**Module 10 - Challenge Lab: Automating Infrastructure Deployment**

**Scenario**

Up to this point, the café staff created their AWS resources and configured their applications manually—mostly by using the AWS Management Console. This approach worked well as a way for the café to get started with a web presence quickly. However, they find it challenging to replicate their deployments to new AWS Regions so that they can support new café locations in multiple countries. They would also like to have separate development and production environments that reliably have matching configurations.

In this challenge lab, you will take on the role of Sofía as you work to automate the café's deployments and replicate them to another AWS Region.

**Lab overview and objectives**

In this lab, you will gain experience with creating AWS CloudFormation templates. You will use the templates to create and update AWS CloudFormation stacks. The stacks create and manage updates to resources in multiple AWS service areas in your AWS account. You will practice using AWS CodeCommit to control the version of your templates. You will also observe how you can use AWS CodePipeline to automate stack updates.

After completing this lab, you should be able to:

* Deploy a virtual private cloud (VPC) networking layer by using an AWS CloudFormation template
* Deploy an application layer by using an AWS CloudFormation template
* Use Git to invoke AWS CodePipeline, and to create or update stacks from templates that are stored in AWS CodeCommit
* Duplicate network and application resources to another AWS Region by using AWS CloudFormation

When you *start* the lab, the following resources are already created for you in the AWS account:

Note that in this challenge lab, you will encounter a few tasks where step-by-step instructions are not provided. You must figure out how to complete the tasks on your own.

**Duration**

This lab will require approximately **90 minutes** to complete.

**AWS service restrictions**

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

**Accessing the AWS Management Console**

1. At the top of these instructions, choose Start Lab to launch your lab.

A **Start Lab** panel opens, and it displays the lab status.

**Tip**: If you ever need more time to complete the lab that is displayed on the timer, choose the Start Lab button again to restart the timer for the environment. Doing so will not delete resources you have created.

1. Wait until you see the message *Lab status: ready*, then close the **Start Lab** panel by choosing the **X**.
2. At the top of these instructions, choose AWS.

This opens the AWS Management Console in a new browser tab. The system will automatically log you in.

**Tip**: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose **Allow pop-ups**.

1. Arrange the AWS Management Console tab so that it displays alongside these instructions. Ideally, you will have both browser tabs open at the same time so that you can follow the lab steps more easily.

**Note**: To hide the terminal window, you can also clear the **Terminal** box at the top of the screen.

**A business request: Creating a static website for the café by using AWS CloudFormation (Challenge #1)**

The café would like to start using AWS CloudFormation to create and maintain resources in the AWS account. As a simple first attempt at this process, you will take on the role of Sofía and create a simple AWS CloudFormation template that can be used to create an Amazon Simple Storage Service (Amazon S3) bucket. Then, you will add more detail to the template so that when you update the stack, it configures the bucket to host a static website for the café.

**Task 1: Creating an AWS CloudFormation template from scratch**

In this first task, you will create an AWS CloudFormation template that creates an S3 bucket. You will then run an AWS Command Line Interface (AWS CLI) command that created the AWS CloudFormation stack. (The stack is the resource that creates the bucket.)

1. Navigate to the AWS Cloud9 service and open the integrated development environment (IDE) of the existing AWS Cloud9 instance.

1. In the AWS Cloud9 IDE, choose **File > New File**, then choose **File > Save**, and save the new file as: S3.yaml

1. At the top of the file, add the following two lines:

AWSTemplateFormatVersion: "2010-09-09"

Description:

1. Next, add the following three lines to your template:

Resources:

S3Bucket:

  Type: AWS::S3::Bucket

**Tip**: Make sure that you keep the correct number of spaces for each indentation level. The Resources: line should have no indentation. The S3Bucket: line should be indented by 2 spaces. Finally, the Type: AWS::S3::Bucket line should be indented by 4 spaces.

AWS CloudFormation supports the YAML Version 1.1 specification, with a few exceptions. For more information about YAML, go to [the YAML website](http://www.yaml.org/).

1. Add a description (such as "cafe S3 template") on the **Description:** line. Before you start your description, be sure that you have a space *after* the colon (:). After you enter the description, **Save** the changes to file.

In the guided lab earlier in this module, you used the AWS Management Console to create an AWS CloudFormation stack. Here, you use the AWS CLI instead.

1. In the Bash terminal, run these two lines of code:

aws configure get region

aws cloudformation create-stack --stack-name CreateBucket --template-body file://S3.yaml

The first line of code that you ran returned the default AWS Region of the AWS CLI client that is installed on the AWS Cloud9 instance. You could modify the default AWS Region by running aws configure. However, for this lab, you should leave the default Region.

The second line of code that you ran created a stack that used the template you defined. Because you did not specify the Region in the command, the stack will be created in the default Region.

If the create-stack command ran successfully, you should see some output that is formatted in JavaScript Object Notation (JSON). This output should indicate a *StackId*.

This diagram illustrates the actions you just completed.

1. In the AWS Management Console, navigate to the AWS CloudFormation service and observe the details of the *CreateBucket* stack.

For example, look at the information in the **Events**, **Resources**, **Outputs**, and **Template** tabs.

1. Navigate to the Amazon S3 service page to observe the bucket that your template created.

**Tip**: The bucket has the bucket name *createbucket-s3bucket-<random-string>*.

**Answering questions about the AWS CloudFormation stack**

The answers will be recorded when you choose the blue **Submit** button at the end of the lab.

1. Access the questions in this lab.
   * Choose the Details  menu, and choose Show.
   * At the bottom of the page, choose the **Access the multiple choice questions** link.

1. In the page that you loaded, submit answers for each of the following questions:
   * **Question 1:** Was an S3 bucket created, even if you did not specify a name for the bucket? If so, what name was it given?
   * **Question 2:** What Region was the bucket created in, and why was it created in this Region?
   * **Question 3:** To define an S3 bucket, how many lines of code did you need to enter in the Resources: section of the template file?

**Note:** Leave the browser tab with the questions in it open, so that you can return to it later in the lab.

**Task 2: Configuring the bucket as a website and updating the stack**

In this next task, you will update the AWS CloudFormation template. The update will configure the S3 bucket to host a static website. This task is similar to the results from the Module 3 challenge lab. In that challenge lab, you created and configured the S3 bucket manually by using the AWS Management Console. However, in this lab, you will instead configure the bucket by using an AWS CloudFormation template.

1. Upload static website assets to the bucket.

To do this task, run the following commands in the Bash terminal (replace <*bucket-name*> with your actual bucket name):

wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod10-challenge/static-website.zip

unzip static-website.zip -d static

cd static

aws s3 cp --recursive . s3://<bucket-name>/ --acl public-read

If these operations are successful, you should see numerous *upload:<file\_name>* messages in the command output.

1. In a new browser tab, open the AWS CloudFormation template documentation for defining S3 bucket resources.
   * Go to the [AWS resource and property types reference](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-template-resource-type-ref.html) documentation
   * Scroll down, choose **Amazon S3**, and then choose the **AWS::S3::Bucket** resource type.

1. Using the documentation as a reference, modify your S3.yaml template to set the following characteristics on the S3 bucket resource:
   * Attach a *deletion policy* that will retain the bucket
   * Configure the bucket to host a static website with *index.html* set as the index document

**Tip**: You can accomplish this task by adding two additional lines of code to your template. See the code in the *Examples* section of the documentation page that you opened in the last step.

1. To your AWS CloudFormation template, add an *output* that provides the website URL.

Again, consult the **Examples** section of the documentation as a reference.

1. Save the changes to your S3.yaml file.

1. Validate your template.

Back in the Bash terminal, change the directory back to the location of the S3.yaml file and validate your template by running the following commands.

cd ../

aws cloudformation validate-template --template-body file://S3.yaml

If the output indicates that your template has syntax or other errors, correct them, and then run the command again to verify that they have been resolved.

1. Update the stack by running this command:

aws cloudformation update-stack --stack-name CreateBucket --template-body file://S3.yaml

**Tip**: Proper YAML syntax is important. If you receive a *ValidationError* when you run update-stack, review your use of colons and confirm that you indented each line appropriately. The example templates in the documentation provide a good reference for well-structured YAML templates.

1. Browse to the AWS CloudFormation service and confirm that your stack update completed successfully.
   * The stack should show status *UPDATE\_COMPLETE*.
   * If the stack does not attain a status of *UPDATE\_COMPLETE*, try these troubleshooting tips.
     + If you see that the stack has a *ROLLBACK* status of some kind, go the **Events** tab and search for an *UPDATE\_FAILED* entry. (Read the *Status* reason for that event to understand why the stack update failed.)
     + After you think that you resolved any errors, run the update-stack command again. In the console, return to the AWS CloudFormation stack and go to the **Events** tab to confirm whether you successfully updated the stack.
     + Repeat as necessary.

1. Verify success.
   * Does the stack's **Outputs** tab list an output with a URL value? If so, choose the link.
   * Does the static website open? (You previously copied the website assets into the bucket.)

If so, congratulations!

**Note:** If the stack does not have any output—or if the output hyperlink does not display the contents of the café website—you can try these troubleshooting steps.

* + - Browse to the Amazon S3 console and choose your bucket. The **Overview** tab should list the index.html file and two folders that are named *css* and *images*. If these resources are not listed, you might want to revisit the first step in this challenge section.
    - Choose the **index.html** file and then choose **Permissions**. Under **Public access**, the value for **Read object** should be *Yes*.
    - Return to the bucket view. In the **Properties** tab, confirm that **Static website hosting** is enabled, with a **Hosting type** of *Bucket hosting*.
    - All of the permissions and properties that are described in this list should be set in your S3.yaml template. If necessary, adjust the details in the template and run the update-stack AWS CLI command again.

**Note:** In this first challenge, you manually copied the website files into the bucket. You can also perform this action by using a custom resource from AWS CloudFormation, combined with an AWS Lambda function. Both of these resources can be defined in an AWS CloudFormation template. This approach is a more advanced use of AWS CloudFormation beyond the scope of this lab. However, if you are interested in this topic, refer to the [AWS Lambda-backed custom resources](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-custom-resources-lambda.html) page in the AWS Documentation.

**New business requirement: Storing templates in a version control system (Challenge #2)**

The café team was impressed that Sofía configured an entire static website by using an AWS CloudFormation template. Given this success, the team decided that they would like to expand their use of infrastructure as code (IaC) to build out other application resources in the AWS account.

The team understands that it is a best practice to store IaC templates in a version control system, so they asked Sofía to take on this challenge. Sofía spoke with Mateo about this new business requirement when he stopped by the café. He mentioned that AWS CodeCommit would be a good choice for storing templates and managing version control for them. Mateo created a CodeCommit repository with some sample AWS CloudFormation templates in it. Sofía is eager to start using this code repository.

**Task 3: Cloning a CodeCommit repository that contains AWS CloudFormation templates**

In this task, you will work as Sofía to clone a CodeCommit repository. The café team will use the repository to store and control the versions of the AWS CloudFormation templates.

1. Browse to the CodeCommit service and in your account, notice the repository that is named *CFTemplatesRepo*.

CodeCommit is a source control service that can be used to host Git-based repositories. It can be used in a way that's similar to GitHub repositories. For details about AWS CodeCommit, see the [AWS Documentation](https://aws.amazon.com/codecommit/).

1. Choose **CFTemplatesRepo** and then choose the **templates** folder.

Notice that it has AWS CloudFormation templates in it.

In this part of the lab, you will store your IaC AWS CloudFormation templates in CodeCommit.

1. Open the *CFTemplatesRepo/templates/****start-lab.yaml*** file and analyze the contents.
   * Notice that this template defines a few of the resources that you observed in this AWS account.
   * For example:
     + Starting on line 6, the template defines an *AWS Cloud9 instance*
     + Starting on line 12, the template defines the *CodeCommit repository* that you now have open

The lab platform that hosts this lab created an AWS CloudFormation stack when you chose **Start Lab**. The AWS CloudFormation template that it ran includes the resource definitions that are contained in this template. However, this example template does not contain all the resource definitions that are in the *actual* template that was used to start this lab.

1. In the breadcrumbs at the top of the page, choose **Repositories** and in the **Clone URL** column, choose **HTTPS**.

This action copies the CodeCommit repository's HTTPS clone URL to your clipboard.

1. Return to the AWS Cloud9 IDE and clone the existing CodeCommit repository to your workspace (replace <*url*> with the clone URL that you copied)

In the Bash terminal in the AWS Cloud9 IDE, enter this command:

git clone <url>

This command clones a copy of the CodeCommit repository that you just observed. The command creates a *CFTemplatesRepo* directory that should now appear in the navigation pane (which is the left pane in the IDE).

Use the Git client software to analyze your local copy of the repository.

cd CFTemplatesRepo

git status

The git status command shows what branch of the repository you are connected to. It also shows that your local copy is up to date with the source branch in CodeCommit.

**New business requirement: Using a continuous delivery service, create the network and application layers for the café (Challenge #3)**

The next challenge is for Sofía to use AWS CloudFormation to create all the network resources that the dynamic website café application can be deployed to. Then, she must deploy the café application itself.

Also, Sofía would like to find an easier way to update stacks when she updates an AWS CloudFormation template. She is now updating templates regularly, and she thinks that she should be able to automate stack updates.

Sofía spoke with Mateo about this issue. He mentioned that AWS CodePipeline provides the continuous integration and continuous delivery (CI/CD) service capabilities that she is looking for. Mateo then created two pipelines for Sofía, and she is eager to start working with them.

In this challenge, you will work as Sofía and make use of these pipelines. You will also define—in AWS CloudFormation templates—all the resources that are needed to deploy the dynamic café website.

**Task 4: Creating a new network layer with AWS CloudFormation, CodeCommit, and CodePipeline**

In this task, you will use an AWS CloudFormation template to create a VPC with a public subnet, along with other network resources. You will gain experience with using a CI/CD pipeline. When you use Git to push the template into a CodeCommit repository, it will trigger a pipeline that will create an AWS CloudFormation stack.

1. Create a new AWS CloudFormation template that will create a VPC, public subnet, and other resources.
   * In the navigation pane of the AWS Cloud9 IDE, expand the **CFTemplatesRepo/templates** directory.
   * In the **templates** directory, right-click template1.yaml and create a duplicate of it.
   * Rename the duplicate to: cafe-network.yaml
   * In the text editor, open cafe-network.yaml and set the description to: Network layer for the cafe
   * Observe the details of the seven resources that this template creates.

1. Observe the AWS CodePipeline details that were preconfigured in your account.
   * In the AWS Management Console, from the **Services** menu, choose **CodePipeline**.
   * Choose **Pipelines**.
   * Notice that two pipelines have been predefined for you:
     + CafeAppPipeline
     + CafeNetworkPipeline

**Important**: The status of the most recent attempt to run each pipeline will show that they failed. However, this status is expected. The AWS CloudFormation template files that the pipelines reference do not exist in their expected location.

1. Analyze the *Source* stage of the CafeNetworkPipeline.
   * Choose **CafeNetworkPipeline** and observe the pipeline details.

In the **Source** area, you can see that this pipeline's **SourceAction** is *AWS CodeCommit*.

* + To the right of the **SourceAction** heading, choose

The details in the **Configuration** window show that the source is the *CFTemplatesRepo* CodeCommit repository.

* + To return to the **CafeNetworkPipeline** page, choose **Done**.

1. Analyze the *Deploy* stage of the CafeNetworkPipeline.
   * Notice that the *Deploy* action will be performed by using AWS CloudFormation.
   * To the right of the **RunChangeSet** heading, choose

**Analysis**: The details in the **Configuration** window show that a stack named *update-cafe-network* will be run or be updated. To perform these actions, the stack will use the cafe-network.yaml AWS CloudFormation template. This *Deploy* action receives the template from the *Source* stage, which found the template in the CodeCommit repository.

The following diagram illustrates how you will trigger this pipeline and what the pipeline will do. It also shows some of the AWS account resources that the resulting AWS CloudFormation stack will create or update.

1. For more details about AWS CodePipeline, refer to the [AWS Documentation](https://aws.amazon.com/codepipeline/).

1. Return to the AWS Cloud9 instance and trigger the creation of the *update-cafe-network* by checking your AWS CloudFormation template into CodeCommit.
   * Observe how the local copy of the repository differs from the origin. In the Bash terminal, run the following command:

git status

The output should show that the cafe-network.yaml file that you created is currently untracked in Git.

* + Run these two commands to add the new file to the repository and then commit it to the repository with a comment.

git add templates/cafe-network.yaml

git commit -m 'initial commit of network template' templates/cafe-network.yaml

* + Check the status of your local copy of the repository:

git status

The information that is returned should report that your branch is ahead of the origin by one commit.

* + Finally, push the commit to the remote repository (this command actually copies the file to CodeCommit):

git push

1. Return to the CodePipeline console and choose the **CafeNetworkPipeline**.
   * Observe that the creation of the stack is automatically triggered.

**Note:** It might take a minute or two for the *Source* stage to update and for the *Deploy* stage to show that it is *In progress*. Eventually, the *Deploy* stage status should show *Succeeded*.

* + Notice that the details for both *Source* and *Deploy* show the commit number that was returned when you ran git push. The details also show the comment that you added to the commit.

Troubleshooting tips:

* If the *Deploy* step has a status of *Failed - Just now*, access the error details by opening the **Details** link. For example, you could have a template-formatting error that must be resolved.
* After you update the template, you can update the stack by running the appropriate git commit and git push commands again.
  + The **Release change** button can also trigger the pipeline to run again. It will do so even if you do not make changes to the CodeCommit repository (such as by issuing a git push command).
  + Similarly, you can use the **Retry** button in the *Deploy* stage of the pipeline. It will retry the *Deploy* stage without retrying the *Source* stage.
* If the stack fails to roll back—and prevents you from performing additional updates to the stack—you can delete the stack. To do so, go to the stacks page in the AWS CloudFormation console and delete the stack. If you delete the network stack, push a new update to Git. This action will trigger the re-creation of the stack.

1. In the AWS CloudFormation console, confirm that the *update-cafe-network* stack ran. It should have a status *CREATE\_COMPLETE* or *UPDATE\_COMPLETE*.

Also, check the **Outputs** tab for the stack. It currently shows no outputs. Soon, however, you will update the stack so that it creates outputs.

1. In the Amazon VPC console, observe that the resources defined in the cafe-network.yaml template were created in the AWS account.

For example, the console should list a VPC named *Cafe VPC*, and a subnet named *Cafe Public Subnet*.

Congratulations! You have successfully created the network resources that are needed to run the café website.

**Task 5: Updating the network stack**

In this task, you update the network stack so that it exports essential information about two of the resources that it creates. These two outputs can then be referenced by the application stack that you create later.

1. Add the following lines to the bottom of *cafe-network.yaml*.

Outputs:

PublicSubnet:

  Description: The subnet ID to use for public web servers

  Value:

    Ref: PublicSubnet

  Export:

    Name:

      'Fn::Sub': '${AWS::StackName}-SubnetID'

VpcId:

  Description: The VPC ID

  Value:

    Ref: VPC

  Export:

    Name:

      'Fn::Sub': '${AWS::StackName}-VpcID'

1. Save the change and in the Bash terminal, add and commit the code, and then push it to CodeCommit by using Git.

1. Verify that the AWS CloudFormation stack update occurs. Also verify that the **Outputs** tab now lists two keys with export names.

| **Name** | **Export Name** |
| --- | --- |
| *PublicSubnet* | *update-cafe-network-SubnetID* |
| *VpcId* | *update-cafe-network-VpcID* |

**Task 6: Defining an EC2 instance resource and creating the application stack**

In this task, you will create a new AWS CloudFormation template that will be used to create a stack. The new stack deploys a dynamic website for the café. The *CafeAppPipeline* pipeline (which you observed earlier) creates or updates the *update-cafe-app* stack when you push the cafe-app.yaml template to the CodeCommit repository.

1. Back in AWS Cloud9, duplicate the **template2.yaml** file in the templates directory and rename the duplicate as cafe-app.yaml.

1. In the cafe-app.yaml template, analyze the existing template contents:
   * In the **Parameters** area, the **LatestAmiId** performs a lookup. It finds the latest Amazon Linux 2 Amazon Machine Image (AMI) ID in the AWS Region where you create the stack. It can be referenced when you define an Amazon Elastic Compute Cloud (Amazon EC2) instance.
   * Also in the **Parameters** area, the **CafeNetworkParameter** defines a string value. The value defaults to the name of the stack that you created when you ran the cafe-network.yaml AWS CloudFormation template. Setting this string as a parameter provides you with the flexibility to point to a different stack name if you must reference resources in another stack.
   * In the **Mappings** area, the **RegionMap** mapping can be referenced when you define an EC2 instance. Using this mapping can help ensure that the correct key pair will be used for the instance. However, use of this feature depends on the AWS Region where you run the template.
   * In the **Resources** area, an **EC2 security group** is defined. It opens TCP ports 80 and 22 for inbound network traffic. It is created in the VPC that the *update-cafe-network* stack created.
   * In the **Outputs** area, an output named **WebServerPublicIP** returns the public IPv4 address of the EC2 instance that you will define next.

1. In the cafe-app.yaml template, define a third *parameter* so that a user can choose between different instance types when they launch an EC2 instance.
   * Browse to the [AWS Documentation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html). Under the *Defining a parameter in a template* section, copy the example YAML parameter.
   * Paste the parameter into your template. Then, modify the parameter so that the permitted instance types are *t2.micro*, *t2.small*, *t3.micro*, and *t3.small*. Also, set the default to t2.small and update the description so that it reflects the options that a user can choose.

1. In a new browser tab, open the [AWS Documentation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-instance.html) and use the information in that page as a reference.

1. Back in the cafe-app.yaml template, create a new *EC2 instance* resource that has the following characteristics:
   * Set the **Logical ID** to CafeInstance (see <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resources-section-structure.html> for reference, if needed)
   * Include an **ImageId** that references the *LatestAmiId* parameter
   * For **instance type**, reference the instance type parameter that you defined in the previous step.
   * For **KeyName**, use the following line of code, which references the RegionMap mapping that is already defined in the template:

KeyName: !FindInMap [RegionMap, !Ref "AWS::Region", keypair]

* + For the **instance profile** (the AWS Identity and Access Management, or IAM, role that is attached to the instance), specify CafeRole

**Note**: The CafeRole IAM role already exists in your account. Attaching it grants your EC2 instance the permissions to retrieve Parameter Store values from AWS Systems Manager.

* + In the **Properties** section, include the following lines of code:

NetworkInterfaces:

- DeviceIndex: '0'

  AssociatePublicIpAddress: 'true'

  SubnetId: !ImportValue

    'Fn::Sub': '${CafeNetworkParameter}-SubnetID'

  GroupSet:

    - !Ref CafeSG

* + - **Analysis**: The previous lines help ensure that your instance deploys to the *Public Subnet* that you created when you ran the café network stack. Recall that at the beginning of this task, you updated the network stack to define outputs with *export* names. In the preceding code, you *import* the value for the **SubnetId**. The preceding code also helps ensure that the instance you create will be in the *CafeSG* security group that is already defined for you in this template.
  + Set a **tag** with a *key* of *Name* and a *value* of *Cafe Web Server*
    - **Tip:** Observe how a *Name* tag was applied to the security group resource that is already defined in the template.
  + In the **Properties** section, include the following additional **UserData** code:

UserData:

  Fn::Base64:

    !Sub |

       #!/bin/bash

      yum -y update

      yum install -y httpd mariadb-server wget

      amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2

      systemctl enable httpd

      systemctl start httpd

      systemctl enable mariadb

      systemctl start mariadb

      wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod10-challenge/cafe-app.sh

      chmod +x cafe-app.sh

      ./cafe-app.sh

**Analysis**: The previous code runs on the instance at the end of the boot process. It installs an Apache HTTP web server, a MariaDB database, and PHP on the Amazon Linux instance. Next, it starts the web server and the database. Then, it downloads a script named cafe-app.sh and runs it. The cafe-app script configures the database and installs the PHP code that makes the café website function.

1. After you are satisfied with your template updates, save the changes. To validate the template format in the Bash terminal, run the following command:

aws cloudformation validate-template --template-body file:///home/ec2-user/environment/CFTemplatesRepo/templates/cafe-app.yaml

If you receive a JSON-formatted response that includes the three parameters that were defined at the top of your template, then your template passed the validation. However, if you received a *ValidationError* response (or some other error response), you must correct the issue. Then, save the changes and run the validate-template command again.

1. If your template passed the validation check, add the file to CodeCommit. In the Bash terminal, run git commands to add the file, commit it, and push it to the repository.

**Tip**: If it helps, refer back to the Git commands in Task 3. However, remember that the name of the template that you want to push to CodeCommit for this task is different.

1. Return to the CodePipeline console and choose the **CafeAppPipeline**.

**Note**: It might take a minute or two for the *Source* stage to update and for the *Deploy* stage to show that it is *In progress*. Eventually, the *Deploy* stage status should show *Succeeded - Just now*.

* + If the status shows a failure, try these troubleshooting tips.
    - If you see that the *Deploy* stage has a status of *Failed - Just now*, open the error information by choosing the **Details** link. It might provide a link that takes you to the AWS CloudFormation stack details. (Go to the **Events** tab to figure out which error was the first one that caused the stack to roll back).
    - If the stack fails to roll back, or if it has a *ROLLBACK\_COMPLETE* status that prevents you from updating the stack with the pipeline, you can delete the stack from the AWS CloudFormation stacks page. Then, push a new update to Git to trigger the stack to be created again.

1. In the AWS CloudFormation console, confirm that the *update-cafe-app* stack ran successfully and has a status of *CREATE\_COMPLETE*.

1. Go to the Amazon EC2 console. Observe that the EC2 instance and security group resources (which were defined in the cafe-app.yaml template) were created.

1. After the EC2 instance has started and passed both status checks, test the café website. In a browser tab, load the following URL, where <*public-ip-address*> is the *public IPv4 address* of the EC2 instance that you defined: http://<public-ip-address>/cafe

You should see the café website.

**Tip**: It can take 2 minutes or so for the user data script details that you defined to finish running. Be patient if you do not see the website immediately.

Notice that the website shows server information, such as the Region and Availability Zone where the web server is running.

Congratulations! You deployed a network layer and an application layer by using a CI/CD pipeline and an IaC approach.

**Answering questions about the results of creating an application layer**

1. Return to the browser tab with the multiple-choice questions for this lab, and answer the following questions:
   * **Question 4:** Go to the **Parameters** tab of the *update-cafe-app* stack. What value do you see for the **LatestAmiId**?
   * **Question 5:** Go to the **Stack info** tab of the *update-cafe-app* stack. What is the Amazon Resource Name (ARN) of the IAM role that grants the permissions to create and update the *update-cafe-app* stack?
   * **Question 6:** In the AWS Management Console, navigate to the CodeCommit repository where your AWS CloudFormation templates are stored. Choose **Commits** and in the **Commits** list, open one of the commits by choosing its commit ID. What you do observe?

**New business requirement: Duplicating the network and application resources in a second AWS Region (Challenge #4)**

Sofía is pleased that she was able to create both the network layer and the application layer for the dynamic café website by using AWS CloudFormation. Sofía also just learned that the café staff would like her to duplicate these resources into a second AWS Region, so she is even more pleased.

Sofía will soon experience the benefits of the hard work that she did to define the resources and configurations in AWS CloudFormation templates. She will observe that it is easier to duplicate environments through an IaC approach instead of creating all the resources manually.

**Task 7: Duplicating the café network and website to another AWS Region**

In this final lab task, you will experience how quickly you can duplicate a deployment. A quick deployment is possible because you defined all your resources in AWS CloudFormation templates.

In Tasks 4, 5, and 6, the AWS CloudFormation stacks were created or updated automatically. A pipeline was defined to monitor when the CodeCommit repository was updated. It then invoked AWS CloudFormation to create or update the stack. However, in this task, you will use the AWS CLI to duplicate the café network resources in another AWS Region. Then, you will use the AWS CloudFormation console to create the application stack in the second Region.

1. Back in the AWS Cloud9 IDE, run the following command to duplicate the café *network* to another AWS Region:

aws cloudformation create-stack --stack-name update-cafe-network --template-body file:///home/ec2-user/environment/CFTemplatesRepo/templates/cafe-network.yaml --region us-west-2

It should return a *StackId*. Notice that you could override the default Region for the creation of this stack by specifying the Region when you ran the command.

1. Browse to the AWS CloudFormation console and change the Region to **US West (Oregon) us-west-2**.
   * The *update-cafe-network* stack should be listed
   * Verify that the status of the second *update-cafe-region* stack eventually changes to *CREATE\_COMPLETE*

**Tip**: Use the refresh icon to see the status change more quickly when it completes.

1. Browse to the Amazon VPC service page, and also confirm that you are using the **Oregon** Region (*us-west-2*).

You should be able to observe the network resources that were created.

1. In the **Oregon** Region (*us-west-2*), create an EC2 key pair named cafe-oregon.
   * Browse to the Amazon EC2 console and confirm that you are in the **Oregon** Region.
   * From the navigation pane, choose **Network & Security > Key Pairs**.
   * Choose **Create key pair**.
   * Name the key pair cafe-oregon and choose **Create key pair** again.

**Tip**: You can optionally save the key pair, or you can choose **Cancel**. You don't need to use the key pair in this lab. However, in a typical use case, you must save the key pair—you will not have another opportunity to do so.

1. Revisit the application template details.
   * Return to the AWS Cloud9 IDE and observe the **cafe-app.yaml** template details in the text editor.
   * Notice the **KeyName** property in the resource definition for the EC2 instance. It references the **RegionMap** mapping that is defined in the template.
   * The mapping indicates that if the instance is launched in the *us-east-1 (N. Virginia) Region*, it should use the *vockey key pair*. However, if the instance is launched in the *us-west-2 (Oregon) Region*, it should use the *cafe-oregon key pair* that you just created.
   * Also notice the **InstanceTypeParameter** that you defined earlier. It provides a few instance type options in the **AllowedValues** area, but it also sets *t2.small* as the default. You will use this configuration in a moment.

1. In the AWS Cloud9 IDE, copy the template file to an S3 bucket. (In the following command, replace <*repobucket-bucketname*> with the actual S3 bucket name in your account. Its name should contain the string *repobucket*.)

aws s3 cp templates/cafe-app.yaml s3://<repobucket-bucketname>/

1. In the Amazon S3 console, copy the **Object URL** (which is an *https* address) of the file that you just uploaded.

1. In the AWS CloudFormation console, change the Region to **Oregon** (*us-west-2*).

1. Create a stack (with new resources).
   * In the **Amazon S3 URL** box of the **Create stack** screen, paste the object URL that you just copied.
   * In the next screen (**Specify stack details**) -
     + **Stack name**: Enter an appropriate name
     + **InstanceTypeParameter**: *t3.micro*

Notice that you can set the instance type at stack creation because you defined it as a parameter in the AWS CloudFormation template.

* + Advance through the remaining screens (accepting all the default settings), and finish creating the stack.
  + Verify that the stack created successfully.

1. Browse to the Amazon EC2 console and observe the created resources.
   * Be sure to give the web server a few minutes to finish booting and to run the user data script.
   * Notice the *key pair* that is used by the instance, and the instance type. These settings are different than the settings on the web server that runs in the *us-east-1* Region. You used the same template, *without modifying it*, to launch this stack.
   * After the server has fully started, you should be able to access the website at http://<public-ip-address>/cafe (where <*public-ip-address*> is the public IPv4 IP address of the EC2 instance.
   * Notice that the server information on the website shows that this second instance of the café website is running in the *us-west-2* Region. The first web server that you created shows it is running in the *us-east-1* Region.

**Update from the café**

Sofía is full with ideas as a result of what she just learned how to do!

She used AWS CloudFormation to deploy a static version of the café website successfully. She then deployed the dynamic café website as a web application successfully. For the dynamic website, Sofía used a CI/CD pipeline that used AWS CodeCommit, AWS CodePipeline, and AWS CloudFormation. In addition, she quickly duplicated both the network resources and the café application resources to another AWS Region.

Sofía imagines how she could use the AWS CloudFormation templates as part of a *backup and disaster recovery (DR)* solution. She just experienced how quickly she was able to re-create the essential café infrastructure. If her production deployment ever experiences a failure for any reason, she can now recreate it or duplicate it quickly.

Sofía also thinks about how she can now spin up *test environments* quickly. She can be confident that the configuration details of the test environments will match the production environment. She can also specifically control the ways that the test environment differs from the production environment by using features such as parameters and mappings.

The benefits of DevOps automation are many. Sofía now plans to make automation and CI/CD pipelines central to the way her team develops, tests, and deploys updates to the café's cloud resources.

**Submitting your work**

1. At the top of these instructions, choose **Submit** to record your progress and when prompted, choose **Yes**.
2. If the results don't display after a couple of minutes, return to the top of these instructions and choose Grades

**Tip**: You can submit your work multiple times. After you change your work, choose **Submit** again. Your last submission is what will be recorded for this lab.

1. To find detailed feedback on your work, choose Details followed by **View Submission Report**.

**Lab complete**

Congratulations! You have completed the lab.

1. To confirm that you want to end the lab, at the top of this page, choose **End Lab**, and then choose **Yes**.

A panel should appear with this message: *DELETE has been initiated... You may close this message box now.*

1. To close the panel, choose the **X** in the top-right corner.

*©2020 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.*

**Module 10 - Guided Lab: Automating Infrastructure Deployment with AWS CloudFormation**

**Lab overview and objectives**

Deploying infrastructure in a consistent, reliable manner is difficult. It requires people to follow documented procedures without taking any undocumented shortcuts. It can also be difficult to deploy infrastructure out-of-hours when fewer staff are available. AWS CloudFormation changes this situation by defining infrastructure in a template that can be automatically deployed—even on an automated schedule.

In this lab, you will learn how to deploy multiple layers of infrastructure with AWS CloudFormation, update a CloudFormation stack, and delete a stack (while retaining some resources).

After completing this lab, you should be able to:

* Use AWS CloudFormation to deploy a virtual private cloud (VPC) networking layer
* Use AWS CloudFormation to deploy an application layer that references the networking layer
* Explore templates with AWS CloudFormation Designer
* Delete a stack that has a deletion policy

**Duration**

This lab will require approximately **20 minutes** to complete.

**AWS service restrictions**

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

**Accessing the AWS Management Console**

1. At the top of these instructions, choose Start Lab to launch your lab.

A **Start Lab** panel opens, and it displays the lab status.

**Tip**: If you need more time to complete the lab, restart the timer for the environment by choosing the Start Lab button again.

1. Wait until the **Start Lab** panel displays the message *Lab status: ready*, then close the panel by choosing the **X**.
2. At the top of these instructions, choose AWS.

This action opens the AWS Management Console in a new browser tab. The system automatically logs you in.

**Tip**: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose **Allow pop-ups**.

1. Arrange the **AWS Management Console** tab so that it displays alongside these instructions. Ideally, you will have both browser tabs open at the same time so that you can follow the lab steps more easily.

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

**Task 1: Deploying a networking layer**

It is a best practice to deploy infrastructure in *layers*. Common layers are:

* Network (Amazon VPC)
* Database
* Application

This way, templates can be reused between systems. For example, you can deploy a common network topology between development, test, and production environments, or deploy a standard database for multiple applications.

In this task, you will deploy an AWS CloudFormation template that creates a *networking layer* by using Amazon VPC.

1. Right-click the following link and download the template to your computer: [lab-network.yaml](https://labs.vocareum.com/web/1466849/360628.0/ASNLIB/public/scripts/lab-network.yaml)

 If you want, you can open the template in a text editor to see how the AWS resources are defined.

Templates can be written in JavaScript Object Notation (JSON) or YAML Ain't Markup Language (YAML). YAML is a markup language that is similar to JSON, but it is easier to read and edit.

1. In the **AWS Management Console**, from the **Services** menu, choose **CloudFormation**.
2. If you see this message, click Try it out now and provide us feedback:
3. Choose **Create stack** and configure these settings.

**Step 1: Specify template**

* + **Template source:** **Upload a template file**
  + **Upload a template file:** Click **Choose file** then select the **lab-network.yaml** file that you downloaded.
  + Choose **Next**

**Step 2: Create Stack**

* + **Stack name:** lab-network
  + Choose **Next**

**Step 3: Configure stack options**

* + In the **Tags** section, enter these values.
    - **Key:** application
    - **Value:** inventory
  + Choose **Next**

**Step 4: Review lab-network**

* + Choose **Create stack**

The *template* will now be used by AWS CloudFormation to generate a *stack* of resources in the AWS account.

The specified *tags* are automatically propagated to the resources that are created, which makes it easier to identify resources that are used by particular applications.

1. Choose the **Stack info** tab.
2. Wait for the **Status** to change to CREATE\_COMPLETE.

 Choose **Refresh**  every 15 seconds to update the display, if necessary.

You can now examine the resources that were created.

1. Choose the **Resources** tab.

You will see a list of the resources that were created by the template.

 If the list is empty, update the list by choosing **Refresh** .

1. Choose the **Events** tab and scroll through the events log.

The events log shows (from more recent to less recent) the activities that were performed by AWS CloudFormation. Example events include starting to create a resource and then completing the resource creation. Any errors that were encountered during the creation of the stack will be listed in this tab.

1. Choose the **Outputs** tab.

A CloudFormation stack can provide *output information*, such as the ID of specific resources and links to resources.

Two outputs are listed.

* + **PublicSubnet:** The ID of the public subnet that was created (for example: \_subnet-08aafd57f745035f1\_\_
  + **VPC:** The ID of the VPC that was created (for example: *vpc-08e2b7d1272ee9fb4*)

Outputs can also be used to provide values to other stacks. This is shown in the **Export name** column. In this case, the VPC and subnet IDs are given export names so that other stacks can retrieve the values. These other stacks can then build resources inside the VPC and subnet that were just created. You will use these values in the next task.

1. Choose the **Template** tab.

This tab shows the template that was used to create the stack—that is, the template that you uploaded while you created the stack. Feel free to examine the template and see the resources that were created. Also feel free to explore the **Outputs** section at the end (this section defined which values to export).

**Task 2: Deploying an application layer**

Now that you deployed the *network layer*, you will deploy an *application layer* that contains an Amazon Elastic Compute Cloud (Amazon EC2) instance and a security group.

The AWS CloudFormation template will *import* the VPC and subnet IDs from the *Outputs* of the existing CloudFormation stack. It will then use this information to create the security group in the VPC and the EC2 instance in the subnet.

1. Right-click the following link and download the template to your computer: [lab-application.yaml](https://labs.vocareum.com/web/1466849/360628.0/ASNLIB/public/scripts/lab-application.yaml)

 If you want, you can open the template in a text editor to see how resources are defined.

1. In the left navigation pane, choose **Stacks**.
2. Select **Create stack > With new resources (standard)**, and then configure these settings.

**Step 1: Specify template**

* + **Template source:** **Upload a template file**
  + **Upload a template file:** Click **Choose file** then select the **lab-application.yaml** file that you downloaded.
  + Choose **Next**

**Step 2: Create Stack**

* + **Stack name:** lab-application
  + **NetworkStackName:** lab-network
  + Choose **Next**

 The *Network Stack Name* parameter tells the template the name of the first stack that you created (*lab-network*), so it can retrieve values from the *Outputs*.

**Step 3: Configure stack options**

* + In the **Tags** section, enter these values.
    - **Key:** application
    - **Value:** inventory
  + Choose **Next**

**Step 4: Review lab-application**

* + Choose **Create stack**

While the stack is being created, examine the details in the **Events** tab and the **Resources** tab. You can monitor the progress of the resource-creation process and the resource status.

1. In the **Stack info** tab, wait for the **Status** to change to CREATE\_COMPLETE.

Your application is now ready!

1. Choose the **Outputs** tab.
2. Copy the **URL** that is displayed, open a new web browser tab, paste the URL, and press ENTER.

The browser tab will open the application, which is running on the web server that this new CloudFormation stack created.

A CloudFormation stack can use reference values from another CloudFormation stack. For example, this portion of the *lab-application* template references the *lab-network* template:

  WebServerSecurityGroup:

    Type: AWS::EC2::SecurityGroup

    Properties:

      GroupDescription: Enable HTTP ingress

      VpcId:

        Fn::ImportValue:

          !Sub ${NetworkStackName}-VPCID

The last line uses the *network stack name* that you provided (*lab-network*) when the stack was created. It imports the value of *lab-network-VPCID* from the *Outputs* of the first stack. It then inserts the value into the VPC ID field of the security group definition. The result is that the security group is created in the VPC that was created by the first stack.

Here is another example, which is in the CloudFormation template that you just used to create the application stack. This template code places the EC2 instance into the subnet that was created by the network stack:

  SubnetId:

    Fn::ImportValue:

    !Sub ${NetworkStackName}-SubnetID

It takes the *subnet ID* from the *lab-network* stack and uses it in the *lab-application* stack to launch the instance into the public subnet, which was created by the first stack.

**Task 3: Updating a Stack**

AWS CloudFormation can also *update* a stack that has been deployed. When you update a stack, AWS CloudFormation will only modify or replace the resources that are being changed. Any resources that are not being changed will be left as-is.

In this task, you will update the *lab-application* stack to modify a setting in the security group.

First, you will examine the current settings for the security group.

1. In the **AWS Management Console**, from the **Services** menu, choose **EC2**.
2. In the left navigation pane, choose **Security Groups**.
3. Select the check box for  **lab-application-WebServerSecurityGroup...**.
4. Choose the **Inbound rules** tab.

Currently, only one rule is in the security group. The rule permits *HTTP* traffic.

You will now return to AWS CloudFormation to update the stack.

1. From the **Services** menu, choose **CloudFormation**.
2. Right-click the following link and download the updated template to your computer: [lab-application2.yaml](https://labs.vocareum.com/web/1466849/360628.0/ASNLIB/public/scripts/lab-application2.yaml)

This template has an additional configuration to permit inbound Secure Shell (SSH) traffic on port 22:

  - IpProtocol: tcp

    FromPort: 22

    ToPort: 22

    CidrIp: 0.0.0.0/0

1. In the **Stacks** list of the **AWS CloudFormation console**, select **lab-application**.
2. Choose **Update** and configure these settings.
   * Select **Replace current template**
   * **Template source:** **Upload a template file**
   * **Upload a template file:** Click **Choose file** then select the **lab-application2.yaml** file that you downloaded.
3. Choose **Next** in each of the next *three* screens to advance to the **Review lab-application** page.

In the **Change set preview** section at the bottom of the page, AWS CloudFormation displays the resources that will be updated:

This change set preview indicates that AWS CloudFormation will *Modify* the *WebServerSecurityGroup* without needing to replace it (*Replacement = False*). This change set means that the security group will have a minor change applied to it, and no references to the security group will need to change.

1. Choose **Update stack**
2. In the **Stack info** tab, wait for the **Status** to change to UPDATE\_COMPLETE.

 Update the status by choosing **Refresh**  every 15 seconds, if necessary.

You can now verify the change.

1. Return to the **Amazon EC2 console** and from the left navigation pane, choose **Security Groups**.
2. In the **Security Groups** list, select **lab-application-WebServerSecurityGroup**.

The **Inbound rules** tab should display an additional rule that allows *SSH* traffic over *TCP port 22*.

This subtask demonstrates how changes can be deployed in a repeatable, documented process. The AWS CloudFormation templates can be stored in a source code repository (such as AWS CodeCommit). This way, you can maintain versions and a history of the templates and the infrastructure that was deployed.

**Task 4: Exploring templates with AWS CloudFormation Designer**

*AWS CloudFormation Designer* is a graphic tool for creating, viewing, and modifying AWS CloudFormation templates. With Designer, you can diagram your template resources by using a drag-and-drop interface, and then edit their details through the integrated JSON and YAML editor.

Whether you are a new to AWS CloudFormation or an experienced AWS CloudFormation user, Designer can help you quickly see the interrelationship between a template's resources. It also enables you to easily modify templates.

In this task, you will gain some hands-on experience with Designer.

1. From the **Services** menu, choose **CloudFormation**.
2. In the left navigation pane, choose **Designer**.

**Tip:** You might need to expand the left navigation pane by choosing the menu icon.

1. Choose the **File**  menu, select **Open > Local file**, and select the **lab-application2.yaml** template that you downloaded previously.

Designer will display a graphical representation of the template:

Instead of drawing a typical architecture diagram, Designer is a visual editor for AWS CloudFormation templates. It draws the resources that are defined in a template and their relationship to each other.

1. Experiment with the features of the Designer. Some things to try are:
   * Click the displayed resources. The lower pane will then display the portion of the template that defines the resources.
   * Try dragging a new resource—from the **Resource types** pane on the left—into the design area. The definition of the resource will be automatically inserted into the template.
   * Try dragging the resource connector circles to create relationships between resources.
   * Open the **lab-network.yaml** template that you downloaded earlier in the lab and also explore its resources in Designer.

**Task 5: Deleting the stack**

When resources are no longer required, AWS CloudFormation can delete the resources built for the stack.

A *deletion policy* can also be specified against resources. It can preserve or (in some cases) back up a resource when its stack is deleted. This feature is useful for retaining databases, disk volumes, or any resource that might be needed after the stack is deleted.

The *lab-application* stack was configured to take a snapshot of an Amazon Elastic Block Store (Amazon EBS) disk volume before it is deleted. The code in the template that accomplishes that configuration is:

DiskVolume:

  Type: AWS::EC2::Volume

  Properties:

    Size: 100

    AvailabilityZone: !GetAtt WebServerInstance.AvailabilityZone

    Tags:

      - Key: Name

        Value: Web Data

  DeletionPolicy: Snapshot

The *DeletionPolicy* in the final line directs AWS CloudFormation to create a snapshot of the disk volume before it is deleted.

You will now delete the *lab-application* stack and see the results of this deletion policy.

1. Return to the main **AWS CloudFormation console** by choosing the Close link at the top of the Designer page (choose **Leave page** if prompted).
2. In the list of stacks, choose the **lab-application** link.
3. Choose **Delete**
4. Choose **Delete stack**

You can monitor the deletion process in the **Events** tab and update the screen by choosing **Refresh**  occasionally. You might also see an events log entry that indicates that the EBS snapshot is being created.

1. Wait for the stack to be deleted. It will disappear from the stacks list.

The application stack \_\_ removed, but the network stack remained untouched. This scenario reinforces the idea that different teams (for example, the network team or the application team) could manage their own stacks.

You will now verify that a snapshot of the EBS volume was created before the EBS volume was deleted.

1. From the **Services** menu, choose **EC2**.
2. In the left navigation pane, choose **Snapshots**.

You should see a snapshot with a **Started** time in the last few minutes.

**Submitting your work**

1. At the top of these instructions, choose **Submit** to record your progress and when prompted, choose **Yes**.
2. If the results don't display after a couple of minutes, return to the top of these instructions and choose Grades

**Tip**: You can submit your work multiple times. After you change your work, choose **Submit** again. Your last submission is what will be recorded for this lab.

1. To find detailed feedback on your work, choose Details followed by  **View Submission Report**.

**Lab complete**

 Congratulations! You have completed the lab.

1. Choose End Lab at the top of this page, and then select **Yes** to confirm that you want to end the lab.

A panel indicates that *DELETE has been initiated... You may close this message box now.*

1. Select the **X** in the top right corner to close the panel.

*©2020 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.*