

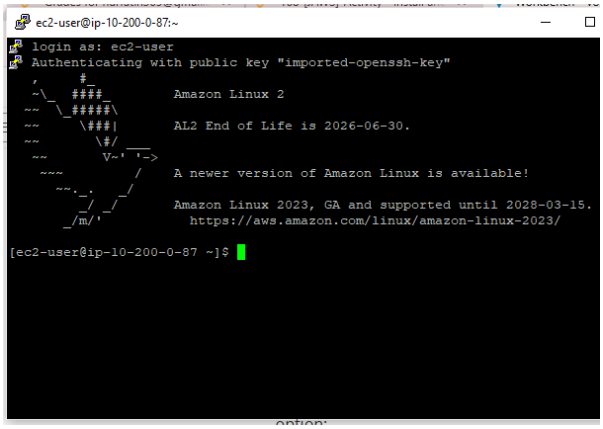
18. To change the permissions on the key to read only, run the following command:

```
chmod 400 labsuser.pem
```

19. In the following command, replace *<ip-address>* with the public IP address that you copied from the previous steps, and run the adjusted command:

```
ssh -i labsuser.pem ec2-user@<ip-address>
```

20. When prompted, enter yes to connect to this remote SSH server. Because you are using a key pair for authentication, you are not prompted for a password.

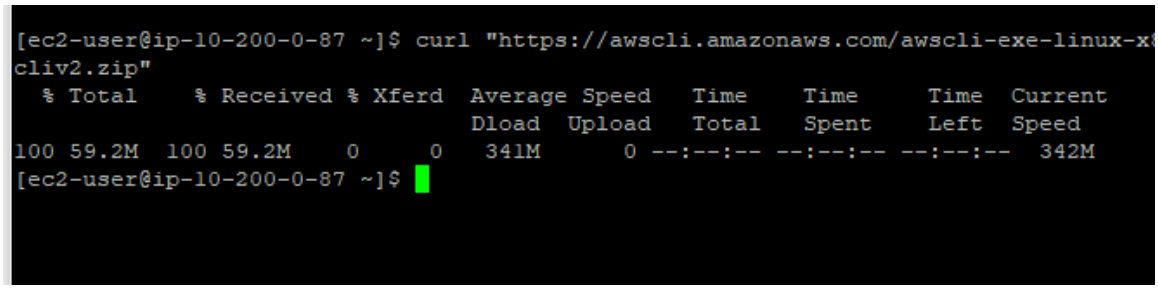


Task 2: Install the AWS CLI on a Red Hat Linux instance

In this task, you follow these steps from the terminal window to install the AWS CLI on a Red Hat Linux instance.

21. To write the downloaded file to the current directory, run the following curl command with the -o option:

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

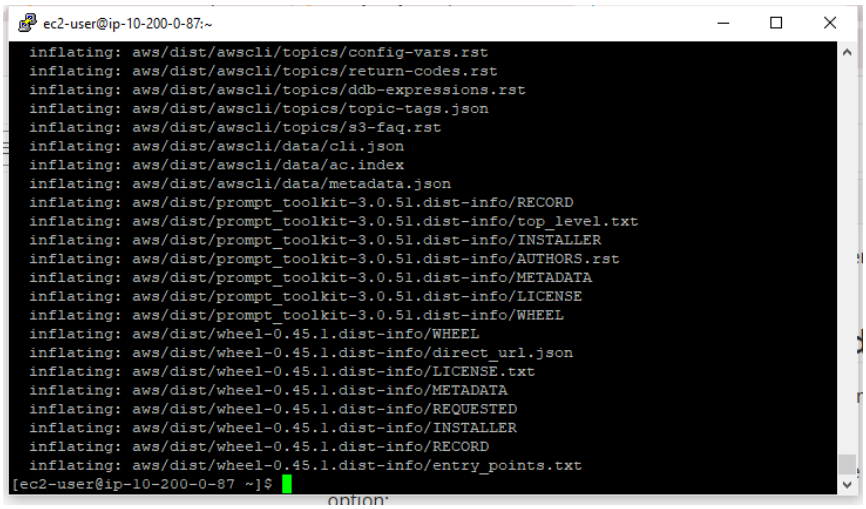


22. To unzip the installer, run the following unzip command with the -u option. In this command, the unzip command prompts you to overwrite any existing files. To skip these prompts, the command includes the -u option.

```
unzip -u awscliv2.zip
```

23. To run the install program, run the following command. This sudo command grants write permissions to the directory. The installation command in the code snippet uses a file named install in the unzipped aws directory to install the AWS CLI.

```
sudo ./aws/install
```



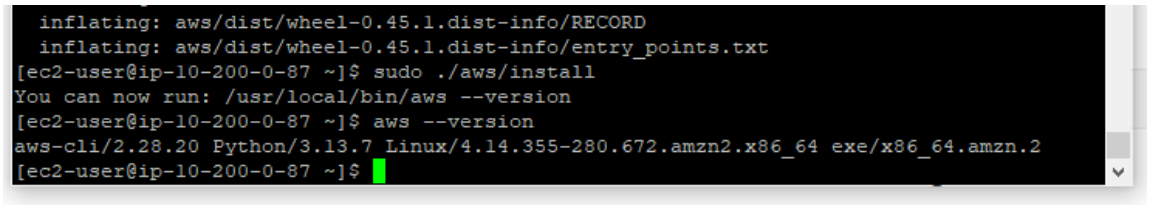
24. To confirm the installation, run the following command:

```
aws --version
```

The following is an example of the output:

```
aws-cli/2.7.24 Python/3.8.8 Linux/4.14.133-113.105.amzn2.x86_64 botocore/2.4.5
```

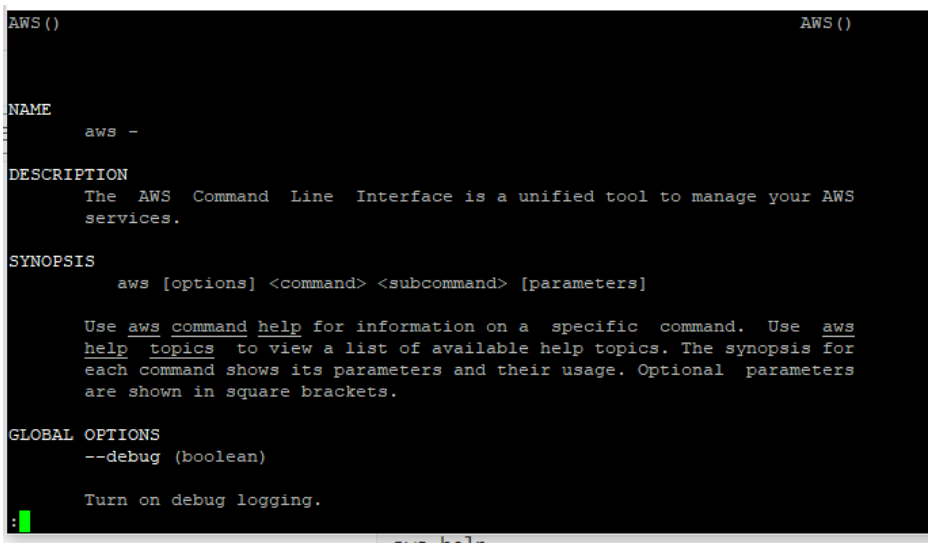
Note: The version numbers that are installed change overtime and might not reflect this example.



25. To verify that the AWS CLI is now working, run the following aws help command. The help command displays the information for the AWS CLI.

```
aws help
```

26. At the: prompt, enter `q` to exit.



Task 3: Observe IAM configuration details in the AWS Management Console

In this task, you observe the IAM configuration details for the EC2 instance in the AWS Management Console.

27. In the AWS Management Console, in the Search box, enter IAM and choose IAM. This option takes you to the IAM console page.

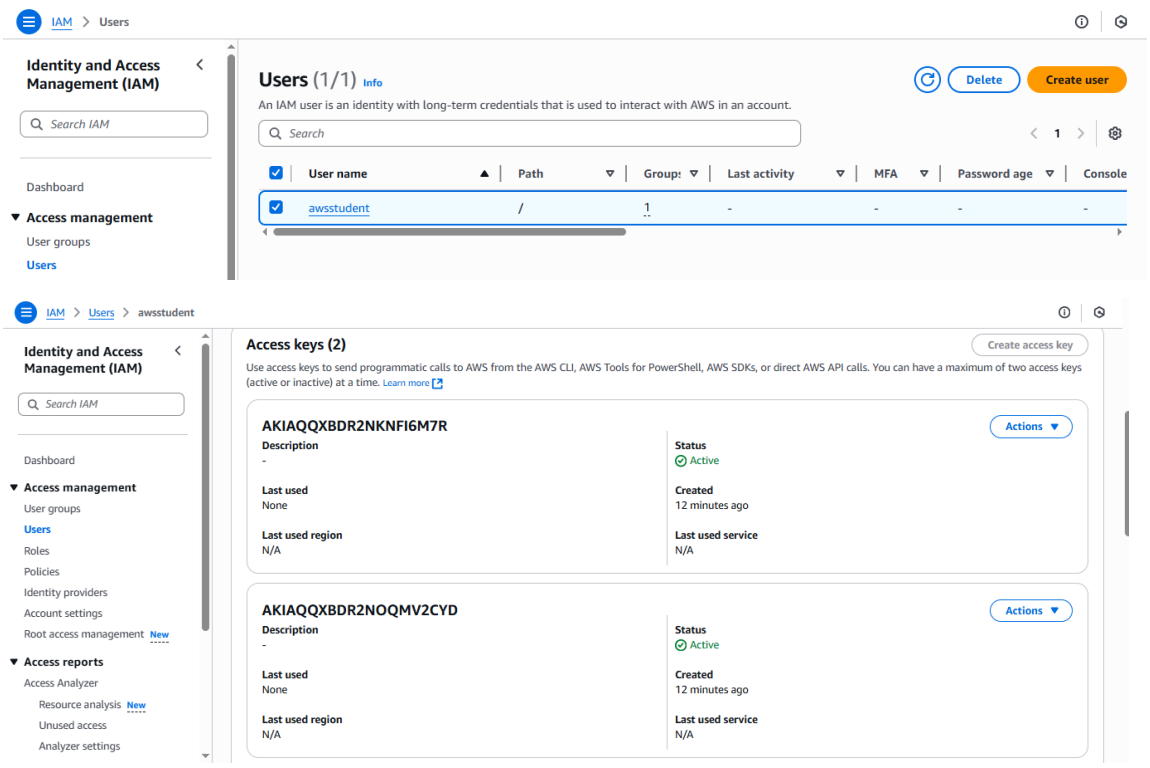
    Note: The IAM page that appears contains messages indicating that you do not have permission to observe some IAM service details. You can safely ignore these messages.

28. In the navigation pane, choose Users, and then choose awsstudent.
29. You are now in the Permissions tab. Next to lab_policy, choose the arrow icon, and then choose the {} JSON button.

    This lab_policy document is formatted in JSON. The IAM policy grants the awsstudent user access to specific AWS services in this account.

30. Choose the Security credentials tab. In the Access keys section, locate the awsstudent user's access key ID.

    Note: Once the access key is created, you must save the secret access key locally at the time that the key is created. For this lab, you can find the access key ID and the secret access key in the Details dropdown list at the top of these instructions.



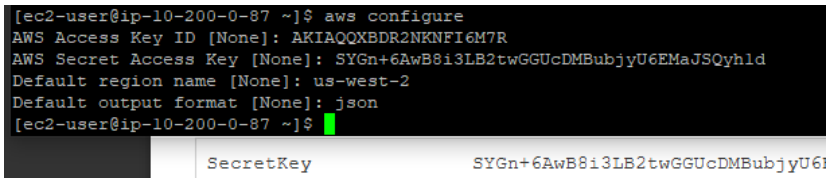
Task 4: Configure the AWS CLI to connect to your AWS Account

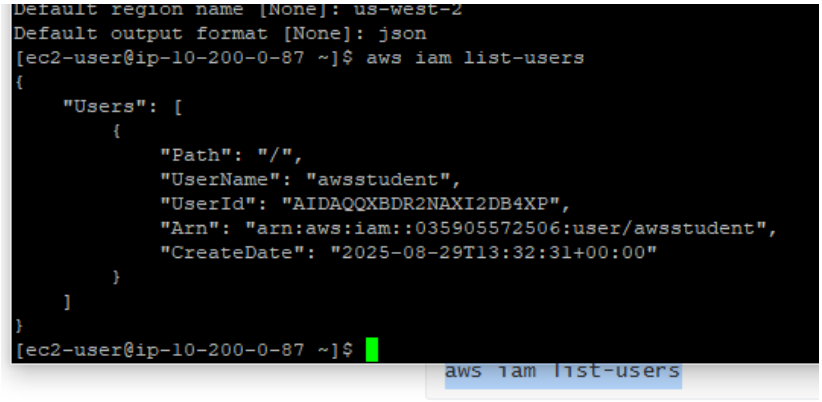
31. In the SSH session terminal window, run the configure command for the AWS CLI:

```
aws configure
```

32. At the prompt, configure the following:

- AWS Access Key ID: Choose the Details dropdown list, and choose Show. Copy and paste the AccessKey value into the terminal window.
- AWS Secret Access Key: Copy and paste the SecretKey value into the terminal window.
- Default region name: Enter `us-west-2`
- Default output format: Enter `json`





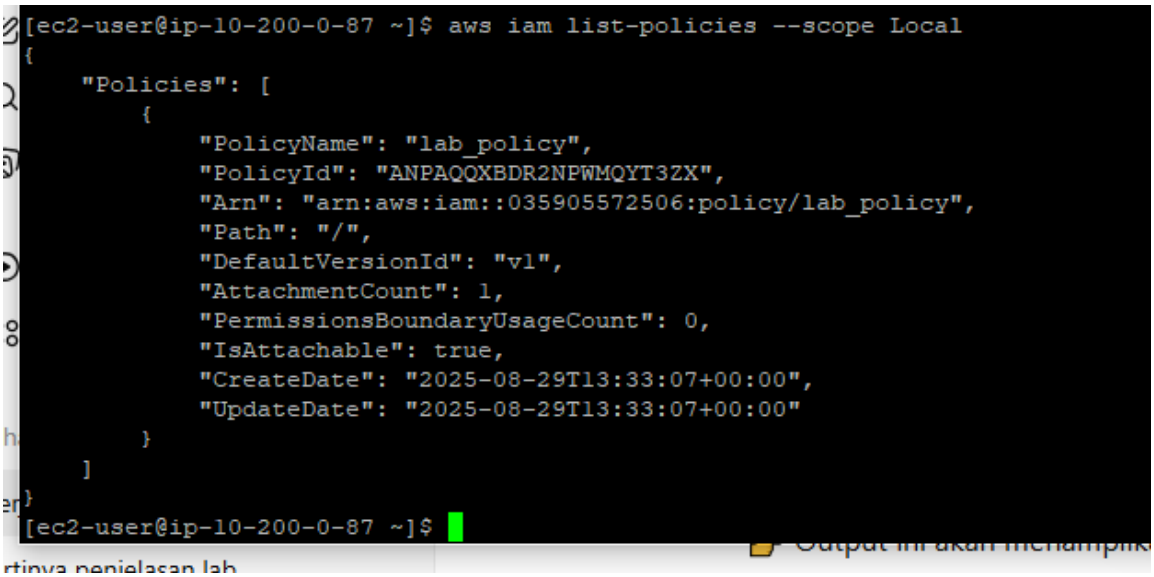
Task 5: Observe IAM configuration details by using the AWS CLI

In this task, you observe the IAM configuration details for the EC2 instance using the AWS CLI.

33. In the terminal window, test the IAM configuration by running the following command:

```
aws iam list-users
```

A successful test shows a JSON response that includes a list of IAM users in the account.



Activity 1 challenge

Use the AWS CLI Command Reference documentation and AWS CLI to download the lab_policy document in a JSON-formatted IAM policy document. This is the same document that is in the AWS Management Console.

Avoid the temptation to use the AWS Management Console.

Note: If permitted, work in a group to complete this challenge.

Activity summary

You successfully installed the AWS CLI on a Red Hat Linux instance and connected it to an AWS account. You used the AWS CLI to retrieve policy information by referencing AWS documentation.

Key takeaways:

- You can use the AWS CLI to manage and control multiple AWS services through the command line. You can also accomplish these tasks by using the AWS Management Console.
- To connect to the same AWS account, the AWS CLI needed an access key ID and secret access key. To sign in to the AWS Management Console, you need a user name and password.

Solution

Activity 1 challenge solution

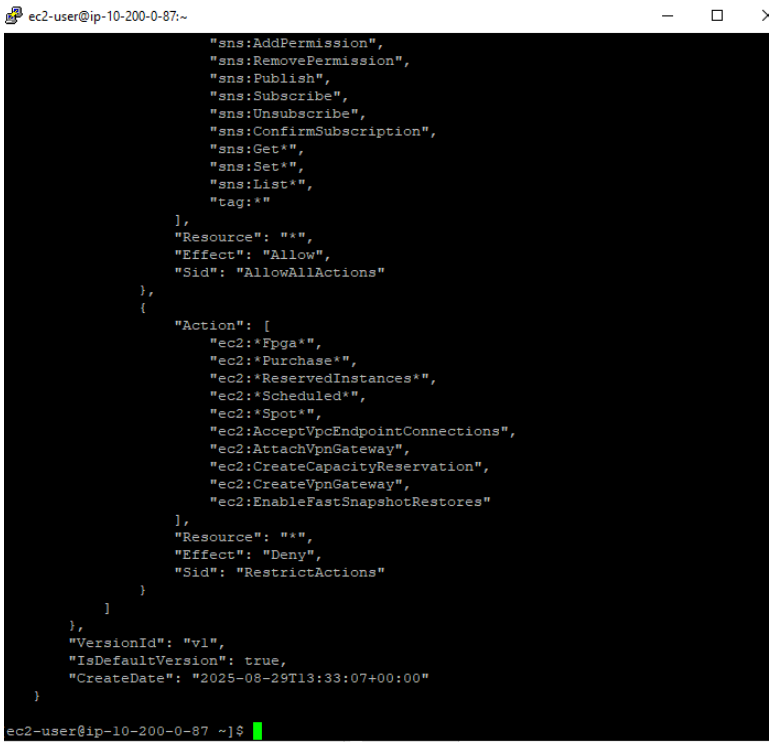
In the IAM AWS CLI Command Reference documentation page, the following command lists IAM policies and filters customer managed policies:

```plain
aws iam list-policies --scope Local
```

```
[ec2-user@ip-10-200-0-87 ~]$ aws iam list-policies --scope Local
{
    "Policies": [
        {
            "PolicyName": "lab_policy",
            "PolicyId": "ANPAQQXBDR2NPWMQYT3ZX",
            "Arn": "arn:aws:iam::035905572506:policy/lab_policy",
            "Path": "/",
            "DefaultVersionId": "v1",
            "AttachmentCount": 1,
            "PermissionsBoundaryUsageCount": 0,
            "IsAttachable": true,
            "CreateDate": "2025-08-29T13:33:07+00:00",
            "UpdateDate": "2025-08-29T13:33:07+00:00"
        }
    ]
}
```

Next, use the version number Arn information and DefaultVersionId found inside the lab_policy document to retrieve the JSON IAM policy. Use the > command to save the file.

```plain
 aws iam get-policy-version --policy-arn arn:aws:iam::038946776283:policy/lab_policy --version-id v1 > lab_policy.json
```




```
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": [
                        "cloudformation:List*",
                        "cloudformation:Describe*",
                        "cloudformation:Detect*",
```

```
                "cloudformation:EstimateTemplateCost",
                "cloudformation:Get*",
                "cloudwatch:*",
                "ec2:*Address*",
                "ec2:*associate*",
                "ec2:AttachVolume",
                "ec2:BundleInstance",
                "ec2:Cancel*",
                "ec2:*Capacity*",
                "ec2:CreateInstanceExportTask",
                "ec2:CreateFlowLogs",
                "ec2:*Credit*",
                "ec2:*Cidr",
                "ec2:Delete*",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:*Dhcp*",
                "ec2:*Ebs*",
                "ec2:*Event*",
                "ec2:*Fleet*",
                "ec2:*Format",
                "ec2:*Gateway*",
                "ec2:Get*",
                "ec2:*InstanceAttribute",
                "ec2:*InternetGateway",
                "ec2:*Image*",
                "ec2:*KeyPair",
                "ec2:*Kms*",
                "ec2:*monitor*",
                "ec2:*Network*",
                "ec2:*Options",
                "ec2:*PrefixList*",
                "ec2:ReportInstanceStatus",
                "ec2:RebootInstances",
                "ec2:ReplaceIamInstanceProfileAssociation",
                "ec2:*Route*",
                "ec2:*SecurityGroup*",
                "ec2:Search*",
                "ec2:SendDiagnosticInterrupt",
                "ec2:StopInstances",
                "ec2:*Snapshot*",
                "ec2:*Subnet*",
                "ec2:*Tag*",
                "ec2:TerminateInstances",
                "ec2:*Traffic*",
```

```
                    "ec2:*Vpn*",
                    "ec2:*Vpc*",
                    "events:*",
                    "iam:List*",
                    "iam:Get*",
                    "kms:List*",
                    "kms:Describe*",
                    "logs:*",
                    "resource-groups:Get*",
                    "resource-groups:List*",
                    "resource-groups:SearchResources",
                    "ssm:List*",
                    "ssm:Describe*",
                    "ssm:Get*",
                    "ssm:PutInventory",
                    "ssm:PutComplianceItems",
                    "ssm:PutConfigurePackageResult",
                    "ssm:UpdateAssociationStatus",
                    "ssm:UpdateInstanceAssociationStatus",
                    "ssm:UpdateInstanceInformation",
                    "ssm:CancelCommand",
                    "ssm:SendCommand",
                    "ssm:StartAutomationExecution",
                    "ssm:StartSession",
                    "ssm:TerminateSession",
                    "ssm:ResumeSession",
                    "ssm:DescribeSessions",
                    "ssm:GetConnectionStatus",
                    "sns:CreateTopic",
                    "sns:DeleteTopic",
                    "sns:AddPermission",
                    "sns:RemovePermission",
                    "sns:Publish",
                    "sns:Subscribe",
                    "sns:Unsubscribe",
                    "sns:ConfirmSubscription",
                    "sns:Get*",
                    "sns:Set*",
                    "sns:List*",
                    "tag:*"
                ],
                "Resource": "*",
                "Effect": "Allow",
                "Sid": "AllowAllActions"
            },
```

```
                {
                    "Action": [
                        "ec2:*Fpga*",
                        "ec2:*Purchase*",
                        "ec2:*ReservedInstances*",
                        "ec2:*Scheduled*",
                        "ec2:*Spot*",
                        "ec2:AcceptVpcEndpointConnections",
                        "ec2:AttachVpnGateway",
                        "ec2:CreateCapacityReservation",
                        "ec2:CreateVpnGateway",
                        "ec2:EnableFastSnapshotRestores"
                    ],
                    "Resource": "*",
                    "Effect": "Deny",
                    "Sid": "RestrictActions"
                }
            ]
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2025-08-29T13:33:07+00:00"
    }
}
```


Conclusion

Congratulations! You now have successfully done the following:

- Installed and configured the AWS CLI
- Connected the AWS CLI to an AWS account
- Accessed IAM by using the AWS CLI

Lab complete

34. At the top of this page, choose End Lab and then choose Yes to confirm that you want to end the lab.