KMS, SSM Parameter Store, Shield, WAF

Encryption 101

Encryption in flight: Achieved via SSL, your connection to the web server is encrypted, so no one can man in the middle you and sniff the packet that you're sending to find sensitive data

SSL certificates is used to established the secure connection. Certificate is used to authenticate the other party.

Server-side encryption at rest: Done by encrypting the data in rest that's stored in the database. The encryption and decryption key must be stored and managed somewhere a key server. The server will talk to it to retrieve the key to do encryption and decryption. The data is decrypted before the data is sent back to the client.

Client side encryption: The data is encrypted by the client and never decrypted by the server. The data will be decrypted by the receiving client. Could leverage envelope encryption to do client side encryption.

KMS

Key management service. A service that will manage the encryption key for us. Used IAM for authorization the access to the keys that's stored in KMS.

Every key usage will be audited using CloudTrail! Which is very nice to track who used the key and when.

Don't store secrets in plaintext, this is very bad!

KMS keys

Symmetric (AES-256 keys): Single key used for encryption and decryption. All AWS service that integrated with KMS use symmetric keys.

Asymmetric (RSA & ECC key pair): Public and private key. Encrypt/decrypt, sign/verify operations. Used for encryption outside of AWS by users who can't call KMS API.

AWS can own keys and they are free. SSE-S3, SSE-SQS.

AWS Managed keys are also free, but only within service that they are assigned to

Customer managed keys: cost $1 / month. You will also pay for the API calls to KMS.

Keys will be automatically rotated every 1 year.

Key scopes

The keys are scoped per region. So other region cannot access the KMS key from another region. You would need snapshots to restore the snapshot with encryption enabled with another KMS key. **Same key cannot be used!!!**

Key policies

Default KMS key policy if you don't have one: it allows everyone in this account to have access to this key

Custom KMS key policy: You define users, role that have access to the KMS key. Can share KMS key via cross-account sharing, then you can copy encrypted snapshots across different accounts which is cool.

Multi-region keys

The same key is going to be replicated across multiple region. This is so that you can encrypt in one region and decrypt it in another region as well.

They are possible because of same key ID, key material, and automatic rotation.

Multi-region are not global! Each are managed independently, therefore, it is not recommended to use them. Use it only for global client-side encryption.

DynanoDB global table + multi-region keys + client-side encryption

This is so that you can encrypt specific column of the DynanoDB it will only be decrypted to specific client. Protection against even database admin.

Same concept can also applied to Aurora as well.

S3 Replication Encryption

For object encryption with SSE-KMS you need to enable it. You specify which key to encrypt with. You are allowed to replicate the encrypted S3 bucketto another target bucket using a different key.

Object encrypted with SSE-C are never replicated.

SS3-S3 are replicated by default.

Sharing encrypted AMI

To first share an AMI you have to modify the image attribute to let other AWS account use it too.

Then you also have to share the KMS key with the other user and have sufficient permission to use the key.

Then you can just launch the EC2 instances from the AMI that's encrypted, then they can create the same encrypted AMI with their own KMS keys.

SSM Parameter Store

System manager. A storage place for you to put secrets, password, and configuration files.

It is serverless scalable, durable, and have an easy SDK to use to retrieve and store those files.

You can have plaintext configuration or encryption of password and secret using KMS.

There is hierarchy for the parameter store just like a S3 bucket.

Standard and advanced parameter

Standard doesn't have parameter policies and is free to use.

Advance isn't free and can have parameter policies.

Parameter policy: Allow you to assign TTL to a parameter to force user to update or delete sensitive data like passwords. You can have multiple policies at a time.

AWS Secret Manager

Used for storing secrets. Different than SSM parameter store because it can force rotation of secrets every X days, and it can generate secrets on rotation using a Lambda function.

Secret can be encrypted using KMS. Integrates really well with RDS, Aurora, and PostgreSQL

Multi-region secrets

The secret can be replicated across regions, it will be kept in sync using read replicas with the primary secret.

Easy failover and promotion if one region fails.

AWS ACM

Certificate Manager. Let you get, manage, and deploy TLS certificates for HTTPS. This will give you in-flight encryption for your website.

ALB will be working with ACM to get the certificate for HTTPS. Supports both public and private TLS certificates.

Automatic TLS certificate renewal as well.

You cannot use ACM with EC2!

Process:

1. List out the domain names to include in the certificate for
2. DNS validation or email validation. DNS validation is preferred using CNAME record
3. The certificate will take few hours to get verified
4. Auto renewal

Importing public certificate

You can generate the certificate outside of ACM then import it, but this won't give you automatic certificate.

Can set up AWS Config to make sure the certificate is valid.

Or you can set up EventBridge for daily expiration events from ACM to invoke SNS notifications.

Integration with ALB

There will be a redirect to HTTPS when user visits HTTP, then it will leverage ACM to sent the certificate in order to establish a secure connection.

Integration with API Gateway

If you use Edge-optimized then TLS certificate must be in the same region as CloudFront which is `us-east-1`.

If you use Regional then TLS certificate must be in the same region as the API Gateway.

Web Application Firewall

Protect your web application from common web exploits at HTTP level. XSS.

Deploy on ALB, API Gateway, CloudFront, Cognito User Pool.

Set up Access Control List rules: To filter based on IP sets, only let those IP through. Filter based on HTTP body. geo-match to allow or block specific countries.

Rate-based rules to protect against DDos protection.

Fixed IP while using WAF with load balancer

WAF doesn't support NLB, ALB don't have fixed IP. To solve this we can use global accelerator for fixed IP and WAF on the ALB after the traffic goes from global accelerator to the ALB.

AWS Shield

Help protect against DDos attacks. Distributed denial of services from all around the world.

AWS Shield standard: Is deployed already for every AWS customer and is free. Protection against SYN/UDP flooding attack, reflection attack.

AWS Shield advanced: This is optional and will cost 3k a month. Protect against more sophisticated attacks. And give you a response team.

Firewall Manager

Manage rules in all accounts of an AWS organization. The security policy will be apply to the entire AWS organization that you deployed.

Rules for WAF, Shield Advanced, Security group for EC2.

So it is a central place for you to manage security rules for your organization.

Newly deployed resources will have those security rules that you have set in firewall manager.

Differences

AWS WAF is good for granular protection for your resources. Use it together with Firewall manager to automate the deployment of WAF configuration on new resources.

AWS Shield gives you DDos protection, but advanced gives you a dedicated response team to help you mitigate DDos attacks if you're prone to DDos.

Amazon GuardDuty

Intelligent threat discovery to protect your AWS account.

Looks like CloudTrail event logs, data events and management events. Looks like VPC flow logs and DNS logs, EKS Audit logs.

Basically AI protecting your AWS account for unusual activity. The findings it finds can trigger EventBridge which then you can notify you accordingly.

Different than CloudTrail insight events in that this is more broad and looks at way more logs.

Very good protection against cryptocurrency attack!

Amazon Inspector

Run automated security assessments on these resources:

- EC2 instances: Find known vulnerbailities
- Container images: See whether the container have any vulnerabilitity
- Lambda function: Find software vulnerabilities and dependencies that it uses

Continuous scanning when it is needed. Database of CVE when updated then it will scan. Network reachability for EC2.

Report finding to AWS Security Hub and event to EventBridge.

Amazon Macie

Use machine learning and pattern matching to find and protect sensitive data in AWS.

Identify sensitive data like personally identifiable information and notify you in EventBridge. Analyze data in say S3 buckets.

Revision #5
Created 2023-02-26 03:58:51 UTC by Tamarine
Updated 2023-02-27 00:27:53 UTC by Tamarine