AWS Certified Solutions Architect: Associate - 11.0 Additional Key Services

File Name: amazon-acsaa-11-2-security_services

Title: Security Services

Subtitle: AWS Certified Solutions Architect: Associate

11.2 Security Services

Security

- AWS Directory Service
  - Fully managed solution
  - Multi-AZ
  - Monitored so that failed DCs are replaced automatically
  - Snapshots taken automatically
  - Three directory types
    - AWS Directory Service for Microsoft Active Directory
      - Managed Microsoft AD
      - Allows for integration with AWS applications
      - Can build a trust with private existing AD
      - Best choice for 5,000+ users or trust is required
    - Simple AD
      - Microsoft AD compatible solution
      - Samba 4
      - Supports most of the functions of MS AD
      - Cannot build trust relationships
      - Can use IAM to control access to the console
      - Best choice for less that 5,000 users and only basic functions required
    - AD Connector
      - Proxy that forwards sign-on requests to your existing DCs
      - No federation/trust required
      - Allows for management to take place like normal
      - Best choice if you want to retain your existing configuration and processes
- AWS Key Management Service and Cloud HSM
  - AWS KMS
    - Provides full lifecycle of key management
    - Secure keys can be generated in the cloud
      - Unable to be exported
    - Customer Managed Key (CMK)
      - CMKs can only encrypt up to 4KB of data
      - Used to encrypt *data keys* that can, in-turn, encrypt everything else
      - CMKs cannot be exported from AWS
    - Data Key
      - Used to encrypt data
      - CMK can generate as many DKs as needed
      - DK's private key is encrypted by the CMK
      - The CMK is called to decrypt the DK's private key as needed
        - Referred to as *envelope encryption*
  - AWS CloudHSM (Diagram)
    - Makes Hardware Security Modules available in the cloud
    - HSMs are designed to securely store keys behind a hardware boundary
    - Usually deployed in pairs for redundancy
    - Keys are stored in accordance with a number of standards
    - Useful for achieving PCI compliance
- AWS CloudTrail
  - Records API calls made on an AWS account
  - Creates a record used for auditing
  - Data recorded
    - Name of the API
    - Identity of the caller
    - Time of the call
    - Request parameters

    - Response elements returned to the caller
- Two types of trails
    - A Trail that Applies to all Regions
        - Default option
        - Log files are stored in an S3 bucket
        - Optionally can store in a CloudWatch log group
    - A Trail that Applies to One Region
- Useful for compliance audits and tracking unauthorized access