AWS Certification – Security & Identity Services – Cheat Sheet

IAM

- securely control access to AWS services and resources
- helps create and manage user identities and grant permissions for those users to access AWS resources
- helps create groups for multiple users with similar permissions
- not appropriate for application authentication
- is Global and does not need to be migrated to a different region
- helps define Policies,
    - in JSON format
    - all permissions are implicitly denied by default
    - most restrictive policy wins
- IAM Role
    - helps grants and delegate access to users and services without the need of creating permanent credentials
    - IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to make AWS API calls
    - needs Trust policy to define who and Permission policy to define what the user or service can access
    - used with Security Token Service (STS), a lightweight

  web service that provides temporary, limited privilege credentials for IAM users or for authenticated federated users
  - IAM role scenarios
    - Service access *for e.g. EC2 to access S3 or DynamoDB*
    - Cross Account access for users
      - with user within the same account
      - with user within an AWS account owned the same owner
      - with user from a Third Party AWS account with External ID for enhanced security
    - Identity Providers & Federation
      - Web Identity Federation, where the user can be authenticated using external authentication Identity providers like Amazon, Google or any OpenId IdP using AssumeRoleWithWebIdentity
      - Identity Provider using SAML 2.0, where the user can be authenticated using on premises Active Directory, Open Ldap or any SAML 2.0 compliant IdP using AssumeRoleWithSAML
      - For other Identity Providers, use Identity Broker to authenticate and provide temporary Credentials using AssumeRole (recommended) or GetFederationToken
- IAM Best Practices

    - Do not use Root account for anything other than billing
    - Create Individual IAM users
    - Use groups to assign permissions to IAM users
    - Grant least privilege
    - Use IAM roles for applications on EC2
    - Delegate using roles instead of sharing credentials
    - Rotate credentials regularly
    - Use Policy conditions for increased granularity
    - Use CloudTrail to keep a history of activity
    - Enforce a strong IAM password policy for IAM users
    - Remove all unused users and credentials

CloudHSM

- provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud
- single tenant, dedicated physical device to securely generate, store, and manage cryptographic keys used for data encryption
- are inside the VPC (not EC2-classic) & isolated from the rest of the network
- can use VPC peering to connect to CloudHSM from multiple VPCs
- integrated with Amazon Redshift and Amazon RDS for Oracle
- EBS volume encryption, S3 object encryption and key management can be done with CloudHSM but requires custom application scripting

- is NOT fault tolerant and would need to build a cluster as if one fails all the keys are lost
- expensive, prefer AWS Key Management Service (KMS) if cost is a criteria

AWS Directory Services

- gives applications in AWS access to Active Directory services
- different from SAML + AD, where the access is granted to AWS services through Temporary Credentials
- Simple AD
    - least expensive but does not support Microsoft AD advance features
    - provides a Samba 4 Microsoft Active Directory compatible standalone directory service on AWS
    - No single point of Authentication or Authorization, as a separate copy is maintained
    - trust relationships cannot be setup between Simple AD and other Active Directory domains
    - Don’t use it, if the requirement is to leverage access and control through centralized authentication service
- AD Connector
    - acts just as an hosted proxy service for instances in AWS to connect to on-premises Active Directory
    - enables consistent enforcement of existing security policies, such as password expiration, password history, and account lockouts, whether users are accessing resources on-premises or in the AWS cloud
    - needs VPN connectivity (or Direct Connect)

    - integrates with existing RADIUS-based MFA solutions to enabled multi-factor authentication
    - does not cache data which might lead to latency
- Read-only Domain Controllers (RODCs)
    - works out as a Read-only Active Directory
    - holds a copy of the Active Directory Domain Service (AD DS) database and respond to authentication requests
    - they cannot be written to and are typically deployed in locations where physical security cannot be guaranteed
    - helps maintain a single point to authentication & authorization controls, however needs to be synced
- Writable Domain Controllers
    - are expensive to setup
    - operate in a multi-master model; changes can be made on any writable server in the forest, and those changes are replicated to servers throughout the entire forest

AWS WAF

- is a web application firewall that helps monitor the HTTP/HTTPS requests forwarded to CloudFront and allows controlling access to the content.
- helps define Web ACLs, which is a combination of Rules, which is a combinations of Conditions and Action to block or allow
- Third Party WAF
    - act as filters that apply a set of rules to web traffic to cover exploits like XSS and SQL injection and also

help build resiliency against DDoS by mitigating HTTP GET or POST floods

- WAF provides a lot of features like OWASP Top 10, HTTP rate limiting, Whitelist or blacklist, inspect and identify requests with abnormal patterns, CAPTCHA etc
- a WAF sandwich pattern can be implemented where an autoscaled WAF sits between the Internet and Internal Load Balancer