1. Login to your AWS account and access the S3 service from the Management Console. Create an S3 bucket in the US East (N. Virginia) Region and upload your VM image.vmdk file that was exported earlier .
2. Check if your CLI Version installed : C:\> aws –version
3. If not open a Command Prompt window. Run the following command: C:\> msiexec.exe /i <https://awscli.amazonaws.com/AWSCLIV2.msi>
4. Issue the aws configure command. The command will prompt you to enter four pieces of information: Access key ID, Secret access key, AWS Region, and Output format

A close-up of a white background

Description automatically generated

1. Use the following command from the AWS CLI to create an IAM role named "vmimport" with the trust policy trust-policy.json that allows the VM import service to assume the role.

$ aws iam create-role --role-name vmimport --assume-role-policydocument <file://C:\import\trust-policy.json>

Replace the my-import-bucket with your S3 bucket name and attach the IAM policy “vmimport” to the IAM role .

* $ aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document <file://C:\import\role-policy.json>
* $ aws ec2 import-image --description "My server VM" --disk-containers <file://C:\import\containers.json> .

Record the AMI ID and replace with the ID that was recorded .

$ aws ec2 describe-import-image-tasks --import-task-ids import-ami1234567890abcdef0

* Import task is completed; please view the EC2 console and click on the AMIs that are displayed.
* Launch the EC2 instance into the public subnet in the VPC service you had created. The AMI will be available using the My AMIs option.
* Configure Inbound SSH Port 22 and HTTP/HTTPS access. If you have selected password-based SSH authentication, proceed without keypair.
* Once EC2 launched and passed status checks, copy the public IP add of EC2 and copy it on your browser . You can append wp-admin to the IP address of your instance (for e.g., 44.203.102.12/wp-admin) to access the login page.