Lab Information

AWS Console Information

BucketNameToDelete
labstack-9cc6e142-

Region
us-west-2

S3DeleteBucketPolicyARN
arn:aws:iam::7795(

Contents

aws training and certification

Lab 1 (Python) - Configure the Development Environment

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at *AWS Training and Certification* .

Duration

This lab will require around **45 minutes** to complete.

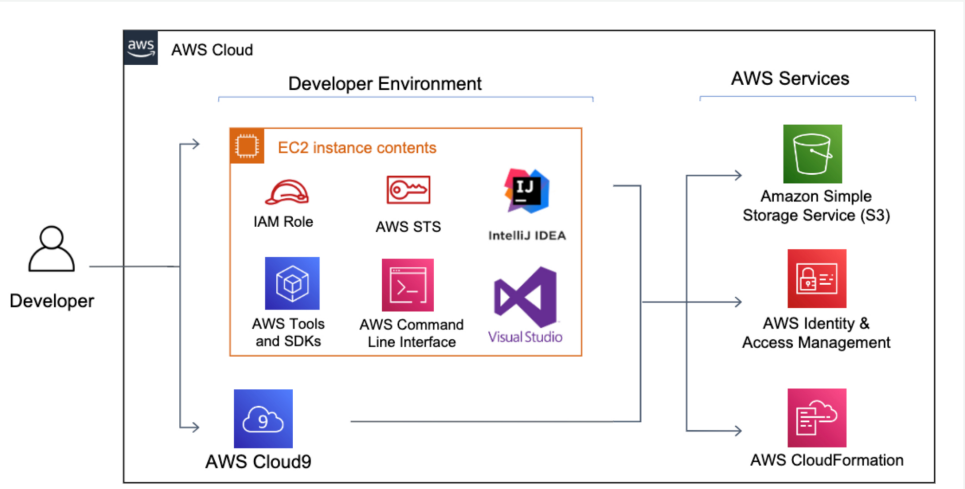
Prerequisites

This lab requires:

- Access to a Microsoft Windows or MacOS notebook computer with a Wi-Fi connection.
- An Internet browser such as Chrome, Firefox, or IE9+.
- **Note:** Previous versions of Internet Explorer are not supported.
- **Note:** You can use an iPad or tablet device to access these directions in the lab console.
- **Additional information:** Review additional lab environment specific details in the Appendix.

Overview

In this lab, you are going to connect to your sandbox environment that you will use to build out your end-to-end application for this course. You will verify that the appropriate development tools are installed and configured to access AWS services. You will review your specific IDE, learn how the AWS Toolkit works, and you will use AWS Identity and Access Management (IAM) to understand how permissions work.



OBJECTIVES

After completing this lab, you will be able to:

- Connect to a development environment.
- Verify IDE and the AWS CLI are installed and configured to use instance profile.
- Verify the necessary permissions have been granted to run AWS CLI commands.
- Assign an IAM policy to a role to delete an Amazon Simple Storage Service (Amazon S3) bucket.

Start lab

1. To launch the lab, at the top of the page, choose Start lab .

You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose Open Console .

You are automatically signed in to the AWS Management Console in a new web browser tab.

⚠ **Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

Error: You must first sign out

If you see the message, **You must first log out before logging into a different AWS account:**

- Choose the **click here** link.
- Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
- Choose **Open Console** again.

Error: Choosing Start Lab has no effect

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

- Add the lab domain name to your pop-up or script blocker's allow list or turn it off.
- Refresh the page and try again.

Task 0: Connect to your development environment

In this task, you will connect to your development environment.

3. From a browser tab opened to the **AWS Management Console** , use the **AWS search bar** to search for and choose **Cloud9** .

4. On the **Environments** page, next to the **Lab1** environment listing, choose **Open** .

Note: By default the AWS Cloud9 environment will open with a different theme. If you want to use a consistent theme for each lab, this is configured in the **Welcome** tab in the card with a title of **Configure AWS Cloud9** . You can choose a theme that is dark, gray, or light.

Note: When lab instructions in subsequent sections require you to issue commands, use the **AWS Cloud9 Terminal** .

Consider: This lab is designed for both experienced and newer developers:

- For more experienced developers who enjoy a challenge, there are **High-Level Instructions** before each task that should provide you enough information to help you complete the task.
- Once you complete the updates test your code to ensure it works, troubleshoot if needed, and then move on to the next task.
- For newer developers, there are **Detailed Instructions** to guide you through each step of the lab.

Task 1: Review the development environment

In this set of tasks, you will verify that the IDE and AWS CLI have been installed and configured. You will learn where the application code files, used in upcoming labs, will be stored. Next, you will disable the AWS managed temporary credentials set by default in AWS Cloud9.

High-Level Instructions:

- Verify that Python is installed.
- Verify that AWS CLI V2 is installed.
- Disable the AWS managed credentials in the AWS Cloud9 environment.
- Run `aws configure` to set the **region** value to the value, shown on the pane left of these instructions, and **output** to `yaml` .
- Verify that the `notes-application-role` is attached to the **AWS Cloud9** environment.

Detailed Instructions:

TASK 1.1: VERIFY INSTALLATION OF AN IDE

5. ⌨ **Command:** To verify which version of **Python** is installed run the following command:

```
python --version
```

Expected Output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

Python 3.7.10
```

Note: This indicates that **Python 3.7.10** is installed. Your version may be newer than the version listed.

TASK 1.2: VERIFY INSTALLATION OF THE AWS CLI

6. ⌨ **Command:** From the terminal, verify that the **AWS CLI** is installed by running the following command:

```
aws --version
```

Expected output:

```
*******************************
**** This is OUTPUT ONLY. ****
*******************************

aws-cli/2.7.4 Python/3.9.11 Linux/4.14.276-211.499.amzn2.x86_64 exe/x86_64.amzn.2 prompt/off
```

Note: The output indicates the version of the AWS CLI installed is **version 2** . Your version may be newer than the version listed.

TASK 1.3: DEACTIVATE THE AWS MANAGED TEMPORARY CREDENTIALS SETTING

In an AWS Cloud9, Amazon Elastic Compute Cloud (Amazon EC2) development environment, temporary AWS access credentials are made available to you. We call these AWS managed temporary credentials. You don't need to manually set up, manage, or attach an instance profile to the Amazon EC2 instance that connects to the environment.

- Learn more about AWS managed temporary credentials

Note: Although the AWS managed temporary credentials can be useful and time saving in many cases, sometimes you may find yourself in a situation where you need elevated credentials to complete a task. For example, in this lab we have attached an instance profile to the AWS Cloud9 Amazon EC2 instance as a security best-practice.

You will open the AWS Cloud9 environment and deactivate the AWS managed temporary credentials.

7. Choose the (gear icon) from the top-right to open the **AWS Cloud9 Preferences** > **AWS SETTINGS** > Untoggle **AWS managed temporary credentials** .

Note: The last step, which will enable you to query AWS services using temporary credentials, is to set the region in the `~/.aws/config` file.

8. Close the **Preferences** tab as you no longer need it open.

9. **Command:** Use the **AWS Cloud9 terminal** to run the `aws configure` command. You need to update the value for `REGION` , with the region value shown to the left of these instructions. And then set the output as `yaml` .

Note: In this example, the region set to **ap-northeast-1** but in your lab this region may be different.

```
aws configure
```

10. When prompted, verify the following:

- **AWS Access Key ID** [leave blank]: *Press ENTER*
- **AWS Secret Access Key** [leave blank]: *Press ENTER*
- **Default region name** [update to proper region]: `REGION`
- **Default output format** [update to yaml]: `yaml`

Example:

```
***********************************
**** This is an EXAMPLE ONLY. ****
***********************************

AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]: ap-northeast-1
Default output format [None]: yaml
```

11. **Command:** Using the AWS CLI Command Reference for AWS Security Token Service (AWS STS), choose the correct command to run to verify which credentials AWS Cloud9 is now using to authenticate requests for **TODO 1** :

- Choice A

```
aws sts get-caller-identity
```

- Choice B

```
aws sts decode-authorization-message
```

Expected output:

```
*******************************
**** This is OUTPUT ONLY. ****
*******************************

Account: '710606863198'
Arn: arn:aws:sts::710606863198:assumed-role/notes-application-role/i-047954185d0aa81f3
UserId: AROAZK43YHNPOOSPO53DF:i-047954185d0aa81f3
```

Answer: You can find the solution to this step in the TODO 1 Solution section at the bottom of these instructions.

Congratulations! You have successfully reviewed the development environment.

Task 2: Review the AWS Toolkit options

Now that AWS CLI is configured, verify that the **AWS Toolkit** is functional.

High-Level Instructions

- Open the **AWSToolkit** extension window.
- Verify the **profile** is set to use `ec2:instance` .
- Verify the **region** matches the value to the left of these instructions.
- Review the service resources in the **AWS Explorer**

- Review the service resources in the **AWS Explorer** .

Detailed Instructions

12. From the side menu, choose the aws (**AWS** icon) which represents a link to the **AWS Explorer** .
    - It should automatically connect because it will use the instance profile attached to the instance. This is represented using **ec2:instance** .
    - Make sure the **Region** matches the region value shown to the left of these instructions.
13. Using the **AWS Explorer** , you can view, create, update, and delete resources for various AWS services. You may want to review the services to familiarize yourself with the options available.

Congratulations! You have successfully reviewed the AWS Toolkit.

Task 3: Verify IAM Permissions

In this set of tasks, you will run a command to list the Amazon S3 buckets in this account, attempt to delete a bucket, and then run the `--debug` command to see where it fails.

High-Level Instructions:

- Run `aws s3` command to **view** all S3 buckets.
- Run `aws s3` command to **delete** an obsolete S3 bucket with `deleteme` in the name.
- Run `aws s3` command to **delete** an obsolete S3 bucket with `deleteme` in the name, and use the debug option.

Detailed Instructions:

TASK 3.1: RUN AWS CLI AMAZON S3 COMMAND TO VIEW BUCKETS

14. **Command:** From a command interface, run the following command to list the Amazon S3 buckets:

```
aws s3 ls
```

Similar output expected:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 17:58:33 6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000
2022-03-24 17:58:34 6nzxc1sjkmarkw5g4ugi-lab1bucket-1g9fvp2ico63h
```

Note: Buckets listed in this output are limited to those with the `lab1` in the name. Your list may include others not mentioned here. They will also have text before the **lab1** descriptor.

TASK 3.2: RUN AN AWS CLI AMAZON S3 COMMAND TO DELETE BUCKET

15. Run the following command to create a variable named **bucketToDelete** to use to specify the bucket name in future commands.

Note: This limits the bucket to only the bucket with **deleteme** in the name.

```
bucketToDelete=$(aws s3api list-buckets --output text --query 'Buckets[?contains(Name, `deletemebucket`) == `true`] | [0].Name')
```

Expected Output:

None, unless there is an error.

16. **Command:** Choose the correct command that will delete the bucket with `deleteme` in the name for **TODO 2** . Use the AWS CLI Command Reference for Amazon S3 as needed.

- Choice A

```
aws s3 remove-bucket s3://$bucketToDelete
```

- Choice B

```
aws s3 rb s3://$bucketToDelete
```

Expected output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

remove_bucket failed: s3://6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000 An error occurred (AccessDenied) when calling the DeleteBucket operation: Access Denied
```

Answer: You can find the solution to this step in the TODO 2 Solution section at the bottom of these instructions.

You encountered the error, **Access Denied** . It appears there is a permissions issue with running this command.

TASK 3.3: RUN AN AWS CLI AMAZON S3 COMMAND TO DELETE BUCKET USING --DEBUG

When you include the **–debug** option it includes details such as:

- Looking for credentials
- Parsing the provided parameters
- Constructing the request sent to AWS servers
- The contents of the request sent to AWS
- The contents of the raw response
- The formatted output

17. **Command:** From a command interface, run the following command to delete the bucket with `deleteme` in the name.

```
aws s3 rb s3://$bucketToDelete --debug
```

Note: The output can be rather lengthy, so the bulleted list below highlights the information in the output that will help you to understand the process and why the request was denied.

Expected output:

- Start of debug which breaks down the request into the individual arguments.

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 19:19:39,813 - MainThread - awscli.clidriver - DEBUG - Arguments entered to CLI: ['s3', 'rb', 's3://6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000', '-
```

- Now it begins the **authentication process** looking at the instance metadata. It finds the instance profile **notes-application-role** to use.

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 19:19:39,839 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: env
2022-03-24 19:19:39,839 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: assume-role
2022-03-24 19:19:39,839 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: assume-role-with-web-identity
2022-03-24 19:19:39,840 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: sso
2022-03-24 19:19:39,840 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: shared-credentials-file
2022-03-24 19:19:39,840 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: custom-process
2022-03-24 19:19:39,840 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: config-file
2022-03-24 19:19:39,841 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: ec2-credentials-file
2022-03-24 19:19:39,841 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: boto-config
2022-03-24 19:19:39,841 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: container-role
2022-03-24 19:19:39,841 - MainThread - botocore.credentials - DEBUG - Looking for credentials via: iam-role

2022-03-24 19:19:39,848 - MainThread - botocore.credentials - DEBUG - Found credentials from IAM Role: notes-application-role
```

- Next, it prepares the **Amazon S3 request** after verifying the **signature** using **v4 auth** , creates response headers, a response body, and returns the list of buckets.

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 19:19:39,893 - MainThread - botocore.auth - DEBUG - Calculating signature using v4 auth.
2022-03-24 19:19:39,893 - MainThread - botocore.auth - DEBUG - CanonicalRequest:
DELETE
/

host:6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000.s3.ap-northeast-1.amazonaws.com
x-amz-content-sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
x-amz-date:20220324T191939Z
x-amz-security-token:IQoJb3JpZ2luX2VjENr//////////wEaDmFwLW5vcnRoZWFzdC0xIkYwRAIgMQ6lF0VuNK96WM5KqACmFmMPSRJpe08nLvahhsIzmNsCIH6lB+/N/dHFnRUPS9AwrmwCBNZTY9iOOy0

host;x-amz-content-sha256;x-amz-date;x-amz-security-token
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
2022-03-24 19:19:39,893 - MainThread - botocore.auth - DEBUG - StringToSign:
AWS4-HMAC-SHA256
20220324T191939Z
20220324/ap-northeast-1/s3/aws4_request
```

- Finally, it connects to the **Amazon S3 endpoint** and encounters a **403 error** of **Access Denied** .

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 19:19:39,894 - MainThread - urllib3.connectionpool - DEBUG - Starting new HTTPS connection (1): 6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000.s3.ap-nc
2022-03-24 19:19:39,981 - MainThread - urllib3.connectionpool - DEBUG - https://6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000.s3.ap-northeast-1.amazonaws.com:443
2022-03-24 19:19:39,982 - MainThread - botocore.parsers - DEBUG - Response headers: {'x-amz-request-id': '7XBWQ3W8JM3KRY1W', 'x-amz-id-2': 'HcRkKJkSag//iCDC+ap7
2022-03-24 19:19:39,982 - MainThread - botocore.parsers - DEBUG - Response body:
b'<?xml version="1.0" encoding="UTF-8"?>\n<Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>7XBWQ3W8JM3KRY1W</RequestId><HostId>HcRkKJk

remove_bucket failed: s3://6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000 An error occurred (AccessDenied) when calling the DeleteBucket operation: Access Denied
```

This command failed because the **notes-application-role** does not have the `s3:DeleteBucket` IAM permission delegated to it.

Congratulations! You have successfully verified the IAM permissions.

Task 4: Add the missing permissions to your developer role

In this set of tasks, to address the permission issue you just encountered, you need to assign the appropriate permission to the **notes-application-role** . To save some time you will use a managed **IAM policy** that has already been created. First you will review the policy, which contains the `s3:DeleteBucket` permission, and then you will attach it to the `notes-application-role` . Then you will run the command to delete the bucket with `deleteme` in the name.

Note: In most organizations, control of granting, removing, and elevating IAM permissions is administered by a member of the security team. For learning purposes, we have enabled you the ability to add a customer managed policy with the **s3:DeleteBucket** permission and apply it to this specific role.

High-Level Instructions:

- Run `aws iam` command to review permissions for **version 1** of the `S3DeleteBucketPolicyARN` .
- Run `aws iam` command to attach the `S3-Delete-Bucket-Policy` to the `notes-application-role` .
- Run `aws s3` command to remove the obsolete bucket with `deleteme` in the name.

Detailed Instructions:

TASK 4.1: REVIEW A CUSTOMER MANAGED IAM POLICY

18. **Command:** Run the command below to assign the policy ARN value to the **$policyArn** variable which will be used in the next command.

```
policyArn=$(aws iam list-policies --output text --query 'Policies[?PolicyName == `S3-Delete-Bucket-Policy`].Arn')
```

Expected output:

None, unless there was an error.

19. **Command:** Run the command below to review the policy document for the `S3-Delete-Bucket-Policy` policy. This policy was created for you to grant delete bucket permissions for your role.

```
aws iam get-policy-version --policy-arn $policyArn --version-id v1
```

Expected output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

PolicyVersion:
  CreateDate: '2022-03-24T17:58:58+00:00'
  Document:
    Statement:
    - Action:
      - s3:DeleteBucket
      Effect: Allow
      Resource: arn:aws:s3:::6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000
    Version: '2012-10-17'
  IsDefaultVersion: true
  VersionId: v1
```

TASK 4.2: ATTACH THE IAM POLICY TO THE NOTES-APPLICATION-ROLE

20. **Command:** Attach the `S3-Delete-Bucket-Policy` policy to the `notes-application-role` role using the correct command for **TODO 3** , based on the AWS CLI Command Reference for IAM

Note: You will specify the **$policyArn** variable for the `policy-arn` value.

- Choice A

```
aws iam attach-role-policy --policy-arn $policyArn --role-name notes-application-role
```

- Choice B

```
aws iam attach-role-policy --policy-arn $policyArn --user-name notes-application-role
```

Expected output:

None, unless there is an error.

Answer: You can find the solution to this step in the TODO 3 Solution section at the bottom of these instructions.

TASK 4.3: REVIEW THE POLICIES ATTACHED TO THE ROLE

- **Command:** To verify the policy was added, run the following IAM command:

```
aws iam list-attached-role-policies --role-name notes-application-role
```

Expected output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

AttachedPolicies:
- PolicyArn: arn:aws:iam::710606863198:policy/S3-Delete-Bucket-Policy
  PolicyName: S3-Delete-Bucket-Policy
- PolicyArn: arn:aws:iam::aws:policy/ReadOnlyAccess
  PolicyName: ReadOnlyAccess
- PolicyArn: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
  PolicyName: AmazonSSMManagedInstanceCore
```

TASK 4.4: RUN THE BUCKET DELETE COMMAND AND VERIFY IT HAS BEEN DELETED

21. **Command:** Now that the **notes-application-role** has the permissions to delete the bucket with `deleteme` in the name, run the command below:

```
aws s3 rb s3://$bucketToDelete
```

Expected output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************
```

```
remove_bucket: 6nzxc1sjkmar-lab1deletemebucket-t63kd50lk000
```

22. **Command:** To verify the bucket has been removed using the **command interface** , type the command below:

```
aws s3 ls
```

Expected output:

```
******************************
**** This is OUTPUT ONLY. ****
******************************

2022-03-24 17:58:34 6nzxc1sjkmarkw5g4ugi-lab1bucket-1g9fvp2ico63h
```

Note: This output is limited to buckets names containing **lab1** only. You may see additional buckets in your output.

- You can verify the bucket has been deleted in the **Amazon S3** console as well.
- You can also verify the bucket has been deleted if you go to the **AWS Explorer** pane and refresh the **Amazon S3** menu.

Summary

Congratulations on completing the lab! For the **Python** version you can now:

- Connect to a development environment.
- Verify the IDE and the AWS CLI are installed and configured to use the instance profile.
- Verify the necessary permissions have been granted to run AWS CLI commands.
- Assign an IAM policy to a role to delete an Amazon S3 bucket.

End lab

Follow these steps to close the console and end your lab.

23. Return to the **AWS Management Console** .

24. At the upper-right corner of the page, choose **AWSLabsUser** , and then choose **Sign out** .

25. Choose End lab and then confirm that you want to end your lab.

For more information about AWS Training and Certification, see *https://aws.amazon.com/training/* .

Your feedback is welcome and appreciated.
If you would like to share any feedback, suggestions, or corrections, please provide the details in our *AWS Training and Certification Contact Form* .

Additional Resources

- Learn more about AWS managed temporary credentials
- AWS CLI Command Reference for AWS Security Token Service (AWS STS)
- AWS CLI Command Reference for Amazon S3
- AWS CLI Command Reference for IAM

Code Challenge Solutions

TODO 1 SOLUTION

- **Choice A is the correct answer.**

```
aws sts get-caller-identity
```

- Choice B is incorrect because it calls the decode-authorization-message command.

Return to the instructions

TODO 2 SOLUTION

- Choice A is incorrect because `remove-bucket` is not an available object operation.
- **Choice B is the correct code snippet.**

```
aws s3 rb s3://$bucketToDelete
```

Return to the instructions

TODO 3 SOLUTION

- **Choice A is the correct code snippet.**

```
aws iam attach-role-policy --policy-arn $policyArn --role-name notes-application-role
```

```
aws iam detach-role-policy --policy-arn $policyARN --role-name notes-application-role
```

- Choice B is incorrect because **–user-name** is not an available option.

Return to the instructions

Appendix

AWS SERVICES NOT USED IN THIS LAB

AWS services that are not used in this lab are deactivated in the lab environment. In addition, the capabilities of the services used in this lab are limited to what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. While not all of the icons will be used, the following list explains the purpose for each icon:

- **Command:** A command that you must run.
- **Expected output:** A sample output that you can use to verify the output of a command or edited file.
- **Note:** A note, tip, or important guidance.
- **Additional information:** Where to find more information.
- **Caution:** Information of special interest or importance (not so important to cause problems with the equipment or data if you miss it, but it could result in the need to repeat certain steps).
- **WARNING:** An action that is irreversible and could potentially impact the failure of a command or process (including warnings about configurations that cannot be changed after they are made).
- **Consider:** A moment to pause to consider how you might apply a concept in your own environment or to initiate a conversation about the topic at hand.
- **Copy/Paste:** A code block that displays the contents of a script or file you need to copy and paste that has been pre-created for you. When you need to copy only a certain part of a code block, there will be numbered **TODO** comments in the code.
- **Knowledge check:** An opportunity to check your knowledge and test what you have learned.
- **Security:** An opportunity to incorporate security best practices.
- **Refresh:** A time when you might need to refresh a web browser page or list to show new information.
- **Copy command:** A time when copying a command, script, or other text to a text editor (to edit specific variables within it) might be easier than editing directly in the command line or terminal.
- **Hint:** A hint to a question or challenge.
- **Answer:** An answer to a question or challenge.
- **Group effort:** A time when you must work together with another student to complete a task.

Return to the instructions