😊 Key Management Service

AWS Key Management Service (KMS) is a managed service that makes it easy to create and control cryptographic keys used to secure your data. Here's a brief overview:

Key Features:

1. **Create and Manage Keys**:
    - Allows you to create, rotate, disable, and delete encryption keys.
    - Supports symmetric and asymmetric keys for different encryption needs.
2. **Integrated Encryption**:
    - Seamlessly integrates with other AWS services like S3, RDS, EBS, and Lambda to provide built-in encryption.
3. **Access Control**:
    - Uses AWS Identity and Access Management (IAM) policies and grants to control who can use and manage keys.
    - Supports fine-grained permissions for specific actions on keys.
4. **Key Usage Auditing**:
    - Integrates with AWS CloudTrail to log all key usage and management activities, helping with compliance and security audits.
5. **Automatic Key Rotation**:
    - Supports automatic rotation of keys, which can reduce the risk of compromised keys by periodically replacing them.
6. **Customer-Managed Keys (CMKs)**:
    - Allows you to create and manage your own encryption keys with full control over their lifecycle.

Common Use Cases:

- **Encrypting Data at Rest**: Secure data stored in AWS services like S3, RDS, and EBS.
- **Secure Communication**: Encrypt sensitive data before sending it over the network.
- **Digital Signatures**: Use asymmetric keys to create and verify digital signatures for data integrity and authenticity.

Benefits:

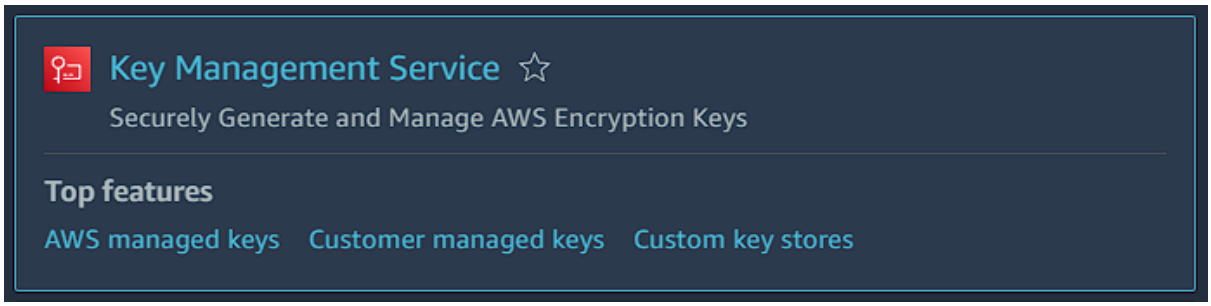
- **Enhanced Security**: Provides strong encryption and key management practices to protect your data.
- **Ease of Use**: Simplifies the complex task of managing encryption keys while integrating with AWS services.

- **Compliance**: Helps meet regulatory and compliance requirements by providing detailed logs and audit trails.

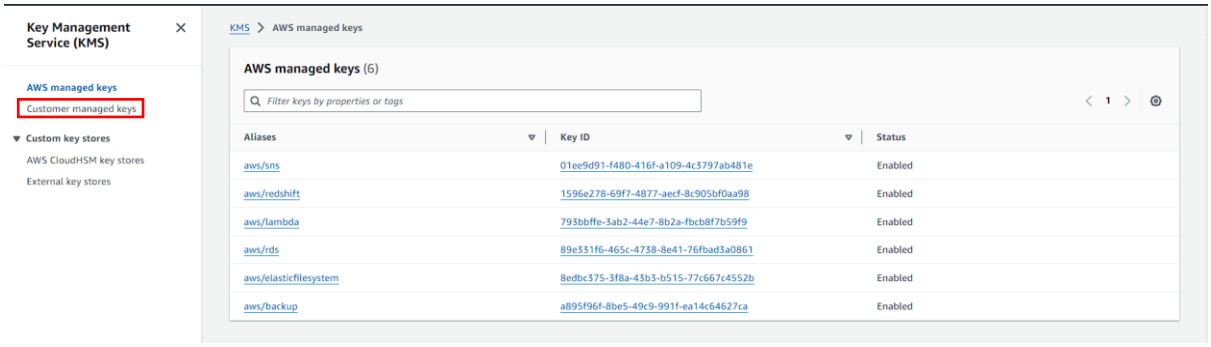
AWS KMS is crucial for managing encryption keys in a secure and scalable manner, ensuring that your data is protected both at rest and in transit.

😄 To begin with the Lab:

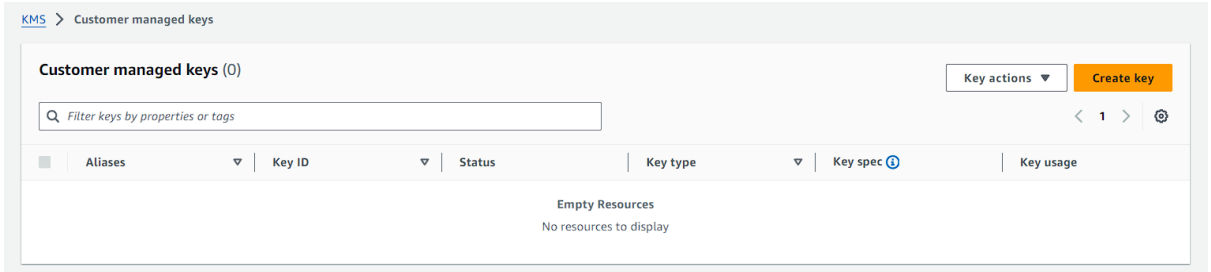
1. Login to AWS Console and search for KMS. Choose this service accordingly.



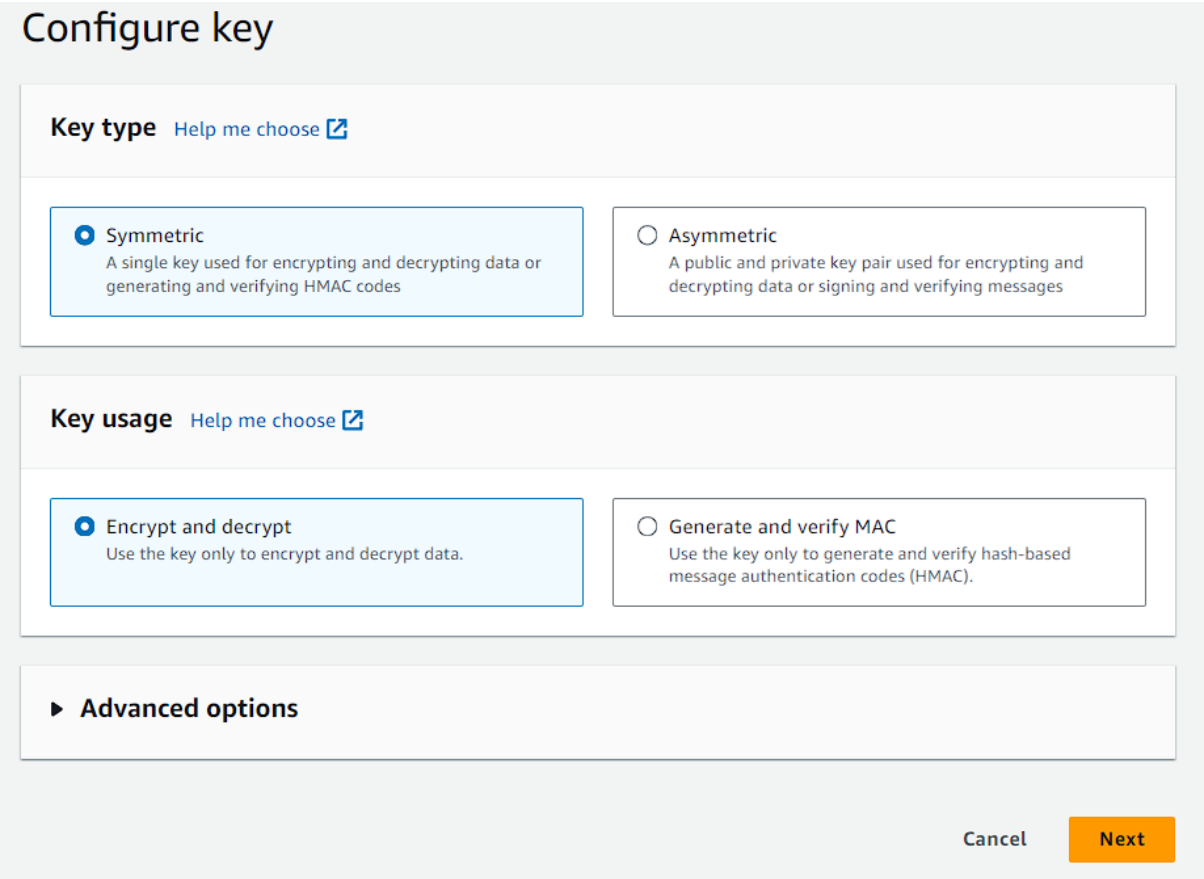
2. Now from KMS dashboard if you will go to AWS Managed keys, there are several keys that are managed by AWS.
3. You can also create your own key, for that click on Customer managed keys.



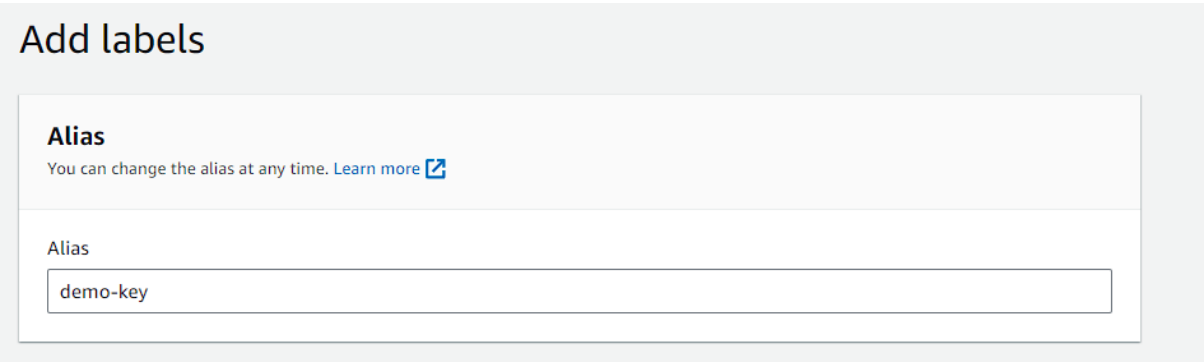
4. Here click on create key.



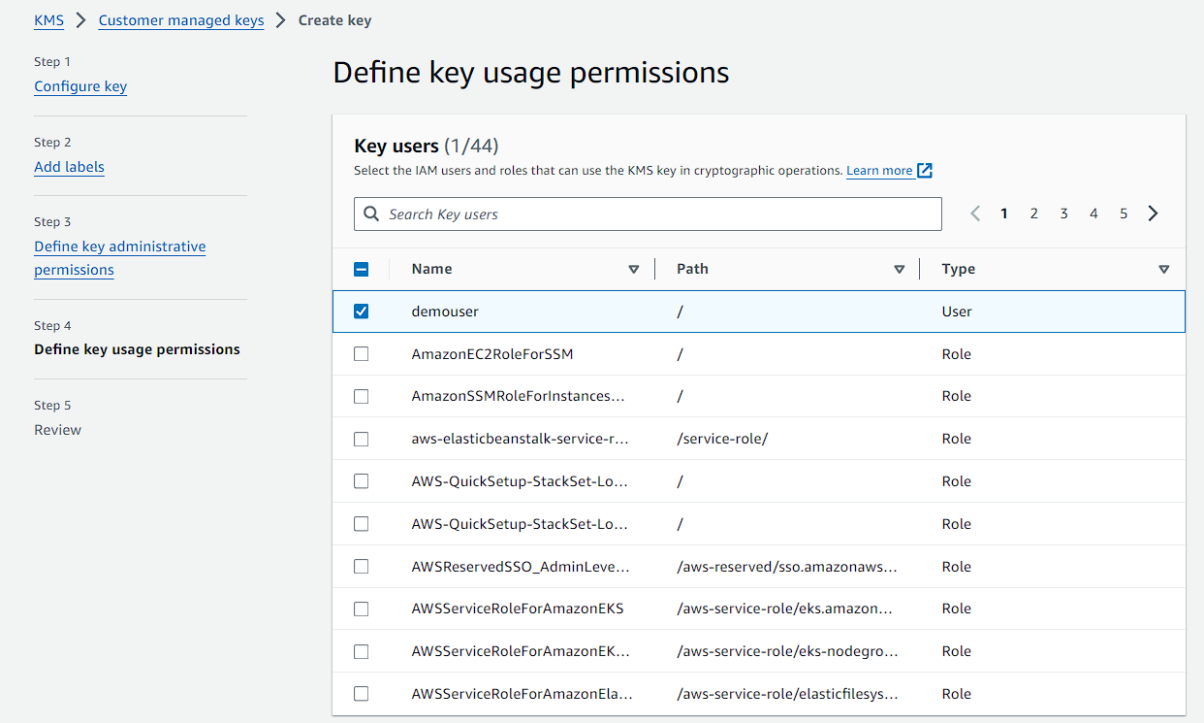
5. Now choose Symmetric key type for encrypt and decrypt usage. Then click on next.

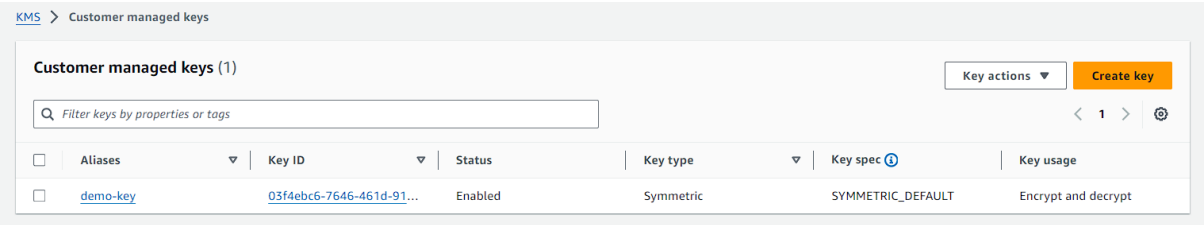


6. On the next page you just need to give it a name. then go to next page.

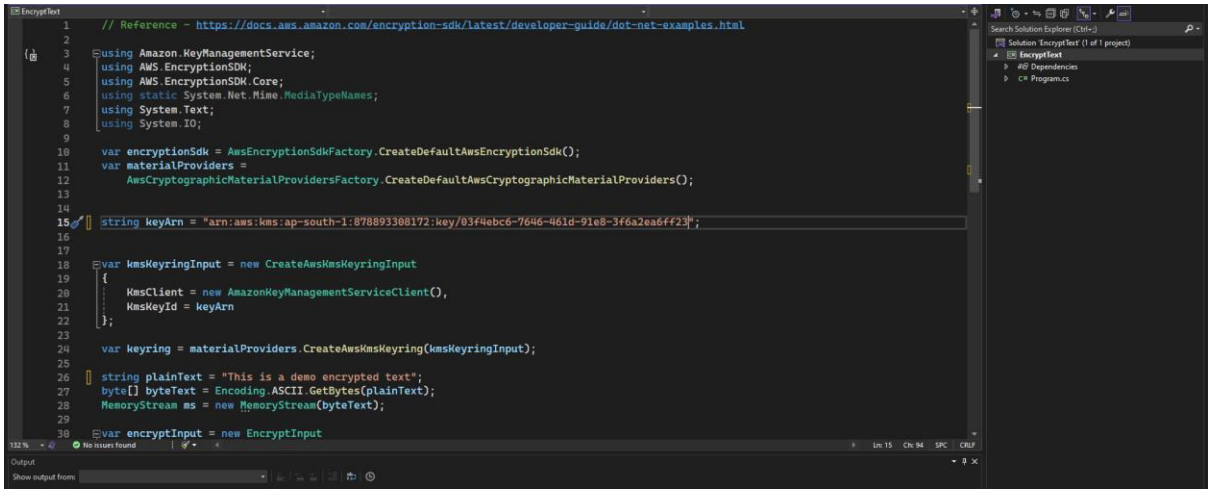


7. For step 3 skip it then on step 4 you need to choose an IAM user. If you don't have any then create one.
8. After that just create your key.

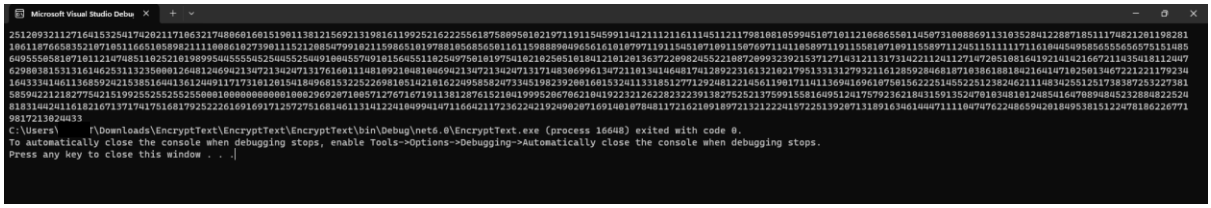




9. After that you need to download a program from GitHub with name encrypttext.zip. it will be in zip format, so download it and unzip it.
10. After that you need to open this program in visual studio.
11. Now go back to AWS Console and open your key, in there you will see your ARN for the key copy it and paste it in the program.



12. After that also remember to configure your IAM user in your local system.
13. Now just run this program locally.
14. You will see the encrypted text.



15. For all the key management service is doing, is it is helping you to store that encryption key. At any point in time, you can make a call onto the key management service from your program. Use that encryption key to encrypt your data.