AWS IAM

- IAM -Identity and Access Management and global Service
- Root account create default

Permissions:

- User or groups can be assigned JSON document called policies
- These policies define the permissions of the users
- AWS you apply the least privilege principle: Don't give more permission than a user need

AWS Access:

-Three Way Access:

1. AWS Console: Protected by Password + MFA
2. AWS CLI : Protected By access key
3. AWS Software Developer Kit (SDK): For code : Protected By Access Keys

Security Tools

- IAM Credentials Report
    - List all account user their status of various credentials
- IAM Access Advisor
    - Which permission to user and last used

IAM Guideline And Best Practices

- Don't use the root account Except for AWS account setup
- One Physical user = One AWS user
- Assign users to Groups And Assign permission to group
- Create a strong password policy
- Use and enforce the use of MFA
- Create role for giving permission to AWS service
- Use access keys for Programmatic Access (CLI/SDK)
- Audit permission of your account with the IAM Credential Report
- NEVER share IAM users & Access Keys

Share Responsibility Model for IAM

AWS	YOU
• Infrastructure(Global Net. security) • Configuration and Vulnerability analysis • Compliance Validation	User, Group, Roles, Policies management and monitoring, Enable MFA on all account, Rotate all yours keys often, Use IAM tools to apply appropriate permissions, analyse access patterns & review permissions

AWS IAM Summary

1. **User**: Mapped to a physical user, has a password for AWS console
2. **Groups**: Contains user only
3. **Policies** : Json document that outlines permissions for User or Groups
4. **Roles**: For EC2 Instance or AWS services
5. **Security**: MFA + Password Policy
6. **Access Keys:** Access AWS using the CLI Or SDK
7. **Audit**: IAM credential Reports and IAM Access Advisor