AWS Certified Solutions Architect: Associate - 12.0 Security on AWS

File Name: amazon-acsaa-12-2-account_security

Title: Account Security

Subtitle: AWS Certified Solutions Architect: Associate

12.2 Account Security

- AWS Credentials
    - Passwords
        - Uses
            - AWS Root Account
            - Other User Accounts
        - Up to 128 characters
        - Password policies can be defined
            - Key expiration
    - Multi-Factor Authentication
        - Uses
            - AWS Root Account
            - Other User Accounts
            - IAM Role Access between accounts
        - Can also be implemented on APIs
        - Generally requires the use of a software MFA
        - RFC 6238 Time-Based One-Time Password (TOTP)
    - Access Keys
        - Uses
            - API Requests
            - SDK/CLI Access
        - Used to digitally sign API calls
        - Hashed Message Authentication Mode (HMAC)-Secure Hash Algorithm (SHA)-256
        - Keys can be compromised
        - Roles are typically better as their access is temporary
    - Key Pairs
        - Uses
            - SSH access to EC2
            - CloudFront Signed URLs
        - RSA 2048 SSH keys
    - X.509 Certificates
        - SSL for use with HTTPS
        - Digitally signed SOAP requests
- AWS CloudTrail
    - Logs access
    - Stores logs in S3
        - The name of the API
        - The identity of the caller
        - The time of the API call
        - The request parameters
        - The response elements returned by the AWS Cloud service
    - Log file integrity
        - SHA-256 for hashing
        - SHA-256 with RSA for digital signing
        - Computationally unfeasible to modify, delete, or forge AWS CloudTrail log files without detection.