AWS Certified Solutions Architect: Associate - 12.0 Security on AWS

File Name: amazon-acsaa-12-1-security_on_aws

Title: Security on AWS

Subtitle: AWS Certified Solutions Architect: Associate

12.1 Security on AWS

Compliance

- Shared responsibility model (Diagram)
- [AWS Compliance Program](#)

Infrastructure Security

- Physical and Environmental Security
  - Fire Detection and Suppression
    - Smoke detection
    - Multiple Sprinkler Types
      - Wet-pipe
      - Double-interlocked pre-action
      - Gaseous
  - Power
    - Fully redundant
    - UPS
    - Generators
  - Climate and Temperature
    - Climate controlled by automated systems and by personnel
  - Management
    - AWS staff monitors the infrastructure 24/7
  - Storage Device Decommissioning
    - Performed in a secure manner
    - Does not allow data to "leak"
  - Business Continuity Management
    - Managed by the Amazon Infrastructure Group
    - Designs for resiliency and carries out recovery if needed
  - Availability (Diagram)
    - Multi-AZ
      - Physically separate
      - UPS and backup generators
      - Multiple tier-1 network transit providers
    - Multi-Region
  - Incident Response
    - Staffed 24/7
    - [Service Health Dashboard](#)
  - Network Security
    - Many services available
      - Security Groups
      - Network ACLs
    - Some rules managed by Amazon Information Security
    - Remainder are left to the customer
  - Secure Access Points
    - API endpoints are secured with HTTPS
    - Heavily secured and monitored
    - Redundant dedicated edge hardware
    - GovCloud SSL Load Balancers are FIPS 140-2 compliant
  - Transmission Protection
    - SSL
    - VPC
    - IPSec VPN
  - Network Monitoring
    - DDoS Mitigation
    - Man in the Middle Attack Mitigation
      - SSH certificate authentication
    - Port Scanning
      - Detected, stopped and blocked
    - Packet Sniffing
      - Promiscuous mode is allowed, but the hypervisor

will not provide other traffic
- Best practice is to encrypt anyway