AWS STS – Security Token Service

- Allows to grant limited and temporary access to AWS resources.
- Token is valid for up to one hour (must be refreshed)
- Assume Role
  - Within your own account: for enhanced security
  - Cross Account Access: assume role in target account to perform actions there
- Assume Role With SAML
  - return credentials for users logged with SAML
- Assume Role with Web Identity
  - return creds for users logged with an IdP (Facebook Login, Google Login, OIDC compatible…)
  - AWS recommends against using this, and using Cognito instead
- Get Session Token
  - for MFA, from a user or AWS account root user

Create a IAM role -- > Define principles which can access this role -- > use AWS STS -- > Credentials available for 15 mins to 1 hour.

Links:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

Federation – External source of truth for validation [User Management is outside AWS]. So, we need that trusted third party source. E.g. SAML2.0

MS AD – s/w on windows server with AD Domain service .DB for all users

Directory service --

AWS Managed MS AD – Supports MFA

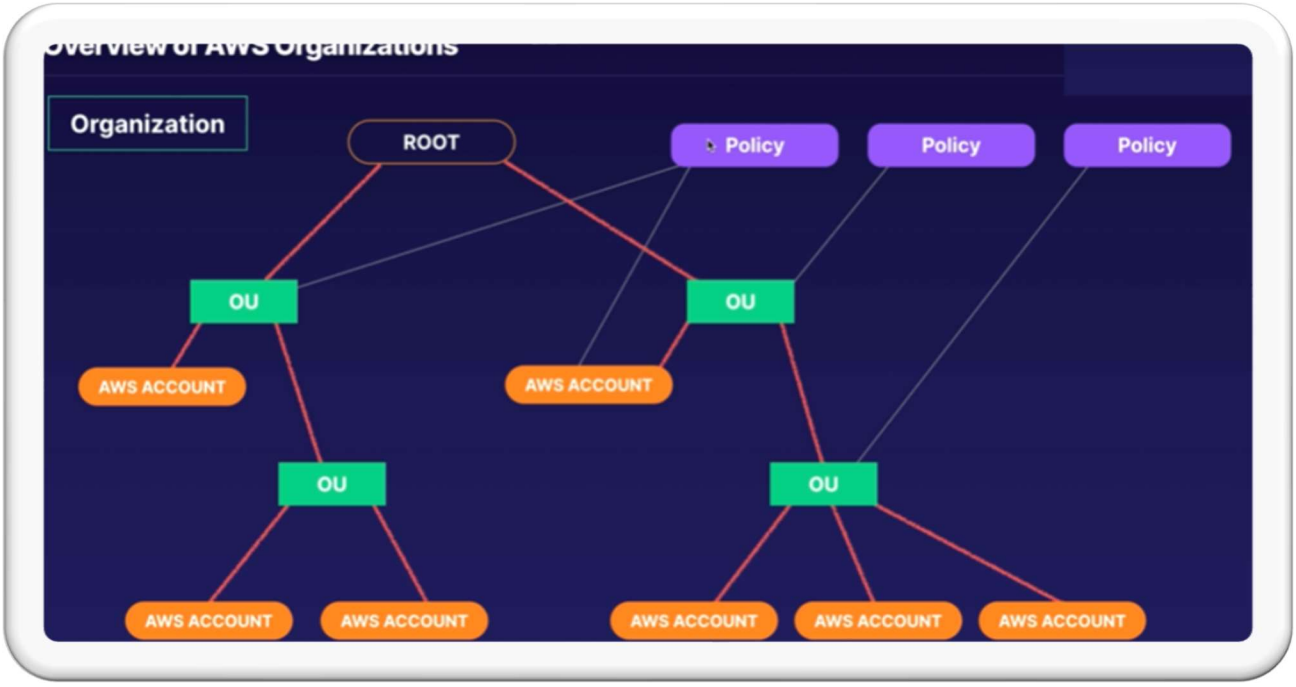
Simple AD – Standalone

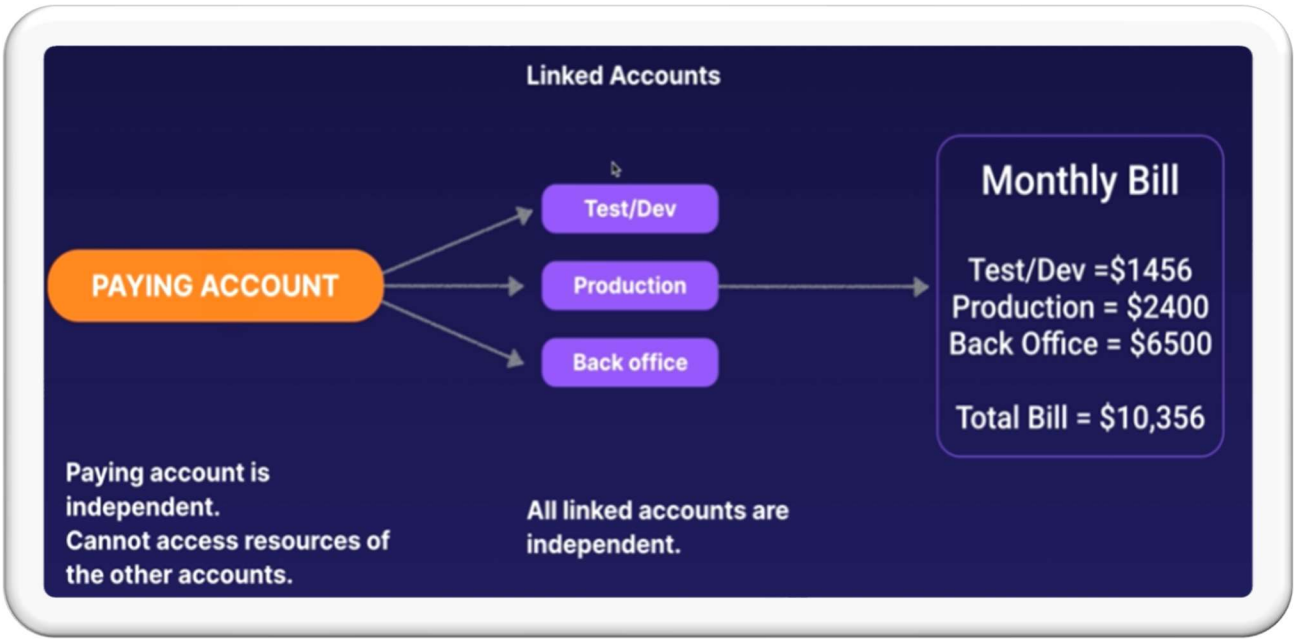
AD Connector – proxy connector

Amazon Cognito User pools

Questions like – cross account or assuming role.

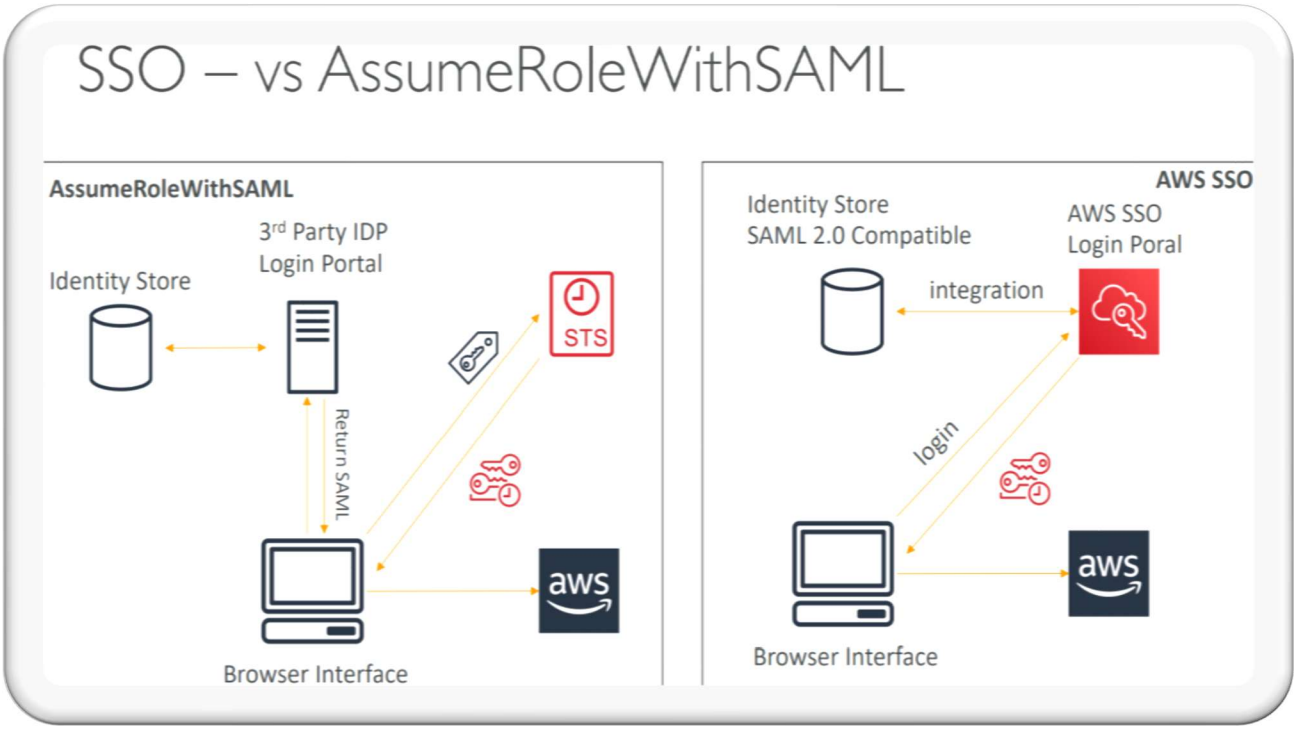
AWS Organization:





AWS SSO: (https://aws.amazon.com/blogs/security/introducing-aws-single-sign-on/)

Mange multiple accounts and third-party applications.



Cloud HSM (Hardware Security Module) is a way of encryption.

AWS - KMS manages the software for encryption but Cloud HSM just provisions encryption Dedicated Hardware and You manage your own encryption keys entirely (not AWS).

• HSM device is tamper resistant, FIPS 140-2 Level 3 compliance – No one even in AWS can touch your hardware.

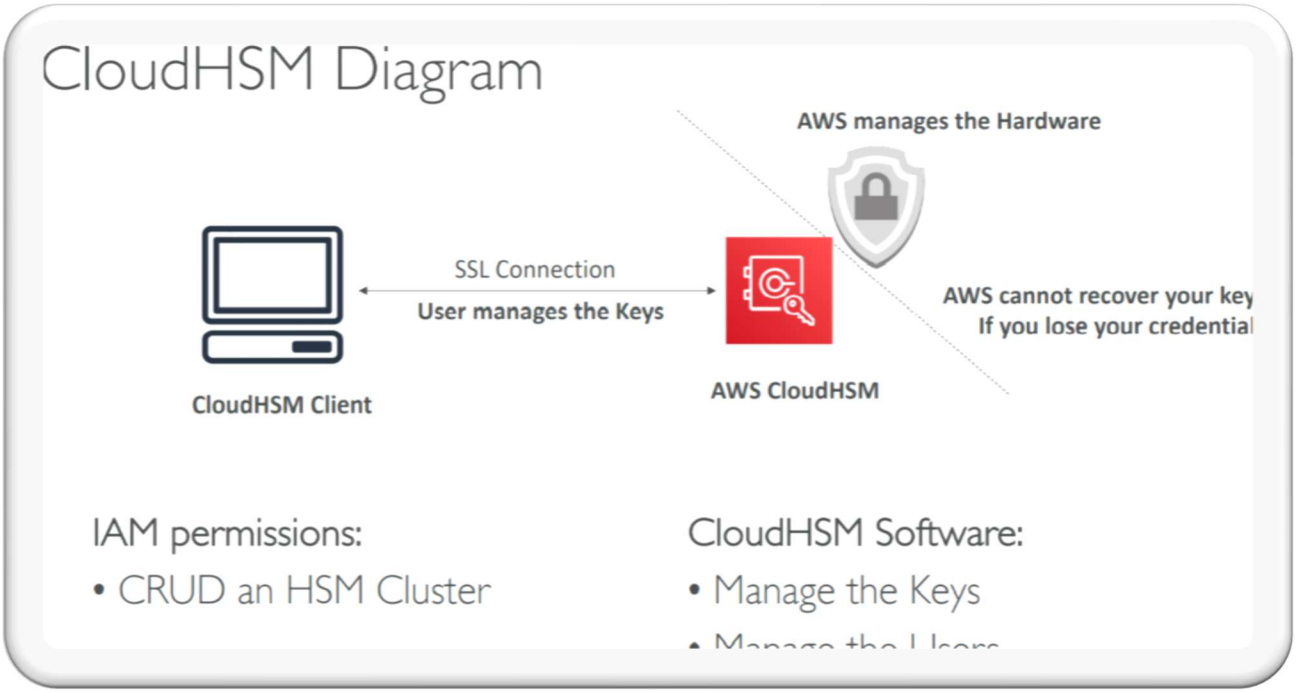
• CloudHSM clusters are spread across Multi AZ (HA) – must setup

• No free tier available

• Must use the CloudHSM Client Software

• Redshift supports CloudHSM for database encryption and key management

• Good option to use with SSE-C encryption



AWS Shield

- AWS Shield Standard:
  - Free service that is activated for every AWS customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other layer 3/layer 4 attacks
- AWS Shield Advanced:
  - Optional DDoS mitigation service ($3,000 per month per organization)
  - Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  - 24/7 access to AWS DDoS response team (DRP)
  - Protect against higher fees during usage spikes due to DDoS

Ddos attack - https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html

https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

https://www.cloudbric.com/blog/2015/03/reflection-attacks-and-amplification-atttacks/#:~:text=Reflection%20attacks%20(also%20known%20as,to%20that%20type%20of%20request.

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

$3000 per month.

AWS Guard Duty

----------–

Intelligent and Cloud scale managed threat detection service. Helps to manage any threat to your application.

Continuously does security monitoring service where it analyses and processes VPC Flow logs, AWS cloud event trail logs and DNS logs.

Flashes unexpected and potentially malicious activity on your AWS environment.

Where can you deploy WAF (Not included in free Tier)?

AWS WAF – Web Application Firewall

- Protects your web applications from common web exploits (Layer 7)
- Layer 7 is HTTP (vs Layer 4 is TCP)
- Deploy on Application Load Balancer, API Gateway, CloudFront

- Define Web ACL (Web Access Control List):
  - Rules can include: IP addresses, HTTP headers, HTTP body, or URI strings
  - Protects from common attack - SQL injection and Cross-Site Scripting (XSS)
  - Size constraints, geo-match (block countries)
  - Rate-based rules (to count occurrences of events) – for DDoS protection

AWS Firewall Manager

• Manage rules in all accounts of an AWS Organization

• Common set of security rules

• WAF rules (Application Load Balancer, API Gateways, CloudFront)

• AWS Shield Advanced (ALB, CLB, Elastic IP, CloudFront)

• Security Groups for EC2 and ENI resources in VP

AWS Config - console

Cognito – Managed service which provides authentication, authorization and user management for web and mobile application.

- Provides enhanced security
- Cross platform consistency
- Guest and social media logins
- MFA & password policy
- Marketing analysis

Two major components:

1. User pool – Directory for sign in and signup choices for application users.
2. Identity Pool – Grant access to other AWS services. Can be either used separately or together with user pool.