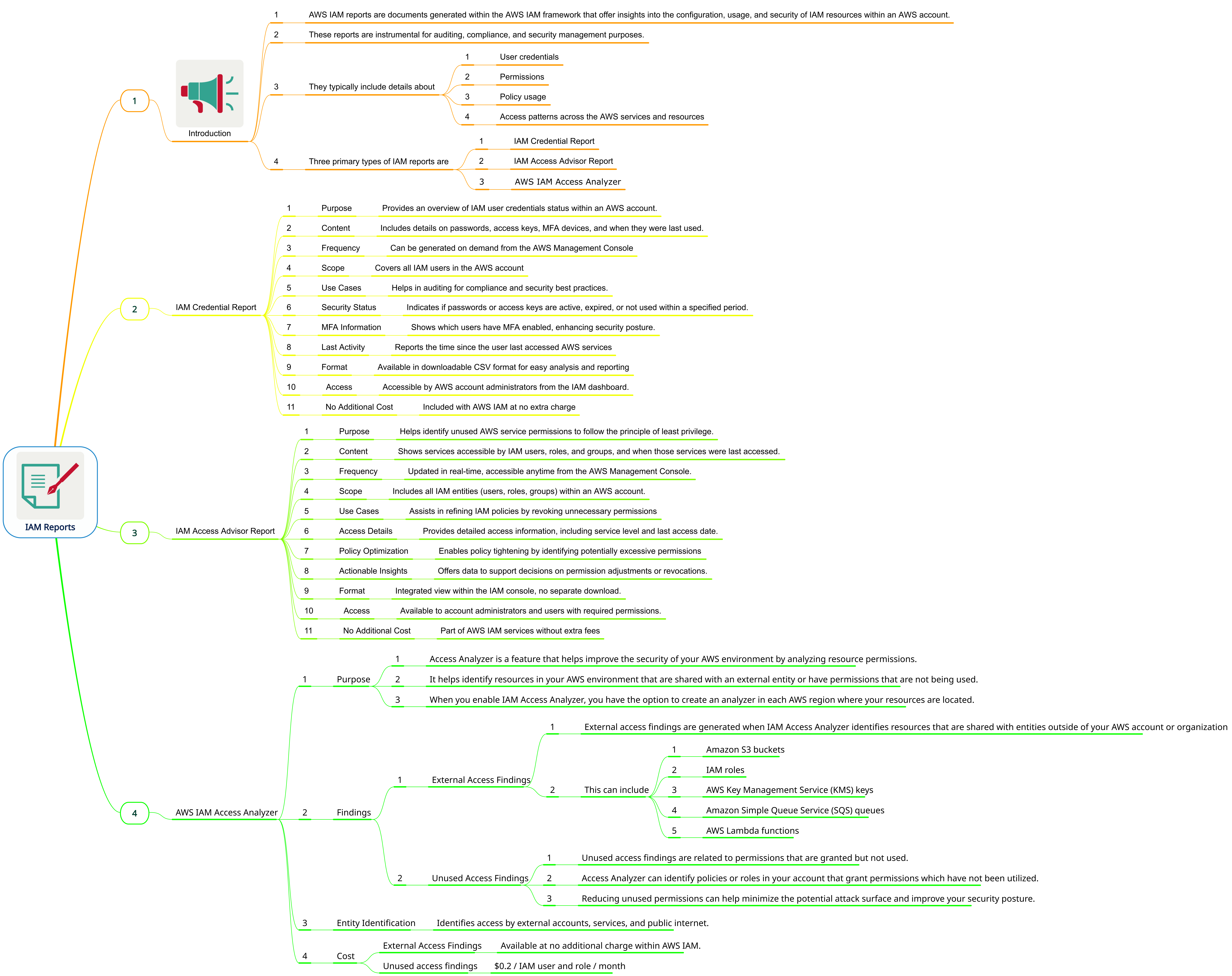

IAM Reports

- 1 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
- 2 IAM Credential Report
  - 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 IAM Access Advisor Report
  - 1 Purpose — Helps identify unused AWS service permissions to follow the principle of least privilege.
  - 2 Content — Shows services accessible by IAM users, roles, and groups, and when those services were last accessed.
  - 3 Frequency — Updated in real-time, accessible anytime from the AWS Management Console.
  - 4 Scope — Includes all IAM entities (users, roles, groups) within an AWS account.
  - 5 Use Cases — Assists in refining IAM policies by revoking unnecessary permissions
  - 6 Access Details — Provides detailed access information, including service level and last access date.
  - 7 Policy Optimization — Enables policy tightening by identifying potentially excessive permissions
  - 8 Actionable Insights — Offers data to support decisions on permission adjustments or revocations.
  - 9 Format — Integrated view within the IAM console, no separate download.
  - 10 Access — Available to account administrators and users with required permissions.
  - 11 No Additional Cost — Part of AWS IAM services without extra fees
- 4 AWS IAM Access Analyzer
  - 1 Purpose
    - 1 Access Analyzer is a feature that helps improve the security of your AWS environment by analyzing resource permissions.
    - 2 It helps identify resources in your AWS environment that are shared with an external entity or have permissions that are not being used.
    - 3 When you enable IAM Access Analyzer, you have the option to create an analyzer in each AWS region where your resources are located.
  - 2 Findings
    - 1 External Access Findings
      - 1 External access findings are generated when IAM Access Analyzer identifies resources that are shared with entities outside of your AWS account or organization
      - 2 This can include
        - 1 Amazon S3 buckets
        - 2 IAM roles
        - 3 AWS Key Management Service (KMS) keys
        - 4 Amazon Simple Queue Service (SQS) queues
        - 5 AWS Lambda functions
    - 2 Unused Access Findings
      - 1 Unused access findings are related to permissions that are granted but not used.
      - 2 Access Analyzer can identify policies or roles in your account that grant permissions which have not been utilized.
      - 3 Reducing unused permissions can help minimize the potential attack surface and improve your security posture.
  - 3 Entity Identification — Identifies access by external accounts, services, and public internet.
  - 4 Cost
    - External Access Findings — Available at no additional charge within AWS IAM.
    - Unused access findings — $0.2 / IAM user and role / month