AWS Certified Solutions Architect: Associate - 12.0 Security on AWS

File Name: amazon-acsaa-12-3-cloud_service_specific_security

Title: Cloud Service-Specific Security

Subtitle: AWS Certified Solutions Architect: Associate

12.3 Cloud Service-Specific Security

- Compute Services (EC2)
  - Multiple levels of security (Diagram)
    - OS of the Host
    - OS of the Guest
    - Firewall
    - Signed API Calls
  - Hypervisor
    - Xen running on Linux
    - Guest OS does not have privileged access to the CPU
      - Ring 0: Host OS
      - Ring 1: Guest OS
      - Ring 3: Applications
  - Instance Isolation
    - Separation provided by Xen
    - Amazon firewall in place between physical and virtual interfaces
      - All traffic passes through the firewall
    - Disk access is entirely virtualized
    - RAM and Disk are reset prior to reprovisioning
  - Host OS
    - Administrators are required to use MFA
    - Access is removed immediately upon task completion
  - Guest OS
    - Controlled by you
    - Should be hardened according to vendor specifications
  - Firewall (Diagram)
    - Firewall is mandatory
    - Can be disabled with loose rules
    - Should provide minimal access
  - API Access
    - API calls to instances are all signed by an access key
    - Can also be encrypted with SSL
  - EBS Security
    - Access to an EBS volume can be controller with IAM policies
    - EBS volumes have redundant replicas
      - Replicas are stored in the same AZ
    - Should be backed up to S3 or replicated from within the guest
      - DB replication
      - rsync
    - EBS volumes and snapshots can be encrypted with AES-256
      - Not available in lower-CPU instances
- Networking
  - ELB Security
    - Supports end-to-end encryption with TLS
    - Can take over TLS workload
    - Uses a predefined cypher-set
      - PCI, SOX, etc may require a specific cypher
      - Advanced options are available
      - Service order can be specified
    - Perfect Forward Secrecy (PFS) is supported
    - ELB access logs can be more accurate than server logs
  - Virtual Private Cloud (Diagram)
    - Isolated networks using RFC1918 subnets
    - API access must be digitally signed (SSL optional)
    - MAC spoofing and ARP spoofing are automatically blocked
    - All traffic is passed through the routing table
    - Provides support for Network ACLs (Diagram)
      - Can be used in conjunction with Security Groups
    - Virtual Private Gateway

        - Internet Gateway
            - Alternate AMIs can be used to provide DPI
        - Dedicated instances can be used within a VPC also
- S3 Security
    - Data Access Controls
        - IAM Policies (and conditions)
        - Bucket Policies
        - ACLs
        - Query String Authentication
            - Pre-signed URLs
    - Data transfers can be encrypted with SSL
    - SSE can be used for data at rest
        - AES-256
    - Access-logs
    - Cross-Origin Resource Sharing (CORS)
        - Policy can be defined on each bucket
- Database Security
    - DynamoDB
        - IAM policies for access control
        - Multi-AZ backups are performed automatically
        - AWS PipeLine can be used for Multi-Region
    - RDS
        - Much the same as EC2
            - VPC
            - SSL
            - Multi-AZ
            - Snapshots
        - Master user account
        - Internal user accounts
        - Replication
            - Replicas are not backups
        - Automatic software patching
            - Maintenance window
            - Multi-AZ minimizes the impact
    - RedShift
        - Much the same
        - Supports using HSM to store the cluster key
- Application Services
    - Amazon SQS
        - Durability is built into the service
        - IAM
            - By default access is only granted to the user who created the queue
        - SQS Access Policy
        - Encryption
            - Not directly supported
            - Message data should be encrypted prior to submitting
    - Amazon SNS
        - IAM
        - HTTPS
        - Some communications methods are inherently insecure (email)
- Analytics Services
    - Elastic Map Reduce
        - Cluster is secured with a key
        - IAM can control access
        - The cluster key can control access
        - EMR clusters are hidden from other IAM users by default
        - VPCs can isolate the clusters
        - Data can be encrypted prior to loading
            - Requires a decrypt step before working with the data
    - Kinesis
        - IAM for access
        - IAM roles are recommended as applications normally perform analystics
        - SSL is required for API access
            - https://kinesis.us-east-1.amazonaws.com
- Deployment and Management Services
    - IAM Roles
        - Federated (Non-AWS) user access
        - Security Assertion Markup Language (SAML) 2.0
        - Cross-Account access
        - Applications in EC2 that need access to other

resources (S3, DynamoDB, etc)

- Mobile Services
  - Amazon Cognito Security
    - Authenticates users and syncs their data across multiple platforms
    - Works with Amazon, Google, Facebook, etc.
    - Uses OAuth or OpenID Connect tokens
    - Individual accounts are not necessary
      - Create an identity pool
      - Assign an IAM Role to the pool
      - Users are assigned an identity when logging in
      - Their access is determined by the role
- Applications
  - Amazon WorkSpaces
    - Domain authentication (local/remote)
    - MFA is supported through RADIUS
    - VPCs can be used to isolate instances
    - Persistent EBS storage is backed up twice a day
    - Windows Update is on by default
    - IAM can only manage the instance itself, not the guest OS