PRJ-CISA-048: Continuous Access Control Monitoring with IAM Access Analyzer

Certification: Certified Information Systems Auditor (CISA) **Domain:** Domain 3 - Information Systems Acquisition, Development, and Implementation

---

1. Project Overview

This project focuses on the critical control of **access permissions** and the principle of **least privilege**. In a complex cloud environment, it is easy to misconfigure an IAM policy or S3 bucket policy, inadvertently granting public or unintended cross-account access to sensitive resources. Manually auditing these policies is complex and does not scale. **AWS IAM Access Analyzer** is a service that solves this by using automated reasoning and formal methods to continuously analyze resource policies and generate findings for any that allow access from outside your defined “zone of trust” (typically your AWS account or Organization).

This project demonstrates how to enable and use IAM Access Analyzer to proactively detect and review unintended external access. We will create a deliberately misconfigured S3 bucket policy, see how Access Analyzer generates a finding, and then build an automated workflow to review, archive, and even auto-remediate these findings. This provides auditors with a powerful, continuous monitoring control that mathematically proves who can access critical resources.

Key Objectives

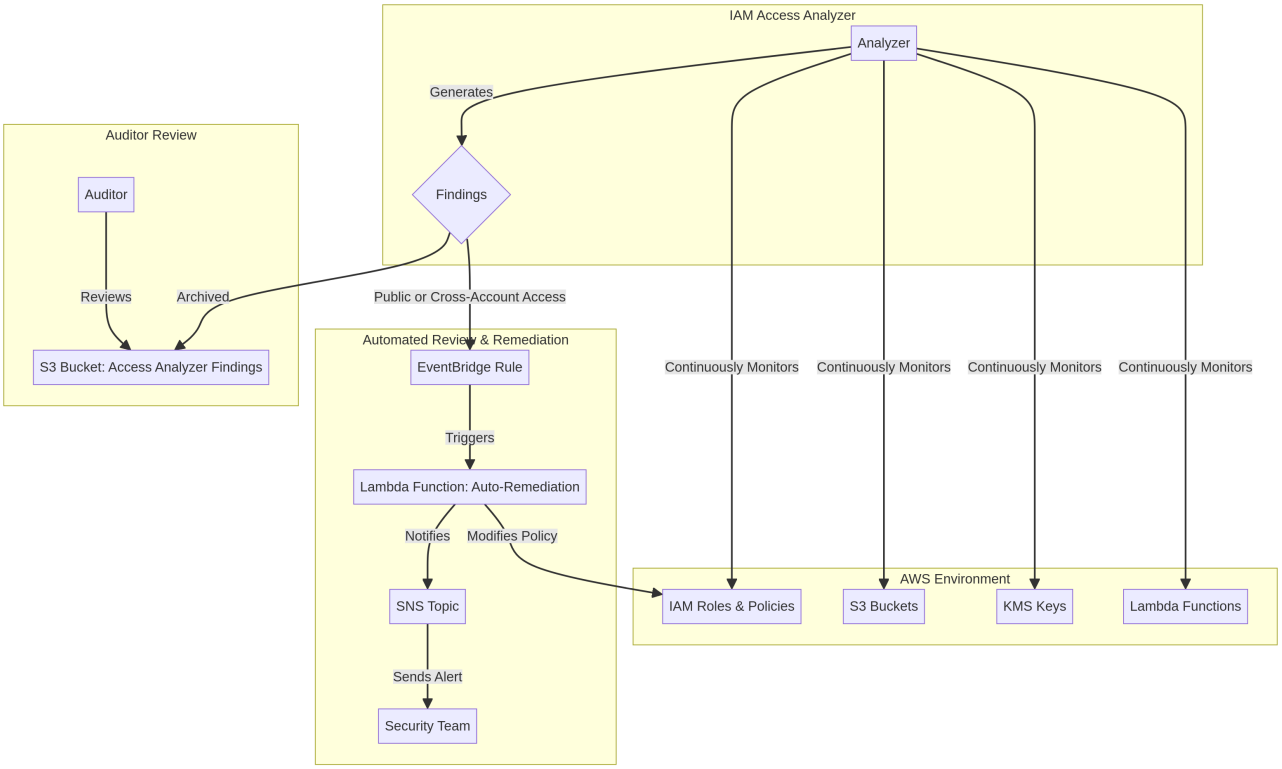
- Understand the importance of continuous monitoring for access control policies.
- Learn how IAM Access Analyzer uses formal logic to analyze policies.
- Enable and configure an analyzer for your AWS account or Organization.

- Intentionally create a resource policy that grants external access and observe the generated finding.
- Develop a workflow to automatically archive findings for audit evidence.
- (Advanced) Create an automated remediation workflow that alerts security teams and can optionally fix the misconfigured policy.

---

2. Architecture

The architecture uses IAM Access Analyzer as the core detection engine, with EventBridge and Lambda providing the automation for review and remediation.



Architectural Flow:

1. **Continuous Monitoring:**
    - Once enabled, the **IAM Access Analyzer** continuously monitors resource-based policies attached to supported services like **S3 buckets, IAM roles, KMS keys, Lambda functions, and SQS queues**.
    - It applies mathematical logic to determine all possible access paths allowed by these policies.

2. **Finding Generation:**
    - If the analyzer discovers a policy that allows access from a principal (e.g., another AWS account, an anonymous user) that is outside your defined zone of trust, it generates a **Finding**.
    - Each finding contains detailed information about the resource, the external principal, and the specific actions allowed.
3. **Automated Review and Remediation:**
    - All Access Analyzer findings are automatically sent to **Amazon EventBridge**.
    - An **EventBridge Rule** is configured to match new findings from Access Analyzer.
    - The rule triggers two parallel actions:
        - **Remediation/Notification:** It invokes a **Lambda function** (`Auto-Remediation`). This function can be programmed to:
            - Send a high-priority alert to the **Security Team** via an **SNS Topic**.
            - (Optional) Automatically remediate the issue by, for example, removing the offending statement from the S3 bucket policy.
        - **Archiving for Audit:** It uses an **EventBridge API Destination** or another Lambda to send the full JSON of the finding to a secure **S3 bucket** for long-term storage as audit evidence.
4. **Auditor Review:**
    - An **Auditor** can review the archived findings in S3 to verify that access control policies are being monitored and that any deviations are being handled according to the organization's incident response plan.

---

3. Prerequisites

- An AWS account with administrative permissions.
- An S3 bucket to act as the target for the misconfigured policy.
- An email address for SNS notifications.

---

4. Step-by-Step Implementation Guide

Step 4.1: Enable IAM Access Analyzer

1. Go to the **IAM Console -> Access Analyzer**.
2. Click **Create analyzer**.
3. **Name:** `My-Organization-Analyzer` (or `My-Account-Analyzer`).
4. **Zone of trust:** By default, this is your AWS account. If you are in an AWS Organization, you can set the zone of trust to be the entire Organization.
5. Click **Create analyzer**. The analyzer is now active and will begin its initial scan.

Step 4.2: Create a Misconfigured Resource

We will create an S3 bucket and apply a policy that makes it publicly readable.

1. Create a new S3 bucket.
2. Go to the bucket's **Permissions** tab and edit the **Bucket policy**.
3. Paste the following policy, replacing `YOUR_BUCKET_NAME` with your bucket's name. This policy grants `GetObject` access to everyone (`"Principal": "*"`).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*"
        }
    ]
}
```

4. Save the policy. You will get a warning that the bucket is now public.

Step 4.3: Review the Finding

1. Go back to the **IAM Access Analyzer** console.
2. Within a few minutes, a new **Active finding** should appear.
3. Click on the finding to see the details. It will clearly state that the S3 bucket is accessible to the public, identify the specific policy statement, and show the permissions granted (`s3:GetObject`).
4. This demonstrates the core detection capability.

Step 4.4: Automate Notification and Archiving

1. **Create an SNS Topic** for security alerts and subscribe your email address to it.
2. **Create an EventBridge Rule:**
    - Go to the **EventBridge Console -> Rules -> Create rule**.
    - **Name:** `IAM-Access-Analyzer-Findings-Rule`
    - **Event bus:** default.
    - **Rule type:** Rule with an event pattern.
    - **Event pattern:**

```
{
    "source": ["aws.access-analyzer"],
    "detail-type": ["Access Analyzer Finding"]
}
```

    - **Select targets:**
        - **Target 1:** SNS topic.
        - **Topic:** Select the SNS topic you created.
        - (Optional) You can configure an **Input transformer** to create a more human-readable message for the email alert.
    - Create the rule.

Step 4.5: Test the Automation

1. To test the rule, you can either create another misconfigured resource or **archive and then un-archive** the existing finding in the Access Analyzer console. When a finding's status changes, it generates a new event.
2. When the event is generated, you should receive an email from SNS containing the full JSON of the finding.
3. This confirms that your automated notification and evidence collection pipeline is working.

---

5. The Auditor's Perspective

As a CISA, this automated system provides several key audit assurances:

- **Completeness:** The analyzer checks all supported resources, ensuring no policies are missed.
- **Accuracy:** The use of formal methods provides a mathematical guarantee that the findings are correct, eliminating false positives.
- **Timeliness:** The continuous monitoring and real-time alerting allow for rapid detection and response to misconfigurations, reducing the window of exposure.
- **Audit Trail:** The archived findings in S3 create an immutable record of all policy violations, which can be reviewed to assess the effectiveness of the organization's access control processes.

---

6. Cleanup

1. Go to the **S3 bucket** and **delete the bucket policy**.
2. In the **IAM Access Analyzer console**, the finding should automatically move to the **Resolved** state.
3. **Delete the EventBridge rule.**
4. **Delete the SNS topic.**
5. Go to the **IAM Access Analyzer console** and **delete the analyzer** itself.

Business Context

The Problem

Organizations need to demonstrate compliance with audit requirements but lack automated evidence collection. Manual audit preparation is time-consuming and error-prone. Auditors struggle to verify security controls and compliance in dynamic cloud environments.

The Solution

Automated compliance monitoring and audit evidence collection system. Continuously assesses AWS environment against compliance frameworks, generates audit reports, and maintains evidence repository. Provides real-time compliance dashboards and automated remediation for non-compliant resources.

Business Value

- **Audit Efficiency:** Reduces audit preparation time from months to days
- **Continuous Compliance:** Real-time monitoring vs. point-in-time assessments
- **Cost Reduction:** Eliminates manual evidence collection, saving 200+ hours per audit
- **Risk Visibility:** Executive dashboards show compliance posture at a glance

Risk Mitigation

Prevents compliance violations, identifies control gaps before audits, ensures evidence availability, and reduces audit findings and remediation costs.

GRC Mapping

Compliance Frameworks

- **COBIT 2019:** APO13 (Manage security), DSS05 (Manage security services)

- **ISO 27001:** A.18.1 (Compliance with legal requirements), A.18.2 (Information security reviews)
- **NIST CSF:** ID.GV-3 (Legal and regulatory requirements), PR.IP-1 (Baseline configuration)
- **ITIL v4:** Service validation and testing

Security Controls Implemented

- Automated compliance assessments
- Continuous control monitoring
- Audit trail and evidence collection
- Configuration compliance checking
- Automated remediation workflows

Audit Evidence

- Compliance assessment reports
- Control effectiveness evidence
- Configuration snapshots and change logs
- Remediation records and timelines

Regulatory Alignment

- **SOX:** Section 404 (Internal controls assessment)
- **PCI DSS:** Requirement 11.3 (Penetration testing), Requirement 12.9 (Service provider compliance)
- **HIPAA:** § 164.308(a)(8) (Evaluation of security measures)
- **SOC 2:** All trust service criteria