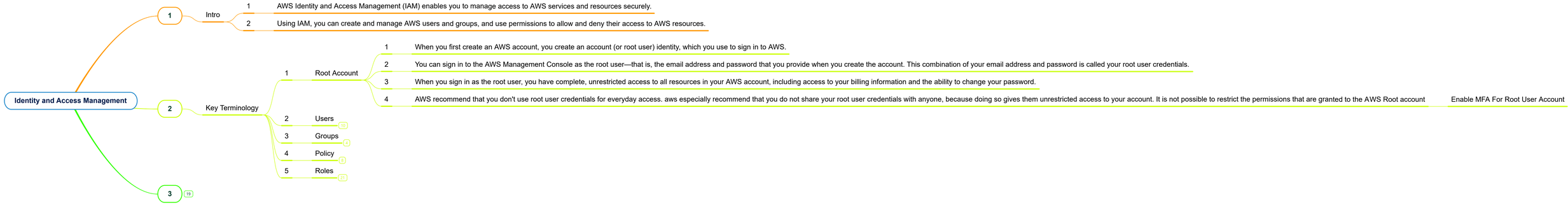
Identity and Access Management
1
Intro
1
AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely.
2
Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.
2
Key Terminology
1
Root Account
1
When you first create an AWS account, you create an account (or root user) identity, which you use to sign in to AWS.
2
You can sign in to the AWS Management Console as the root user—that is, the email address and password that you provide when you create the account. This combination of your email address and password is called your root user credentials.
3
When you sign in as the root user, you have complete, unrestricted access to all resources in your AWS account, including access to your billing information and the ability to change your password.
4
AWS recommend that you don't use root user credentials for everyday access. aws especially recommend that you do not share your root user credentials with anyone, because doing so gives them unrestricted access to your account. It is not possible to restrict the permissions that are granted to the AWS Root account
Enable MFA For Root User Account
2
Users
10
3
Groups
4
4
Policy
8
5
Roles
21
3
19