DevOps Challenges

Challenge 1:

Create a VPC on AWS platform using AWS Cloud formation Service.

Details:

AWS CloudFormation is an fine way to deploy VPCs in a repeatable, reliable manner because the template used by CloudFormation acts as documentation to show exactly what is being deployed.

You can walk through parts of a blueprint for AWS CloudFormation and review the deployed tools. You'll also learn by CloudFormation how to conduct updates.

You can easily customize the network configuration for your virtual private cloud. For example, you can create a public-facing subnet for your web servers that has access to the Internet and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Tasks:

1. Deploy an AWS CloudFormation template that creates an Amazon VPC
2. Examine the components of the template
3. Update a CloudFormation stack
4. Examine a template with the AWS CloudFormation Designer
5. Delete a CloudFormation stack

Pre-requisites

NA

Challenge 2:

Blue/Green Deployment Pattern with AWS Elastic Beanstalk.

Details:
Deploy a simple web application continuously using The Elastic Beanstalk Command Line Interface (EB CLI).

AWS Elastic Beanstalk provides a quick and easy way to deploy your web applications to the AWS cloud without requiring knowledge of the individual pieces that make up the infrastructure required to deploy your app to the cloud. EB CLI is a command line interface for Elastic Beanstalk that provides interactive commands that simplify creating, updating and monitoring environments from a local repository. You can use it to automate deployment tasks and common administrative tasks in AWS.

Steps

1. Deploying web application versions on an Elastic Beanstalk environment
2. Managing environments with the EB CLI
3. Deploying a new version of your application in Rolling
4. update (In-Place Deployment)
5. Deploying a new version of your application in Blue/Green
6. Deployment (Red/Black Deployment)

Pre-requisites

To successfully complete this lab, you should be familiar with basic Linux server administration and comfortable using the Linux command-line.

Challenge 3:

Launching and Managing a Web Application with AWS CloudFormation.

Details:

In the first part you will create a simple resource, an Amazon S3 bucket, with AWS CloudFormation and you will look at different retention policies applied when you delete an AWS CloudFormation stack or during a rollback.

In the second part, you will provision a simple Java web application using an Amazon Linux instance. You will then see how to re-apply an AWS CloudFormation template to the existing application to change some resource attributes such as an Amazon EC2 instance type. Finally, you will add a load balancer and an Auto Scaling group based on an Auto Scaling configuration.

Steps

1. Create an Amazon Simple Storage Service (S3) bucket using AWS CloudFormation
2. Provision a simple PHP web application using an Amazon Linux AMI
3. Apply an AWS CloudFormation template to an existing application
4. Modify an existing application using AWS CloudFormation
5. Add IAM roles and Elastic Load Balancing to the application using AWS CloudFormation

Pre-requisites

vi editor knowledge

Challenge 4:

Monitor the Security Groups with AWS Configuration management.

Details:

Monitor the configuration of a security group for unauthorized changes. You will learn how to use AWS config Rules with an AWS Lambda function to monitor the ingress ports associated with an EC2 security group. The Lambda function will be triggered whenever the security group is modified. If the ingress rule configuration differs from that which is coded in the function, the Lambda function will revert the ingress rules back to the appropriate configuration.

Steps

1. Upload a preconfigured Lambda function
2. Enable AWS Config
3. Create and enable a custom AWS Config rule
4. Use CloudWatch Logs to review the execution of the AWS Config rule.

Pre-requisites

You should be familiar with EC2 security groups. Python programming skills are helpful.