



IAM Reports



Introduction

- 1 AWS IAM reports are documents generated within the AWS IAM framework that offer insights into the configuration, usage, and security of IAM resources within an AWS account.
 - 2 These reports are instrumental for auditing, compliance, and security management purposes.
 - 3 They typically include details about
 - 1 User credentials
 - 2 Permissions
 - 3 Policy usage
 - 4 Access patterns across the AWS services and resources
 - 4 Three primary types of IAM reports are
 - 1 IAM Credential Report
 - 2 IAM Access Advisor Report
 - 3 AWS IAM Access Analyzer
-
- 1 Purpose Provides an overview of IAM user credentials status within an AWS account.
 - 2 Content Includes details on passwords, access keys, MFA devices, and when they were last used.
 - 3 Frequency Can be generated on demand from the AWS Management Console
 - 4 Scope Covers all IAM users in the AWS account
 - 5 Use Cases Helps in auditing for compliance and security best practices.
 - 6 Security Status Indicates if passwords or access keys are active, expired, or not used within a specified period.
 - 7 MFA Information Shows which users have MFA enabled, enhancing security posture.
 - 8 Last Activity Reports the time since the user last accessed AWS services
 - 9 Format Available in downloadable CSV format for easy analysis and reporting
 - 10 Access Accessible by AWS account administrators from the IAM dashboard.
 - 11 No Additional Cost Included with AWS IAM at no extra charge

3

4

34

44