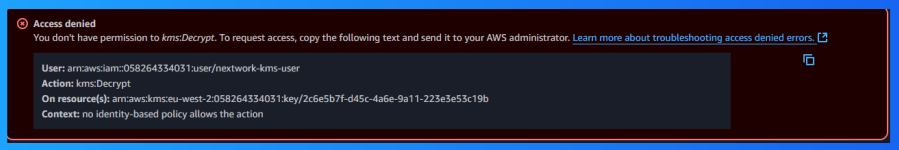
NextWork.org

Encrypt Data with AWS KMS

TA tahirgroot@gmail.com



TA
tahirgroot@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

In this project, I will demonstrate using encyrption to secure data. The goal is to create encryption keys with AWS KMS(Key Management System), encrypt a DynamoDB table's data with that key, then test access using IAM users.

Tools and concepts

Services I used include AWS KMS (Key Management Service), Dynamo DB, AWS IAM, Key concepts I learnt include encryption, databse tables, kms using permission to actions rather than just access to the key itself. creating a user to test access.

Project reflection

1 hour

Yes

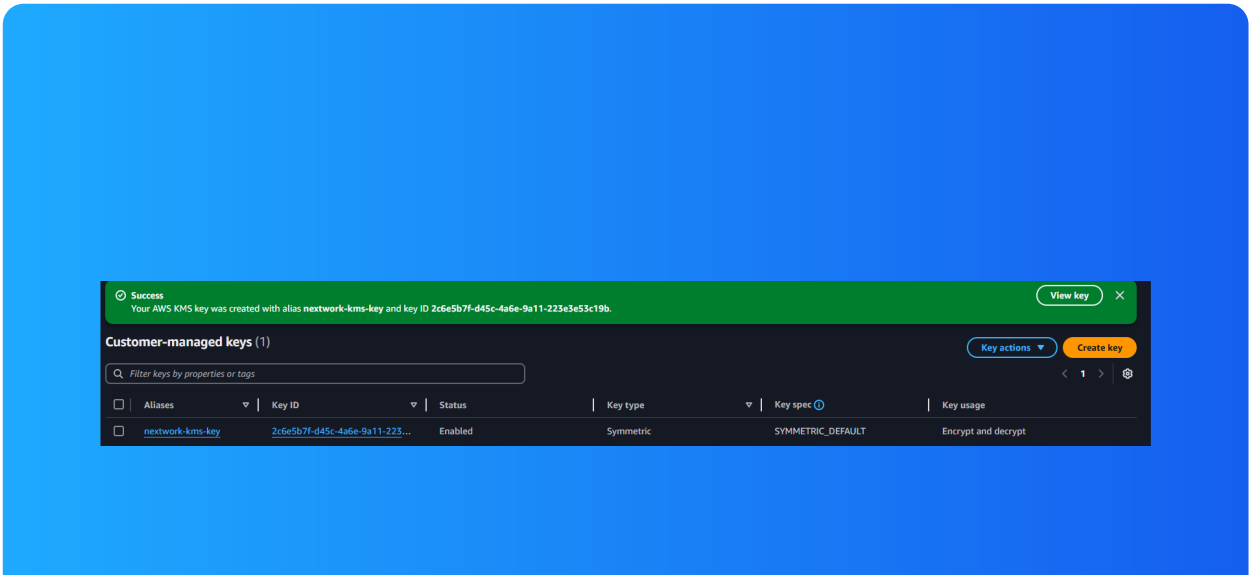
TA
tahirgroot@gmail.com
NextWork Student

Encryption and KMS

Encryption is the process of turning original data/plaintext into a secure format. Companies and developers do this to secure data from unauthorized users. Encryption keys are the secure code that informs an algolorithim on how it should encrypt

AWS KMS is a vault for encryption keys. Key management systems are important because they help us secure and manage the keys I use to encrypt data. Unauthorized acces to the keys = exposing encrypted data, which puts our security at risk

Encryption keys are broadly categorized as symmetric and asymmetric. I set up a symmetric key because we will be using the exact same key to encrypt and decrypt our data. Asymmetric keys would be a good choice if i need different keys for decryption

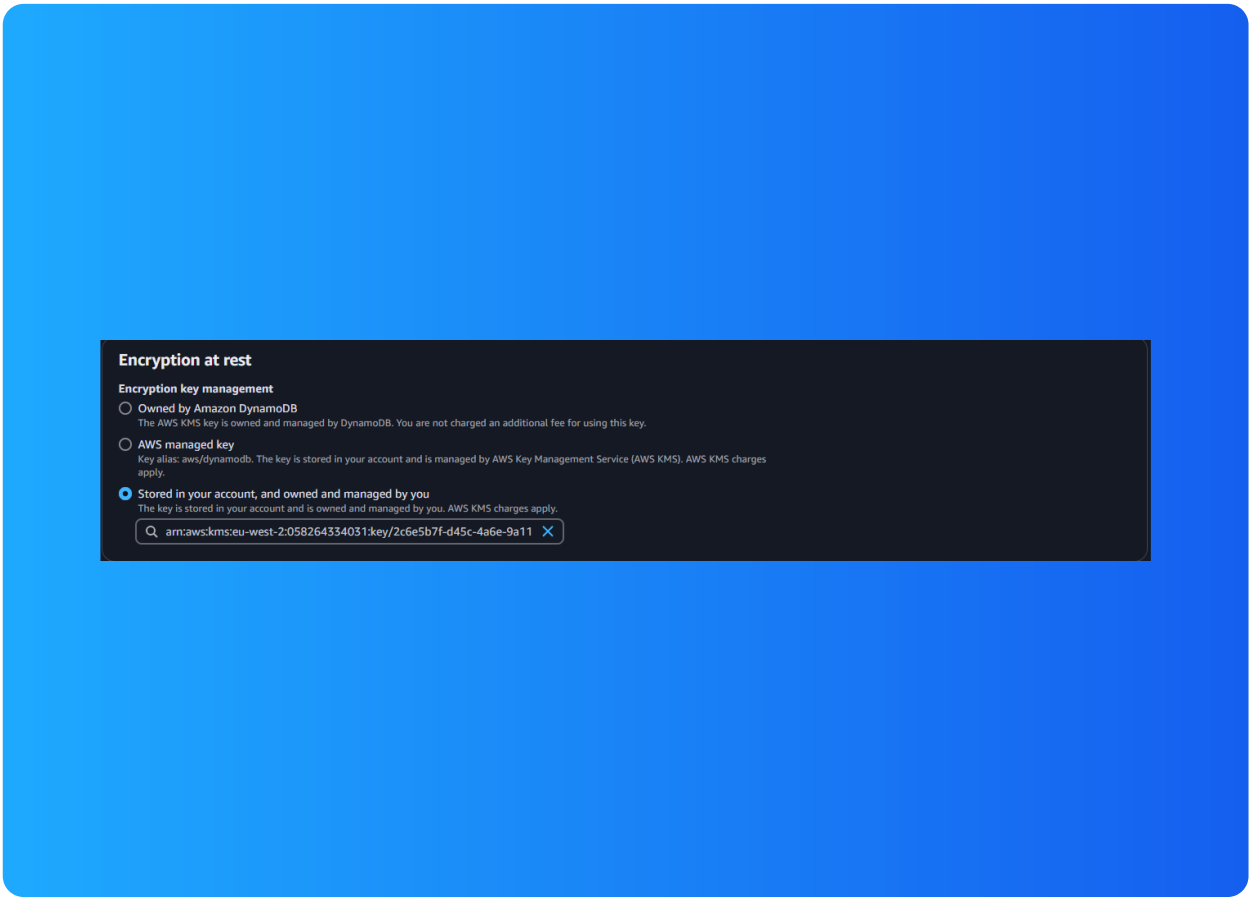


TA
tahirgroot@gmail.com
NextWork Student
NextWork.org

Encrypting Data

My encryption key will safeguard data in DynamoDB, which is a fast and flexible AWS database service. Dynamo DB is great for applications that need fast access to large amounts of data e.g. gaming.

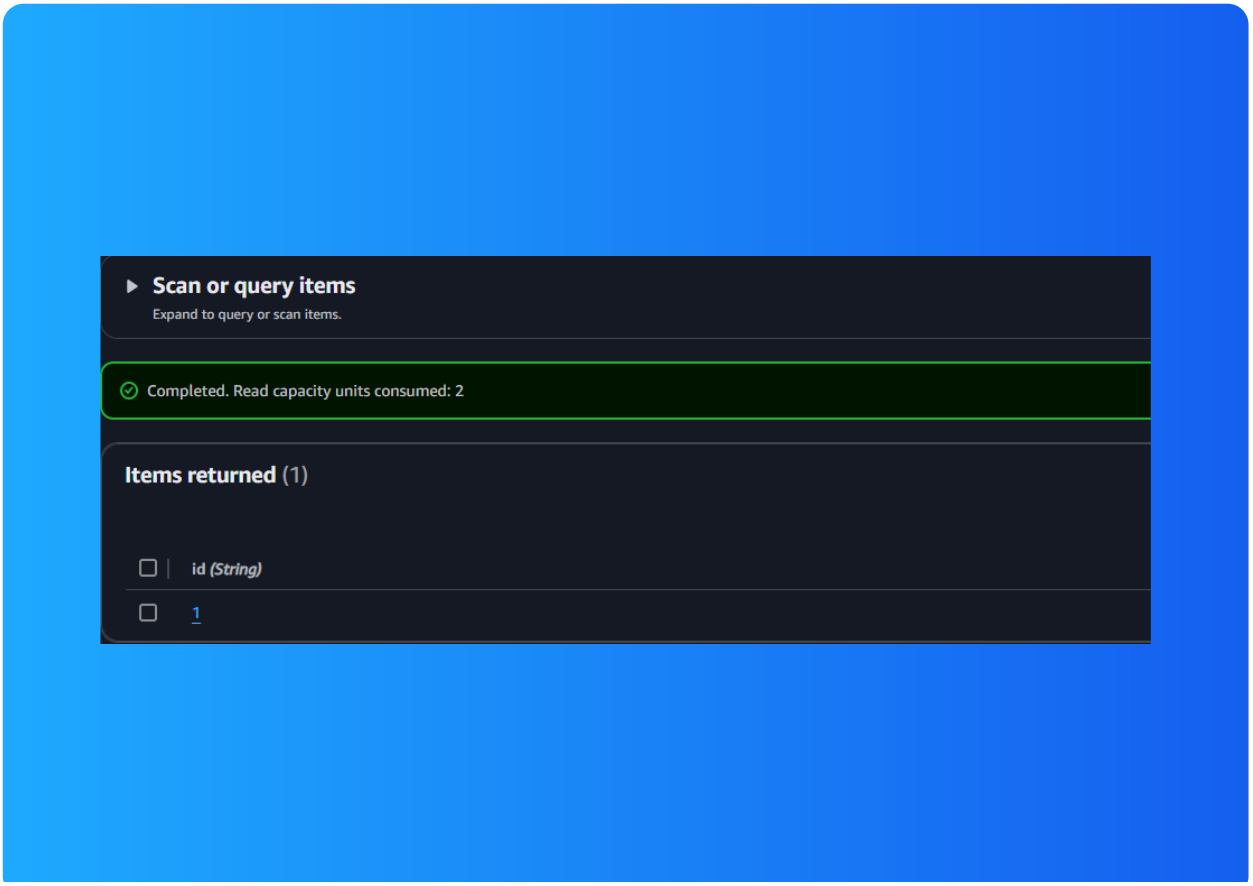
The different encryption options in DynamoDB include Dyanmo DB-owned, AWS Managed and customer managed. Their differences are based on who creates and manages the key; and whetheher we have visibility. I selected the cmk to use our created KMS key.



Data Visibility

Rather than controlling who has access to the key, KMS manages user permissions bycontrolling the actions that people can do with that key. in our case even if we gave our test user the permisison to see the key, it would permission to decrypt.

Despite encrypting my DynamoDB table, I could still see the table's items because we are users of the key DynamoDB uses transparent data encryption, which means it does the encryption/decryption process for us because it knows we're authorized.

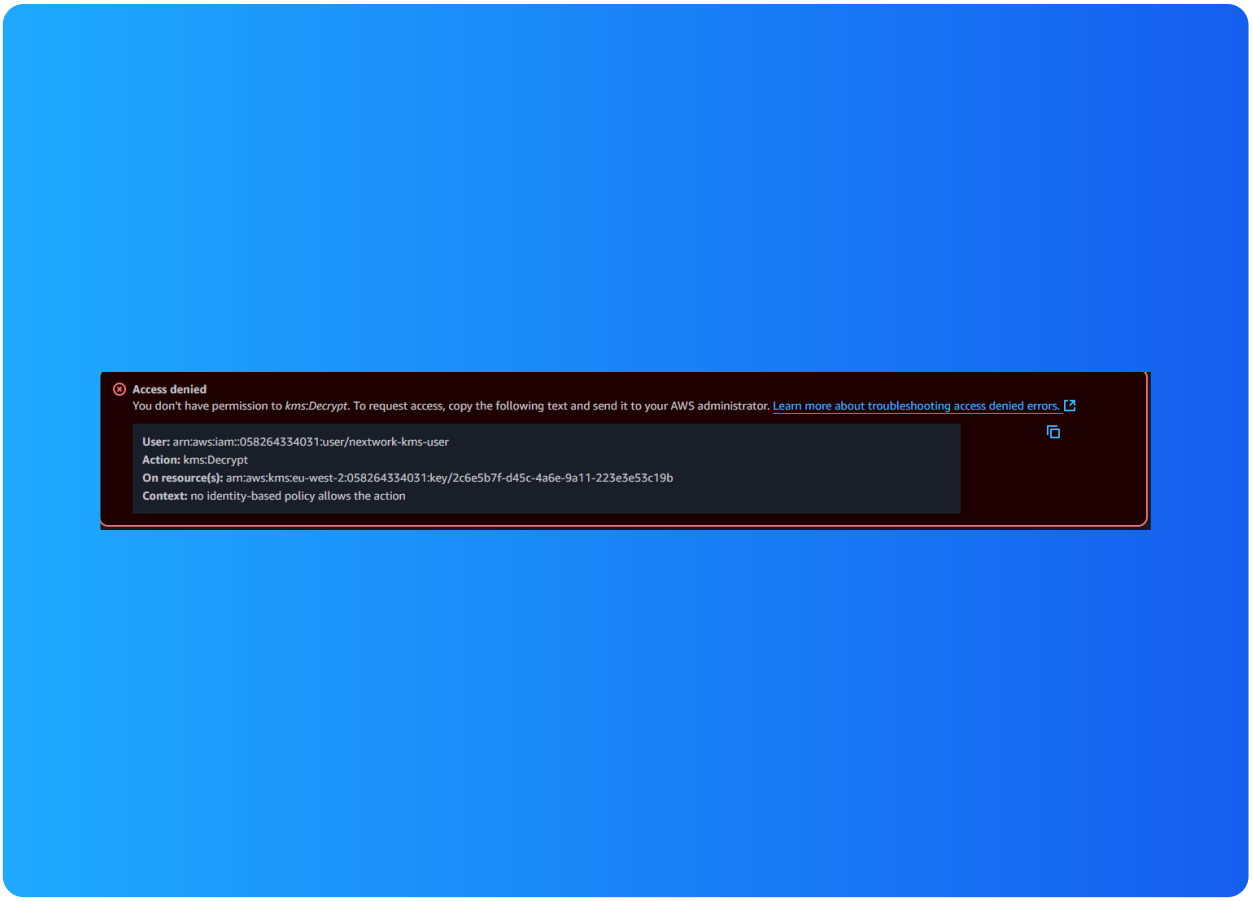


TA
tahirgroot@gmail.com
NextWork Student

Denying Access

I configured a new IAM user to validate whether unauthorized users can still acees encrypted data .The permission policies I granted this user are dynamo DB full access but encryption/decryption permission with AWS KMS.

After accessing the DynamoDB table as the test user, I encountered an access deny message because our test user has no access to decryption with the key. This confirmed that encryption jeys can be used to secure data.

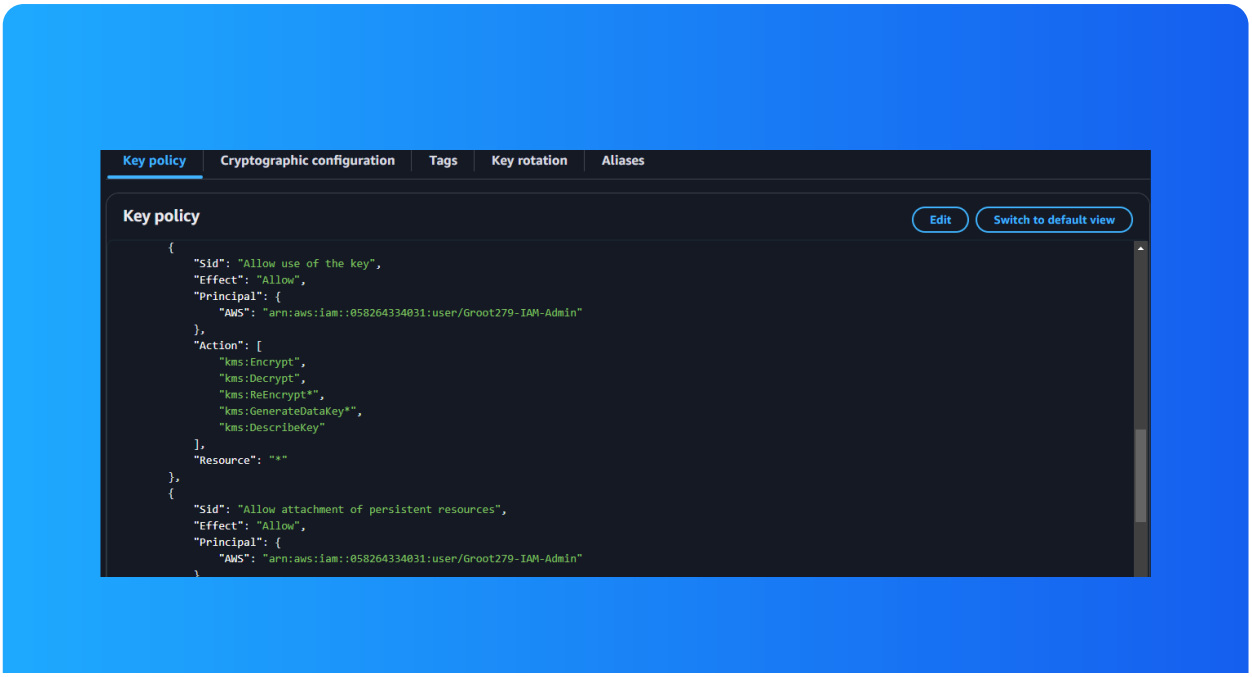


EXTRA: Granting Access

To let my test user use the encryption key, I made it a key user in the KMS console! My key's policy was updated to allow the nextwork kms user to encrypt, decrypt and re-crypt using the key.

Using the test user, I retried accessing the DynamoDB table. I observed that the user can see the data inside which confirmed that making it a key user is an efective way to authorize some to see encrypted data.

Encryption secures data instead of an entire resource or service. I could combine encryption with other acces control tools like security groups and permission policies to have two layers of security - the resource level, and then the data level.



Everyone should be in a job they love.

Check out nextwork.org for more projects