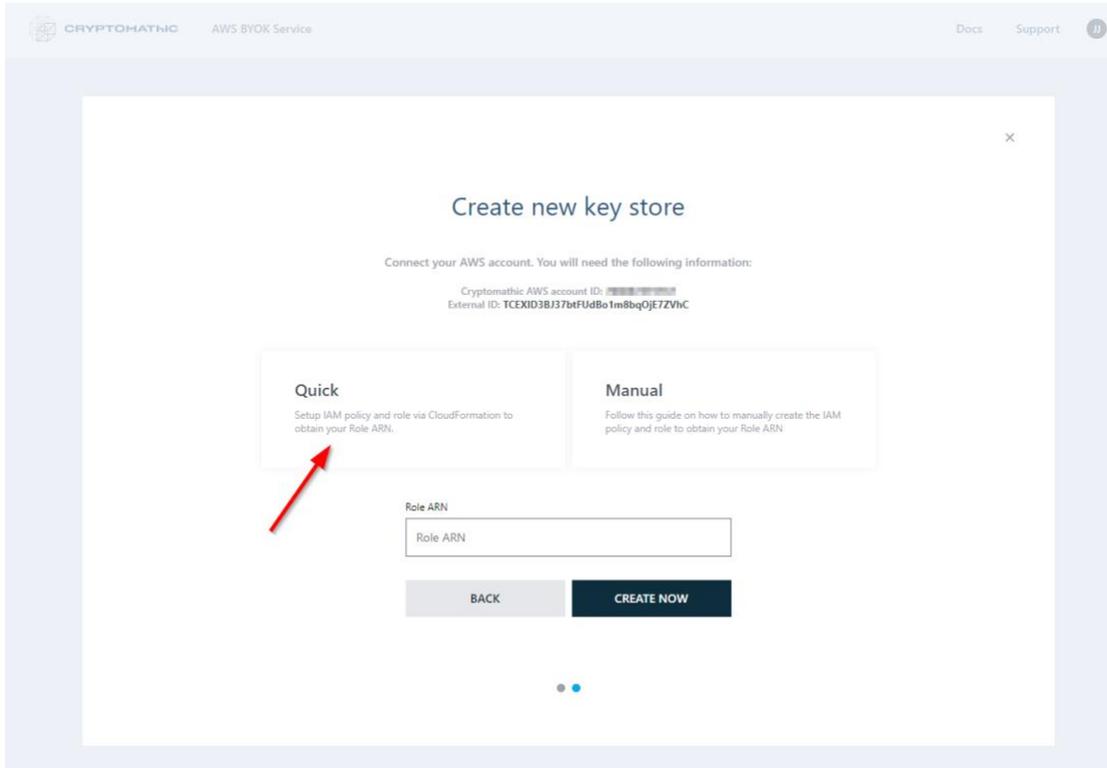




How to Set up a Role Related to a Keystore – Quick Guide

To grant the BYOK web service access to creating and maintaining keys in the KMS of your account, you must create a policy and include it in a role. This guide describes how you can set this up quickly using a CloudFormation template.

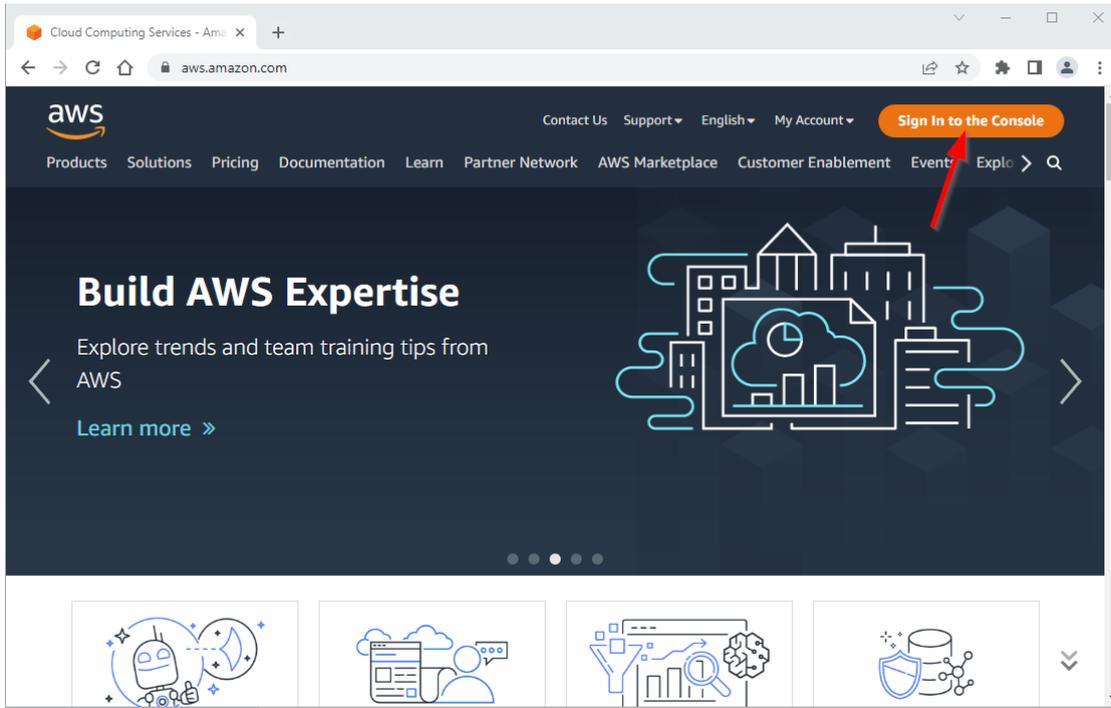
Choose the “Quick” Option



A new browser tab will open when you click the “Quick” button. You will be directed to the AWS login page, unless you are already logged in. Make sure that you log in to the AWS account where you want your keys to be stored in AWS KMS.

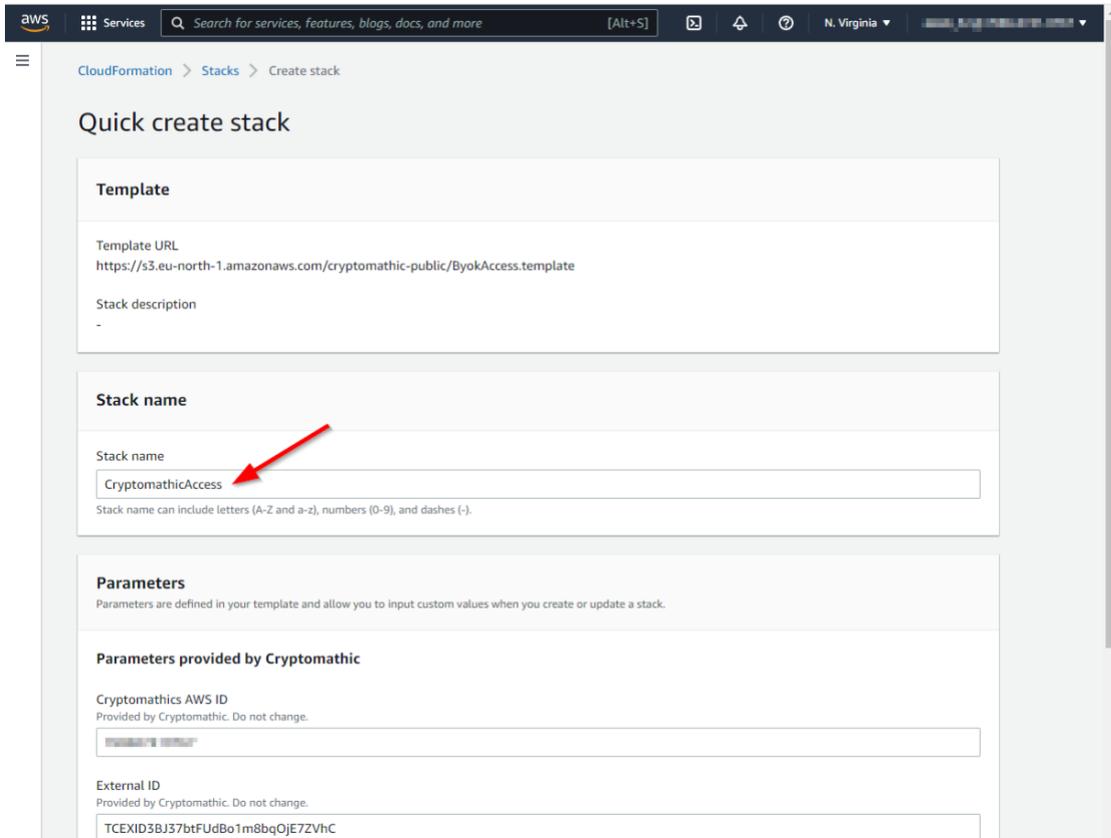
Log in to the AWS Account

First, log in to the AWS account (if not already logged in) where your KMS resides (i.e., where you want your keys to be exist):

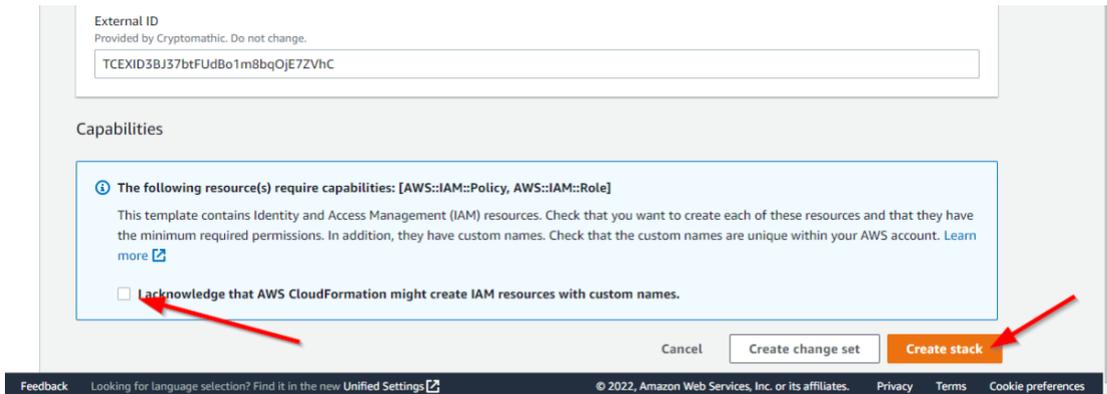


Create CloudFormation Stack

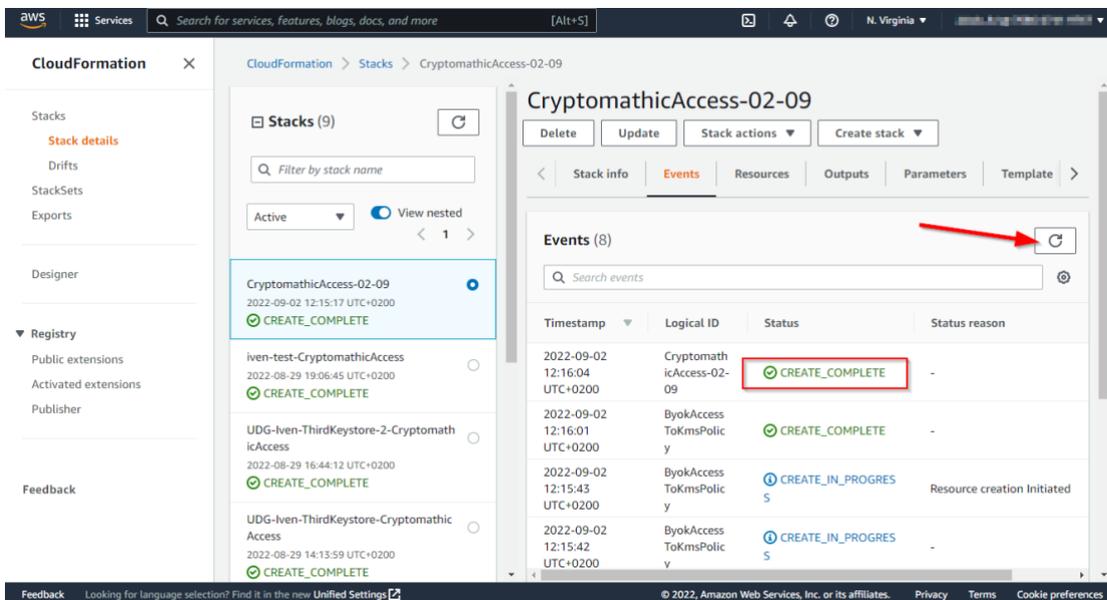
After login, you will be forwarded directly to a form already automatically filled out with all relevant information. All you need to do is ensure that the stack name is not already in use (the stack name in the shown example is "CryptomathicAccess").



Next, check the "I acknowledge..." box in the bottom of the form and click the "Create stack" button:

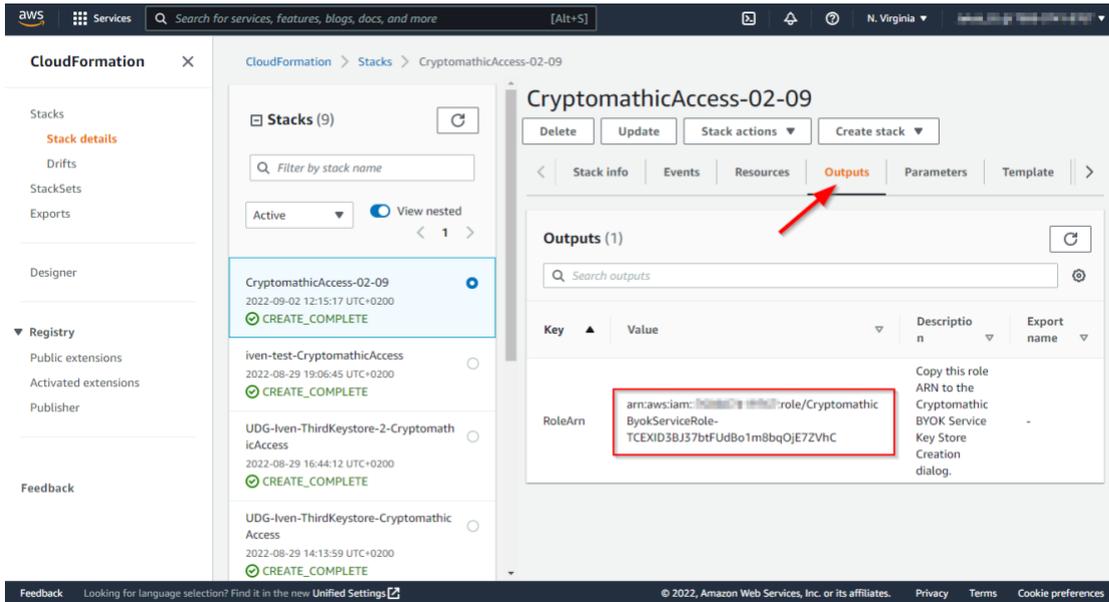


AWS CloudFormation will begin creating the role and policy. To follow its progress, click the update button in the upper right corner to refresh the events list:



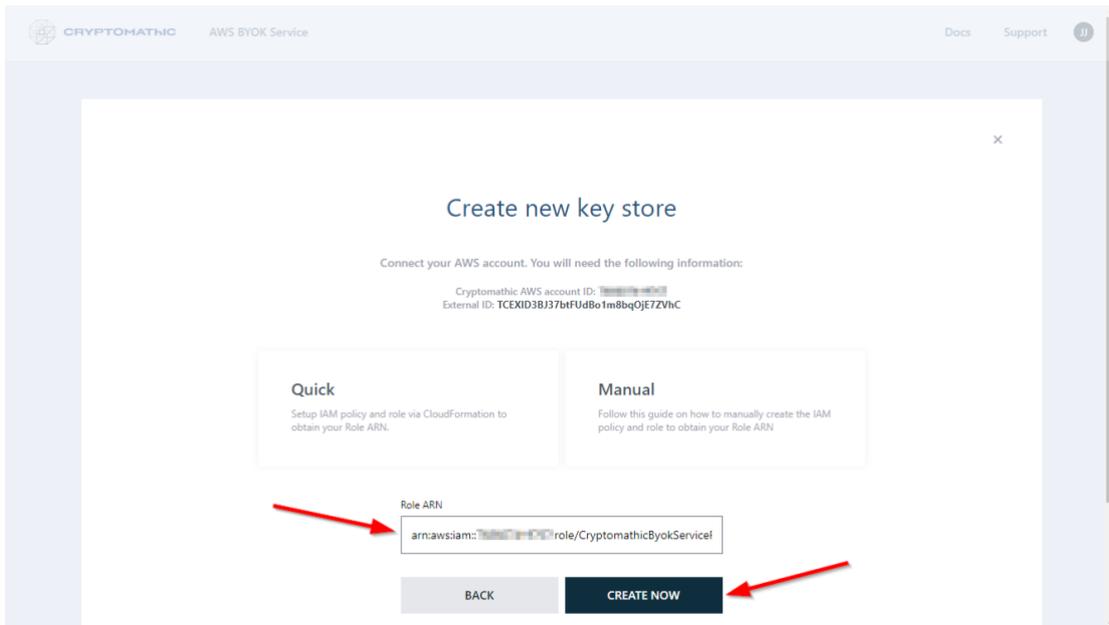
Obtain Role ARN

When the stack reaches the "CREATE_COMPLETE" state, click the Outputs tab. Here you will find a "RoleArn" value. Copy it.



Apply the Role ARN to finish the set up

Return to the "Create new key store" page and paste the "RoleArn" value into the text field.



Click the "Create now" button. This completes creation of the key store, and you are now ready to add the first key.