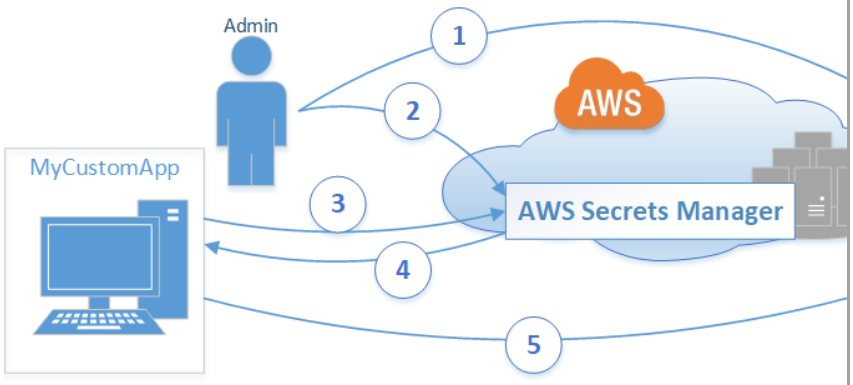
AWS - Secrets Manager

- **AWS Secrets Manager** is an AWS service that makes it easier for you to manage secrets.
  - *Secrets* can be database credentials, passwords, third-party API keys, and even arbitrary text.
- You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs
- Secrets Manager enables you to replace hardcoded credentials in your code (including passwords), with an API call to Secrets Manager to retrieve the secret programmatically.
- This helps ensure that the secret can't be compromised by someone examining your code, because the secret simply isn't there.
- Also, you can configure Secrets Manager to automatically rotate the secret for you according to a schedule that you specify.
- This enables you to replace long-term secrets with short-term ones, which helps to significantly reduce the risk of compromise.

****** WHY SECRETS MANAGER ******

- In the past, when you created a custom application that retrieves information from a database, you typically had to embed the credentials (the secret) for accessing the database directly in the application.
- When it came time to rotate the credentials, you had to do much more than just create new credentials.
- You had to invest time to update the application to use the new credentials.
- Then you had to distribute the updated application.
- If you had multiple applications that shared credentials and you missed updating one of them, the application would break.
- Because of this risk, many customers have chosen not to regularly rotate their credentials, which effectively substitutes one risk for another.



Links

https://aws.amazon.com/secrets-manager/

Check out this AWS Secrets Manager Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-secrets-manager/

	Check out this AWS Systems Manager Cheat Sheet: https://tutorialsdojo.com/aws-cheat-sheet-aws-systems-manager/

References:

https://aws.amazon.com/secrets-manager/

https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-using-aws-secrets-manager/

Check out this AWS Secrets Manager Cheat Sheet:

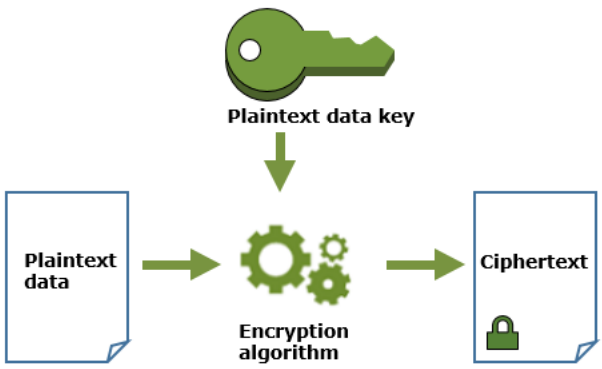
https://tutorialsdojo.com/aws-cheat-sheet-aws-secrets-manager/

Check out this AWS Systems Manager Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-systems-manager/

AWS - KMS

- **AWS Key Management Service (AWS KMS)** is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.
- The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules.
- AWS KMS is integrated with most other AWS services that encrypt your data with encryption keys that you manage.
- AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs.



- By using AWS KMS, you gain more control over access to data you encrypt.
- You can use the key management and cryptographic features directly in your applications or through AWS services that are integrated with AWS KMS.
- Whether you are writing applications for AWS or using AWS services, AWS KMS enables you to maintain control over who can use your customer master keys and gain access to your encrypted data.
- AWS KMS is integrated with AWS CloudTrail, a service that delivers log files to an Amazon S3 bucket that you designate.
- By using CloudTrail you can monitor and investigate how and when your master keys have been used and by whom.

- If you want a managed service for creating and controlling your encryption keys, but you don't want or need to operate your own HSM, consider using AWS Key Management Service.

References:

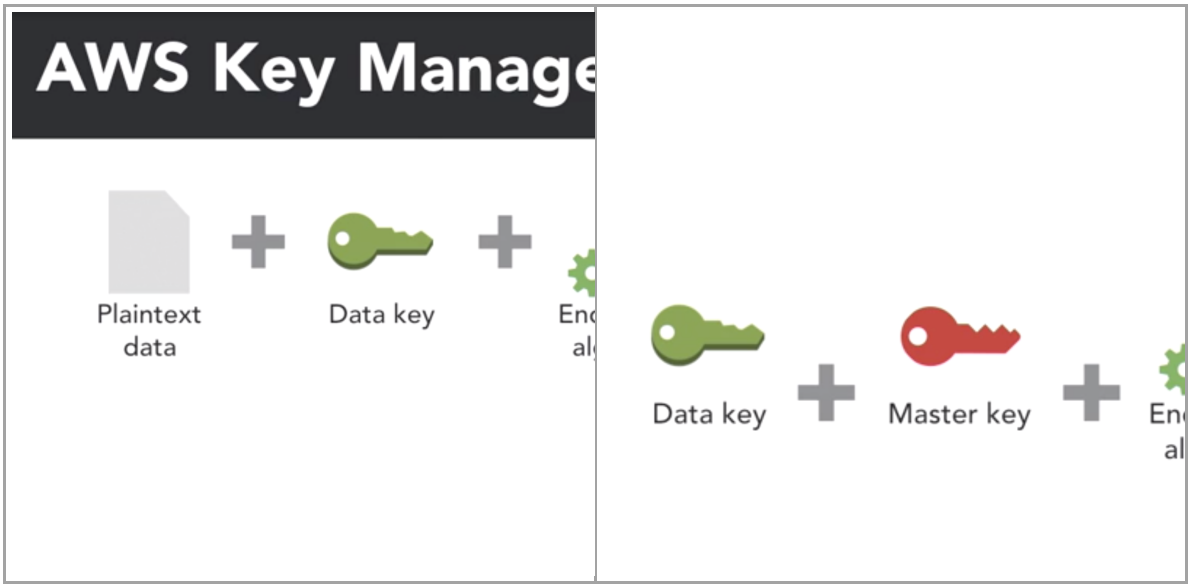
https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

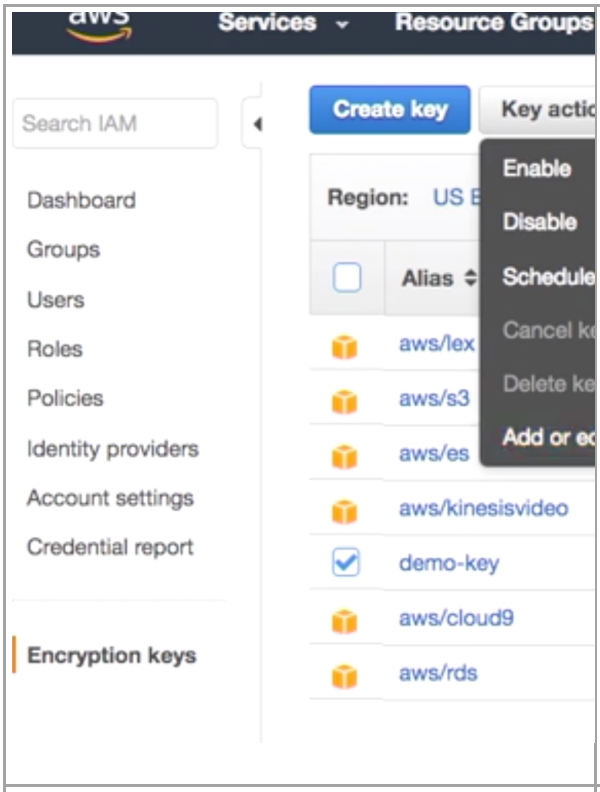
https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys

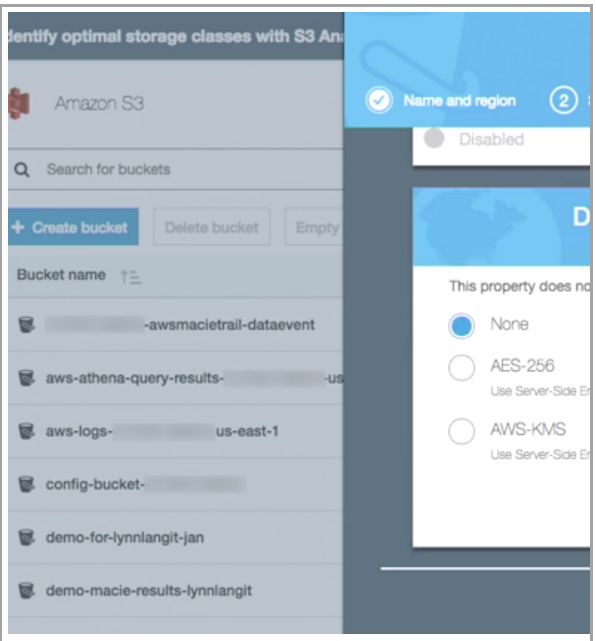
https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html

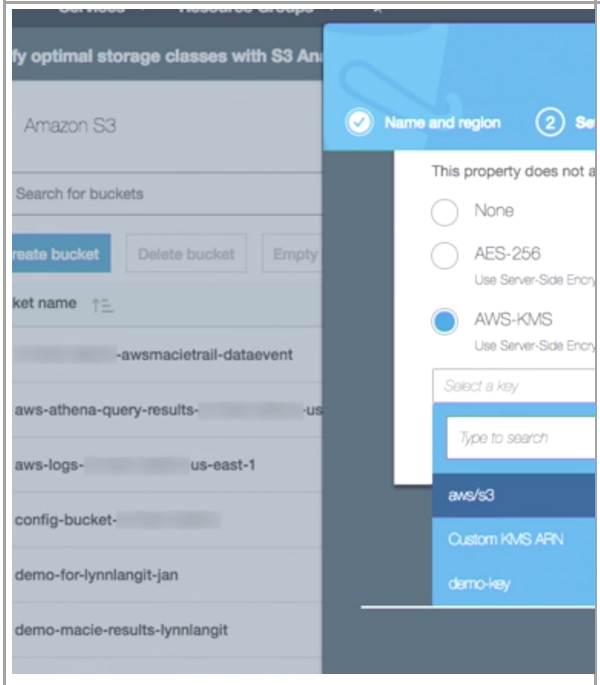
Check out this AWS Key Management Service (KMS) Cheat Sheet:

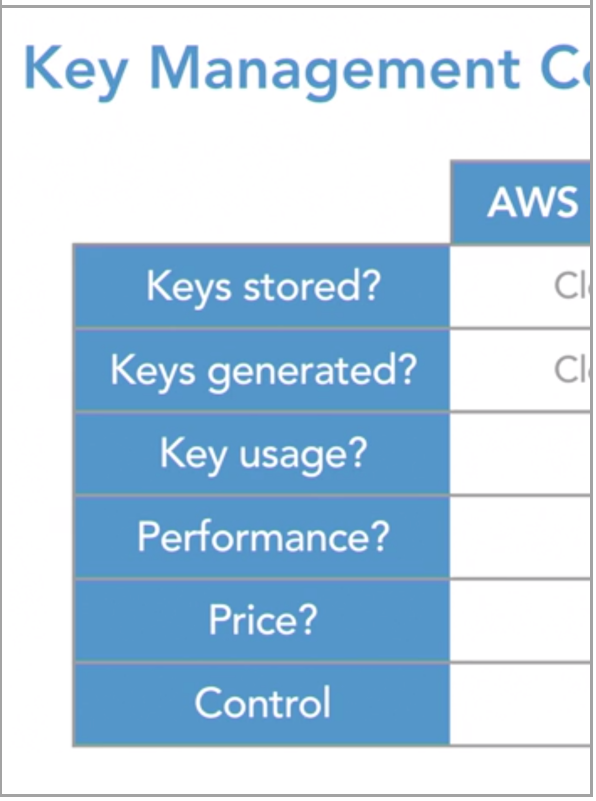
https://tutorialsdojo.com/aws-cheat-sheet-aws-key-management-service-aws-kms/




Services
Resource Groups
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Create key
Enable
Disable
Region:
Alias
aws/lex
aws/s3
aws/es
aws/kinesisvideo
demo-key
aws/cloud9
aws/rds


Amazon S3
Search for buckets
Create bucket
Delete bucket
Empty
Bucket name
-awsmacietrail-dataevent
aws-athena-query-results-
aws-logs-
us-east-1
config-bucket-
demo-for-lynnlangit-jan
demo-macie-results-lynnlangit
Name and region
Disabled
This property does no
None
AES-256
AWS-KMS


Amazon S3
Search for buckets
Delete bucket
Empty
-awsmacietrail-dataevent
aws-athena-query-results-
aws-logs-
us-east-1
config-bucket-
demo-for-lynnlangit-jan
demo-macie-results-lynnlangit
Name and region
This property does not
None
AES-256
AWS-KMS
Select a key
Type to search
aws/s3
Custom KMS ARN
demo-key


Key Management
AWS
Keys stored?
Keys generated?
Key usage?
Performance?
Price?
Control

CloudHSM

- CloudHSM is installed in a
  across multiple Availability
- CloudHSM instances are sy
  by AWS
- Each CloudHSM cluster car
- Automatic encrypted backu
  on your behalf

Key Management Se

- Managed and integrated enc
  to easily encrypt data stored
- KMS customer master keys (
  keys used by each customer
- Unique data keys are used fo
  decryption request
- KMS stores multiple copies o
  with 11 9s of durability

KMS Integration

- Elastic Block Storage
- S3 Buckets
- Redshift
- RDS
- EFS
- FSx

Data Key Generatio

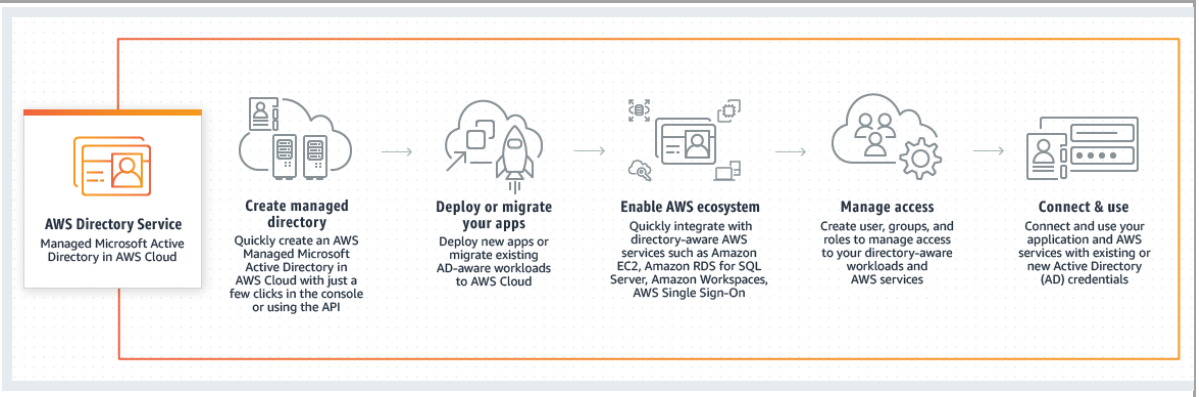
- KMS returns a plaintext ve
  your application
- The plaintext key is used t
- KMS also returns a cipher
  encrypted with the CMK
- The encrypted copy of the
  encrypted data

AWS - AD Connector

- AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud.
- AD Connector comes in two sizes, **small** and **large**.
- A small AD Connector is designed for smaller organizations of up to 500 users.
- A large AD Connector can support larger organizations of up to 5,000 users.

AWS Directory Service AD Connector

- Considering that the company is using a corporate Active Directory, it is best to use **AWS Directory Service AD Connector** for easier integration.
- In addition, since the roles are already assigned using groups in the corporate Active Directory, it would be better to also use **IAM Roles**.
- Take note that you can assign an IAM Role to the users or groups from your Active Directory once it is integrated with your VPC via the AWS Directory Service AD Connector.



- **AWS Directory Service** provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services.
- Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources.
- AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)–aware applications in the cloud.
- It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

Reference:

https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

Check out these AWS IAM and Directory Service Cheat Sheets:

https://tutorialsdojo.com/aws-cheat-sheet-aws-identity-and-access-management-iam/

https://tutorialsdojo.com/aws-cheat-sheet-aws-directory-service/

Here is a video tutorial on AWS Directory Service:

https://youtu.be/4XeqotTYBtY