[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+alnafi07+2025_02+type@vertical+block@d462603c1d6e4b028ecb13f167bd96af?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Lab 3: SysOps Monitoring & Management**

*RQF Level 5*

**Objective:**

The objective of this lab is to provide hands-on experience with key monitoring, management, and logging tools on AWS. Participants will learn to configure Amazon CloudWatch for resource monitoring, set up alarms for proactive alerting, and explore AWS CloudTrail for auditing and tracking AWS API usage.

**Prerequisites:**

* SysOps Advancement Track

**Lab Steps:**

**Step 1: Introduction to SysOps Monitoring on AWS**

- Briefly discuss the importance of monitoring, management, and logging in cloud environments.

- Emphasize the role of Amazon CloudWatch and AWS CloudTrail in SysOps.

**Step 2: Configuring Amazon CloudWatch**

- Access the AWS Management Console and navigate to Amazon CloudWatch.

- Explore the CloudWatch dashboard to understand available metrics.

- Create a custom CloudWatch dashboard for a specific use case or service.

- Set up a basic CloudWatch alarm for an AWS resource (e.g., EC2 instance).

**Step 3: Exploring CloudWatch Metrics and Logs**

- Dive deeper into CloudWatch Metrics for various AWS services.

- Explore CloudWatch Logs and create a log group.

- Configure logging for a specific resource, such as an EC2 instance or an S3 bucket.

**Step 4: Creating Advanced Alarms**

- Build on the basic alarm configuration by creating more advanced alarms.

- Configure composite alarms based on multiple metrics or conditions.

- Set up actions for alarms, such as sending notifications or triggering automated responses.

**Step 5: Introduction to AWS CloudTrail**

- In the AWS Management Console, navigate to AWS CloudTrail.

- Provide an overview of AWS CloudTrail's role in auditing and monitoring AWS API activity.

**Step 6: Configuring AWS CloudTrail**

- Create a new AWS CloudTrail trail.

- Specify the S3 bucket to store CloudTrail logs.

- Enable logging for all regions or select specific regions based on requirements.

**Step 7: Analyzing CloudTrail Logs**

- Explore AWS CloudTrail logs stored in the configured S3 bucket.

- Identify and analyze AWS API activities recorded by CloudTrail.

- Discuss how CloudTrail logs can be used for security analysis and compliance.

**Step 8: Cleanup**

- Guide learners through proper cleanup procedures to avoid incurring unnecessary costs.

- Delete the AWS resources created during the lab, such as CloudWatch alarms and CloudTrail trails.

*Conclusion:*

*By completing this lab, participants have gained practical experience in configuring Amazon CloudWatch for monitoring, setting up alarms, and exploring AWS CloudTrail for auditing. These skills are crucial for SysOps professionals to ensure effective management, monitoring, and security of AWS environments. The lab sets the foundation for continued learning and application of these tools in real-world scenarios.*

