## Lab 7-03: Using AWS Config and CloudTrail

### Service Introduction

AWS Config is a service that allows you to assess, audit, and evaluate the configurations of your AWS resources. AWS CloudTrail records actions taken by users, roles, or AWS services. Together, these services ensure compliance, security, and operational auditing in your AWS environment.

### Problem

Your organization needs to ensure compliance with internal policies and regulatory requirements. You lack visibility into configuration changes and user activities within your AWS environment, making it difficult to audit and investigate potential security issues or misconfigurations.

### Solution

Implement AWS Config to continuously monitor and record configurations of your AWS resources, and use AWS CloudTrail to log and track all API calls made within your AWS account. AWS Config helps detect and remediate non-compliant configurations, while CloudTrail offers detailed logs of user and service activities, enabling comprehensive auditing and rapid identification of unauthorized changes or security breaches.

#### Task 1: Initiate the Scream Test

|  |
| --- |
| 1. Navigate to the EC2 console by entering "EC2" in the search bar at the top and selecting EC2 from the search results.      1. Locate the CorporateServer instance and check the corresponding checkbox. Make a note of the instance ID for reference later in the lab.      1. Click on **Instance state.** 2. From the dropdown menu, click on **Stop instance.**      1. When prompted, click **Stop.**      1. In the Details tab as shown below, click on the blue link under **Subnet ID.**      1. In the new browser tab or window, select the PrivateAZ1 subnet and note the route table ID for later reference in this lab.      1. In the Details tab below, click on the blue link under **Route table.** 2. In the new browser tab or window that opens, click on the **Routes** tab below. 3. Click on **Edit routes.**      1. For the route with the following destination 0.0.0.0/0 and target nat-xxxxxxxxxxxxxxxxx, click on Remove next to the route for the NAT gateway.      1. Click on **Save changes.**      1. In the left-hand navigation menu, click on **Security Groups** under Security. 2. Locate and select the **CorporateApplicationServer** security group. Make sure to note the security group ID for later on in this lab. 3. Click on the **Outbound rules** tab below. 4. Click on **Edit outbound rules.**      1. Click on **Delete** for the one outbound rule with the destination set to 0.0.0.0/0. 2. Click on **Save rules.** |

#### Task 2: Review the Changes for the Scream Test in Config and CloudTrail

|  |
| --- |
| 1. Navigate to **CloudTrail** by entering "cloudtrail" in the search bar and selecting CloudTrail from the search results.      1. Click on the hamburger menu icon (the icon with three horizontal bars) in the top left corner. 2. Click on Event History. 3. Click on the Read-only dropdown menu and select Resource Name.      1. In the search field, paste in the Instance ID noted in the first step and look for the **StopInstances** event. 2. Select the **StopInstances** event and review the details of the change.      1. In the CloudTrail console's search field, paste the previously noted route table ID and search for any **DeleteRoute** events. 2. Select the **DeleteRoute** event and review the details of the changes. 3. At the bottom of the event details, click on View AWS Config resource timeline.      1. In the AWS Config timeline, you will see a Configuration change event at the very top. Click on the **+** icon to see the details of the changes. 2. Take note of the output in the JSON diff results, which specifies the deleted route from the PrivateAZ1 route table, particularly the NAT Gateway ID, as you will need this information later in the lab.      1. In the search field of the **CloudTrail** console, paste in the Security Group ID noted in the first step and look for any RevokeSecurityGroupEgress events. 2. Select the RevokeSecurityGroupEgress event and review the details of the changes. 3. At the bottom of the event details, click on **View AWS Config resource timeline.**      1. Make note of the output in the JSON diff results, which details the specific security group rules that were deleted from the Corporate Application Server security group. |

#### Task 3: Revert the Scream Test Changes and Test Networking

|  |
| --- |
| 1. Navigate to the VPC console by entering "VPC" in the search bar on top and selecting the **VPC** search result.      1. Click on **Security Groups.** 2. Locate and select the **CorporateApplicationServer** security group. 3. Click on the **Outbound rules** tab, and click on **Edit outbound rules.**      1. Select **Add rule** and set the following values:  * Type: Select All Traffic. * Destination: Select Anywhere-IPv4.  1. Click on **Save rules** to complete reverting the security group change.      1. In the left-hand navigation menu, click on **Route Tables.** 2. Locate and select the **PrivateAZ1RT** route table.      1. Click on the **Routes** tab and click on **Edit routes.**      1. Select **Add route** and set the following values:  * Destination: Enter "0.0.0.0/0". * Target: Select NAT Gateway.  1. Click on **Save changes** to complete reverting the route table change.      1. Navigate to the EC2 console by entering "EC2" in the search bar on top and select EC2 from the search results.      1. In the left-hand navigation menu, select Instances. 2. Find the **CorporateServer** instance. 3. Select the instance and click on **Instance state.** 4. Click on **Start instance** and wait a few minutes for the instance to fully boot up and initialize.      1. Select the **CorporateServer** instance and click on **Connect.** 2. Click on the **Session Manager** tab and click on **Connect.**      1. Elevate your permission to the root user on the instance:   sudo –i   1. Run the following command to verify network connectivity:   yum install -y nmap     1. Run a ping test to a Google-resolving DNS server to confirm that we can reach out to the public internet:   ping -c4 8.8.8.8 |