AWS Certified Solutions Architect: Associate - 6.0 Identity and Access Management

filename: amazon-acsaa-6-1-elb_and_auto_scaling
Title: Identity and Access Management
Subtitle: AWS Certified Solutions Architect: Associate

6.1 Identity and Access Management

- IAM
    - Provides permissions and access to AWS resources
    - Does not provide the same for applications or OS deployments
- Principles
    - Root User
        - Initial user account in AWS
        - Username/Password
        - MFA optional
    - IAM User
        - Additional users added to the account
    - Roles / Temporary Security Tokens
        - Grant permissions to an application
        - Can also grant access to:
            - An instance
            - An IAM user from another AWS account (cross-account access)
            - A foreign trusted credential (federation)
    - Groups
        - Grant permissions to a user
- Authentication (Diagram)
    - Username/Password
    - Access Key
    - Access Key + Session Token
- Authorization
    - Policies
        - Effect
            - Allow or Deny
        - Action
            - Specific action being allowed
            - Varies by service
        - Condition
            - Additional criteria that must be met
            - IP Address, Time interval, etc.
        - Resource
            - Specific infrastructure as indicated by an ARN
    - Amazon Resource Name
        - `arn:aws:service:region:account-id:[resourcetype:]resource`
        - `arn:aws:s3:us-east-1:123456789012:my_corporate_bucket/*`
        - `arn:aws:iam:us-east-1:123456789012:user/David`
        - `arn:aws:dynamodb:us-east-1:123456789012:table/tablename`
    - Applying policies
        - User Policies
            - Created directly on a user
        - Managed Policies
            - Created independently and then attached
            - Can be re-used
- Other Features
    - Multi-factor Authentication (MFA)
        - Can be assigned to individual IAM accounts
    - Rotating Keys
        - Create and deploy a new key prior to disabling the old key
    - Multiple Permissions
        - `Deny` always overrides
        - Otherwise, permissions are combined
        - Finally, a defaul `Deny all` applies