

IAM: Security Best Practices & Auditing

What are IAM best practices for a DevOps engineer?

- ✓ **Use least privilege** give only required permissions.
 - **Enable MFA** for root and IAM users.
 - O W Use roles, not users, for services and automation.
 - **Avoid using root account** keep it locked down.
 - Rotate access keys regularly.
 - Use IAM policies with conditions (like IP, time).

 - Delete unused users, roles, policies.
 - Monitor with CloudTrail and IAM Access Analyzer.
 - **Avoid wildcard ("*") permissions** in production. (LEAST Privilege)
 - **Q** Review permissions regularly (every 3–6 months).

How do you audit IAM activity?

Enable AWS CloudTrail - captures all IAM actions.

Purpose:

CloudTrail is AWS's logging service that records all API calls (including IAM actions) made in your AWS account.

Use Cases:

- Track who created/deleted users, roles, policies.
- Audit compliance (SOC2, ISO27001, etc.)
- Investigate incidents (e.g., "Who gave full admin to this user?").

Example:

Someone created a new IAM user with console access. CloudTrail records the CreateUser and CreateLoginProfile events.



💬 💻 Use CloudTrail logs to see who did what, when.

Purpose:

Provides visibility into user actions and timestamps, helping with traceability and accountability.

Use Cases:

- Investigate a data leak by seeing which user accessed an S3 bucket.
- Confirm who rotated a key or changed a password.
- Reconstruct timelines during a breach investigation.

Example:

A user accidentally deleted an EC2 instance. You can check CloudTrail to see when and who ran TerminateInstances.



Filter IAM actions like CreateUser, AttachRolePolicy, etc.

Purpose:

Focus your investigation or audit on specific sensitive IAM events.

Use Cases:

- Audit all AttachUserPolicy or PutRolePolicy actions to detect policy tampering.
- Track when someone added permissions to a role or user.

Example:

Filter CloudTrail for AttachUserPolicy to see all instances where AdminAccess was granted.

III Use AWS CloudTrail Lake or Athena to query logs.

Purpose:

Query logs using SQL without downloading huge JSON files. Makes complex audits fast and efficient.

Use Cases:

- Find all users who performed iam: UpdateAssumeRolePolicy in the past 30 days.
- Get a list of IAM actions performed by a specific IP or service.

Example:

Query Athena to find all IAM users created in the last 60 days.



✓ Enable IAM Access Analyzer – shows unused permissions and risky access.

Purpose:

Helps you detect over-permissioned users/roles and external access risks.

Use Cases:

- Identify roles with permissions not used in the last 90 days.
- Detect if any resource (like S3) is accessible by external accounts or the public.

Example:

You find that a role has ec2: * access, but has only ever used DescribeInstances. You can remove the extra permissions.



Set up Access Advisor – shows last used services per IAM user/role.

Purpose:

Part of the IAM Console – shows **last accessed timestamps** for services per identity.

Use Cases:

- Clean up permissions for roles/users that haven't used a service in months.
- Decommission unused accounts.

Example:

User1 hasn't accessed AWS Glue in 6 months. Revoke Glue-related permissions.



⚠ Use AWS Config – to track IAM resource changes over time.

Purpose:

AWS Config provides a timeline of changes to IAM resources, tracks compliance with custom or AWS-defined rules.

Use Cases:

- Detect when a user was granted elevated privileges.
- Roll back or audit config changes to IAM roles/policies.

Example:

Track when a managed policy was edited and by whom.



Set up CloudWatch Alarms – for sensitive actions (e.g., DeleteUser).

Purpose:

Real-time alerts for high-risk IAM actions.

Use Cases:

- Get notified when someone deletes a user or policy.
- Detect policy escalations (e.g., a user granting themselves Admin access).

Example:

You set up an alarm on DeleteUser. If someone deletes an IAM user, you get an email/SNS alert immediately.

11 Review activity monthly or quarterly.

Purpose:

Regular audits ensure ongoing security and least privilege, help meet compliance.

Use Cases:

- Quarterly review of all IAM roles and their last used services.
- Validate that users who left the organization have been removed.

Example:

In your quarterly audit, you find a test role created 6 months ago that's still active with high privileges. You remove it.

Summary Table

Tool/Feature	What It Does	Common Use Case
CloudTrail	Logs IAM/API actions	Forensics, auditing
CloudTrail + Filter	Narrow down on specific IAM events	Security review
Athena/CloudTrail Lake	Query logs using SQL	Fast investigation
IAM Access Analyzer	Detect risky/unused access	Least privilege
IAM Access Advisor	Show last-used services per role/user	Permissions cleanup
AWS Config	Track IAM resource changes	Audit trail
CloudWatch Alarms	Real-time alerts on IAM changes	Security alerting
Periodic Review	Scheduled manual audit	Governance & compliance

How do you use IAM Access Analyzer to ensure least privilege?

Here's how to use IAM Access Analyzer to ensure least privilege

- Q Access Analyzer scans IAM roles and policies in your account.

- **Find unused permissions** for roles and users.
- Helps you remove extra permissions not being used.
- **to a serior of the line of**
- Download report, remove permissions not in use for 90 days.
- **X** Use it when **writing or editing policies** test them before applying.
- **P** Great tool to **tighten access** without breaking functionality.

Q1: Which of the following is a good IAM best practice?

- A. Use root user for all deployments
- B. Grant full admin access to everyone
- C. Use least privilege for all users and roles
- D. Avoid using roles and use access keys everywhere
- **✓** Correct Answer: C

How do you audit IAM activity?

Q2: What tool helps you track IAM actions like CreateUser or AttachPolicy?

- A. EC2 Dashboard
- B. AWS CloudTrail
- C. Amazon S3
- D. CloudFront

✓ Correct Answer: B

How does IAM Access Analyzer help with least privilege?

Q3: What can IAM Access Analyzer be used for?

- A. Encrypt IAM policies
- B. Identify unused permissions and external access
- C. Auto-create admin users
- D. Launch EC2 instances
- **✓** Correct Answer: B