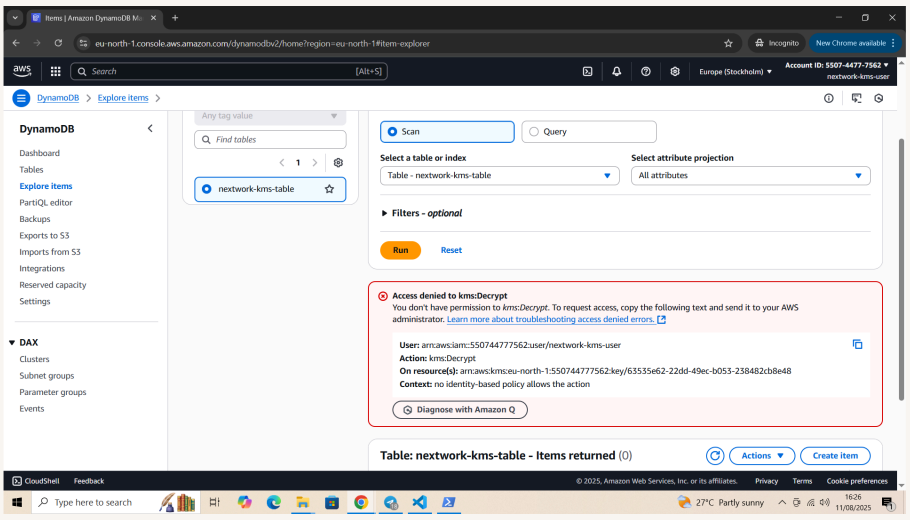
nextwork.org

Encrypt Data with AWS KMS

Nchindo Boris



Nchindo Boris
NextWork Student

Introducing Today's Project!

In this project, I will; - Create encryption keys with AWS KMS (Key Management Service). - Encrypt a DynamoDB database with a KMS key. - Add and retrieve data from your database to test your encryption. - Observe how AWS stops unauthorized access to your data. - Give a user encryption access. The goal is to understand how to to safeguard cloud environments and set up secure access to resources.

Tools and concepts

Services I used include; - AWS Key Management Service (KMS) - Amazon DynamoDB - AWS IAM Key concepts I learnt include encryption, .

Project reflection

This project took me approximately 1 hour. It was most rewarding to actually see a security practice work well and it being understood by me

I did this project as part of my journey to understanding cloud computing and it definitely met one of my goals

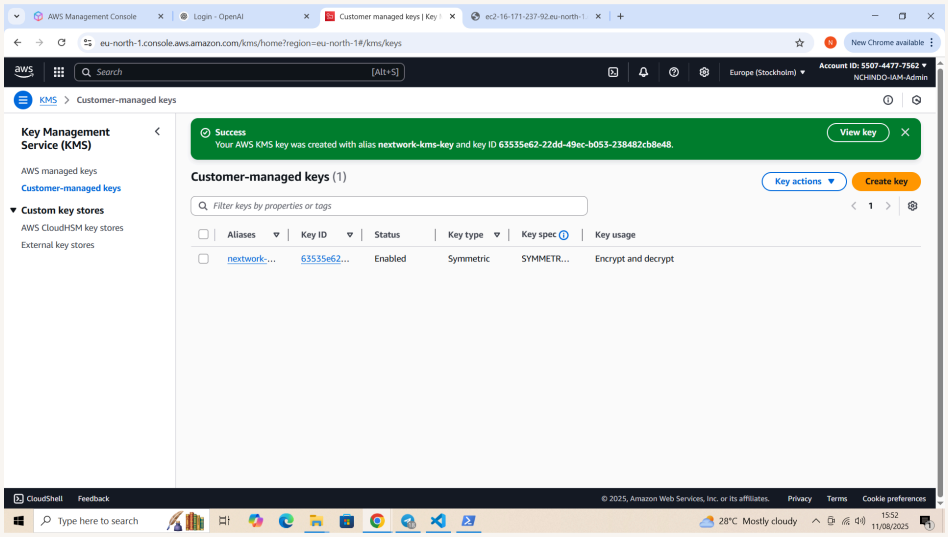
Encryption and KMS

Encryption is the process that uses algorithms to convert data into a secure format called ciphertext. Companies and developers do this to secure user data, transactions, files and more. Encryption keys tells the algorithm exactly how it would transform plain text into the jumbled up format called cipher text.

AWS KMS is a secure vault for your encryption keys. You use KMS to create, manage, and use encryption keys that protect the data in your AWS resources. Key management systems are important because they help to manage all your encryption keys, like what it encrypts or who has access, in one place.

Encryption keys are broadly categorized as symmetric and asymmetric encryption keys. I set up a symmetric key because they are generally faster and more efficient for encrypting large amounts of data, which is why I am using one for my DynamoDB table.

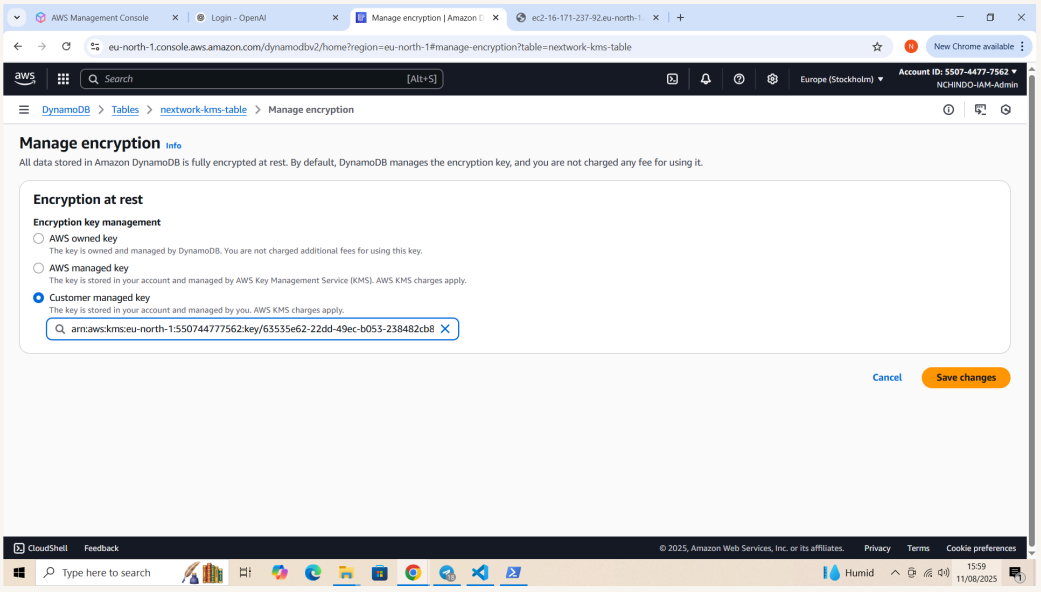
Nchindo Boris
NextWork Student



Encrypting Data

My encryption key will safeguard data in DynamoDB, which is one of AWS's database services.

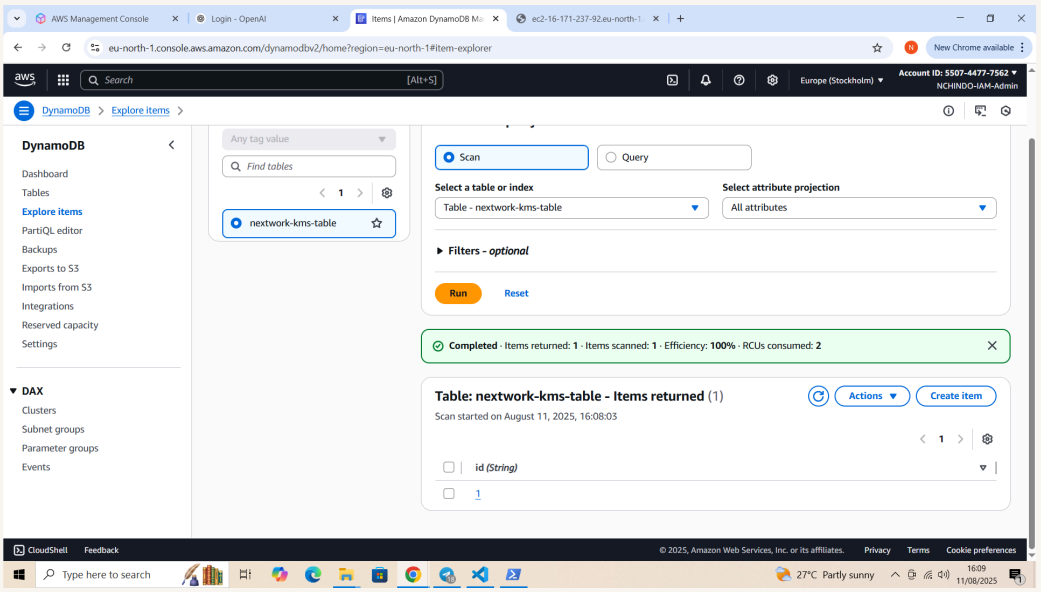
The different encryption options in DynamoDB include; - Owned by Amazon DynamoDB - AWS managed key - Stored in your account, and owned and managed by you Their differences are based on who has control and management. I selected Customer managed key to have full control



Data Visibility

Rather than controlling who has access to the key, KMS manages user permissions by giving the test user the permission to see that a KMS key is available in my AWS environment, but the test user still wouldn't have the permissions to decrypt the data it protects.

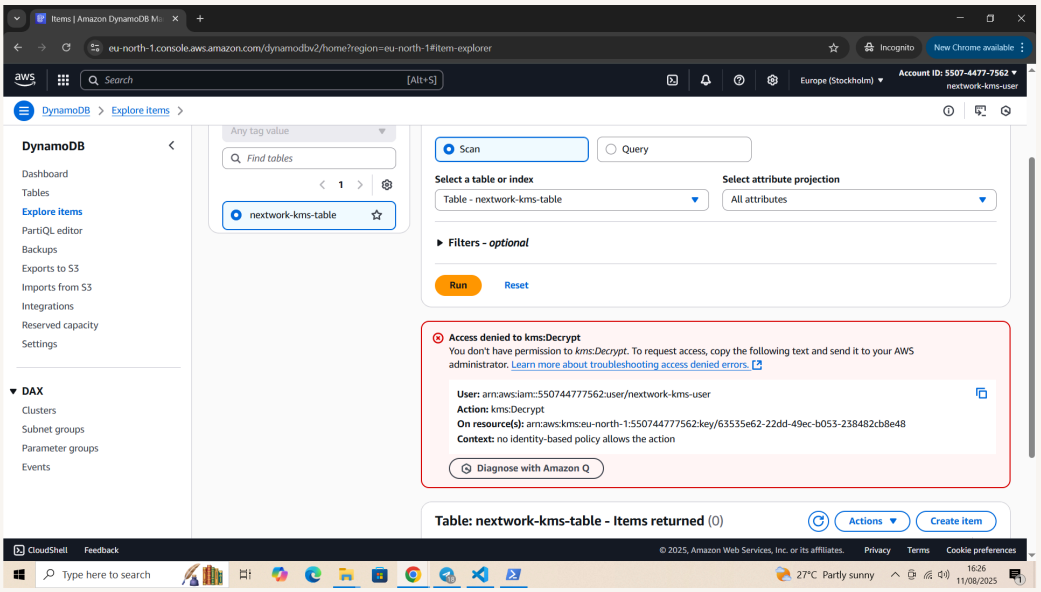
Despite encrypting my DynamoDB table, I could still see the table's items because as an authorised user I have permissions to use the encryption key in KMS. DynamoDB uses transparent data encryption, which makes sure that my data is secure at rest, yet still accessible to authorized users that have the right permissions.



Denying Access

I configured a new IAM user to grant the user full access to DynamoDB but not to my KMS key. The permission policies I granted this user are AmazonDynamoDBFullAccess but not KMS key access

After accessing the DynamoDB table as the test user, I was denied access because the new IAM user I am logged in as (nextwork-kms-user) does not have the permission to decrypt the data. This confirmed that a KMS key can be accessible to many users, but only those with the right permissions can use it to do specific actions like encryption or decryption.

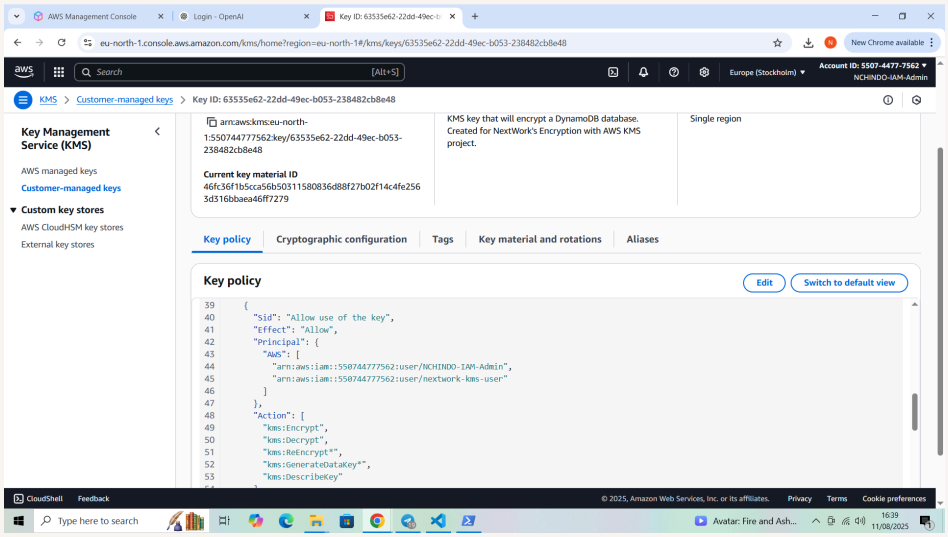


EXTRA: Granting Access

To let my test user use the encryption key, I added the test user to be one of the key users. My key's policy was updated to Allow use of key for test user also

Using the test user, I retried to access the data again. I observed could now see the data which confirmed that I now have access to the data with permissions to decrypt and encrypt

Encryption secures data instead of security groups or permission policies. I could combine encryption with security groups or permission policies to better secure data.



The place to learn & showcase your skills

Check out nextwork.org for more projects