

**Senior Academy - IT training center**

**www.seniorsteps.net**

**contact us: 0224153419 - 01090873748**

**عمارة 4 - شارع محمد توفيق دياب - عباس العقاد - مدينة نصر - الدورال 1**

**(Senior Academy - IT training center)**

**The Place You Can Be A Senior**



**www.seniorsteps.net**

**<https://www.facebook.com/seniorsteps.it>**

**contact us: 0224153419 - 01090873748**

**فرع مدينة نصر 1 : عمارة 4 - شارع محمد توفيق دياب - عباس العقاد - مدينة نصر - الدورال 1**

**Senior Steps - IT training center**

**The place You can be A Senior**

Senior Academy - IT training center

[www.seniorsteps.net](http://www.seniorsteps.net)

contact us: 0224153419 - 01090873748

عمارة 4 - شارع محمد توفيق دياب - عباس العقاد - مدينة نصر - الدورال 1

## *DevOps Engineer Diploma*

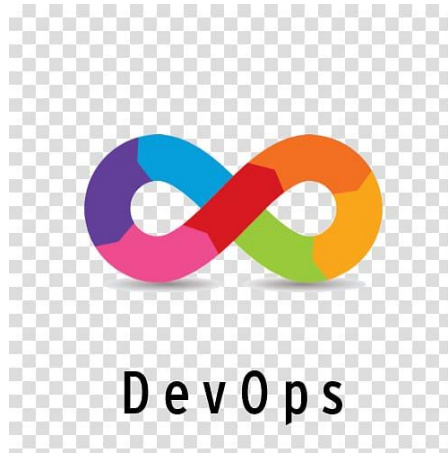


DevOps

Senior Steps - IT training center

The place You can be A Senior

## **DevOps Engineer Diploma**



### **AWS Labs**

### **Lab 21**

## **CloudTrail Setup and S3 Log Integration**

### **### Lab Objectives**

- Creating CloudTrail Trails for Account Activity Monitoring
- Configuring Management Event Logging Across All Regions
- Integrating CloudTrail with S3 for Centralized Log Storage
- Enabling Log File Validation for Integrity and Compliance
- Verifying CloudTrail Log Delivery to S3 Buckets

## Overview

This lab focuses on implementing centralized logging and activity monitoring in AWS using **CloudTrail** and **Amazon S3**. The goal is to create a CloudTrail trail that captures all **account management events** and stores the generated logs in a dedicated S3 bucket. This setup represents a foundational security and compliance practice for monitoring AWS environments.

---

## Scenario

In a real-world AWS environment, organizations must maintain visibility into the changes and actions performed within their cloud accounts. Activities such as user logins, IAM updates, resource creation, deletion, and configuration changes are classified as **management events**. Tracking these actions is critical for:

- Security auditing
- Troubleshooting
- Compliance requirements
- Forensic analysis

AWS **CloudTrail** provides a complete history of such events and allows them to be archived in an Amazon S3 bucket for long-term storage or external analysis tools.

In this lab, you will configure a CloudTrail trail that continuously records all relevant management events, applies the configuration **globally across all AWS regions**, and stores these logs securely in an S3 bucket created specifically for CloudTrail.

---

## Lab Requirements

During this lab, you will be expected to:

- Work within the AWS Management Console
  - Create and configure a CloudTrail trail
  - Create a storage bucket with a naming format that identifies the student (“cloudtrail-logs-yourname”)
  - Ensure CloudTrail log file validation is enabled
  - Confirm that logs are properly uploaded to the S3 bucket
- 

## What You Will Build

### CloudTrail Trail - "MyTrail"

You will create a new CloudTrail trail, which will be responsible for capturing critical account-level

actions such as IAM changes, API calls, and configuration updates. The trail will be configured to enable:

- **All management events**
- **Integration across all AWS regions** for complete coverage
- **Log file integrity validation**, ensuring logs are not modified or tampered with

### S3 Bucket for Log Storage

A new S3 bucket will serve as the centralized location where all CloudTrail logs are delivered. The bucket name will follow a standardized convention (e.g., cloudtrail-logs-yourname) to ensure uniqueness and traceability.

CloudTrail will automatically organize log files into a structured folder hierarchy within the bucket, making it easy to browse and analyze logs.

### Log Delivery Verification

After configuration, CloudTrail will begin delivering logs to the bucket. You will verify that log files appear under the expected S3 prefixes and confirm that the trail is active and functioning correctly.

---

### Deliverables

Participants must submit:

- A screenshot of the **created CloudTrail trail** in the CloudTrail console
- A screenshot showing **CloudTrail log files** successfully delivered to the S3 bucket

These deliverables will confirm that the trail is active and that the S3 bucket integration is working as expected.

You are Welcome

