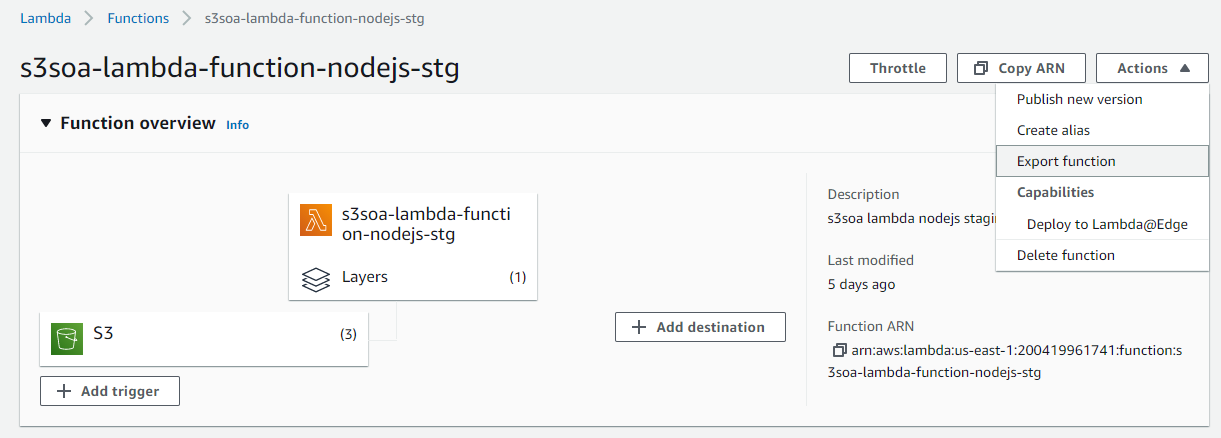
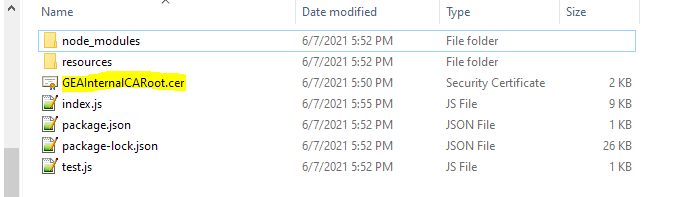
**Method 1**

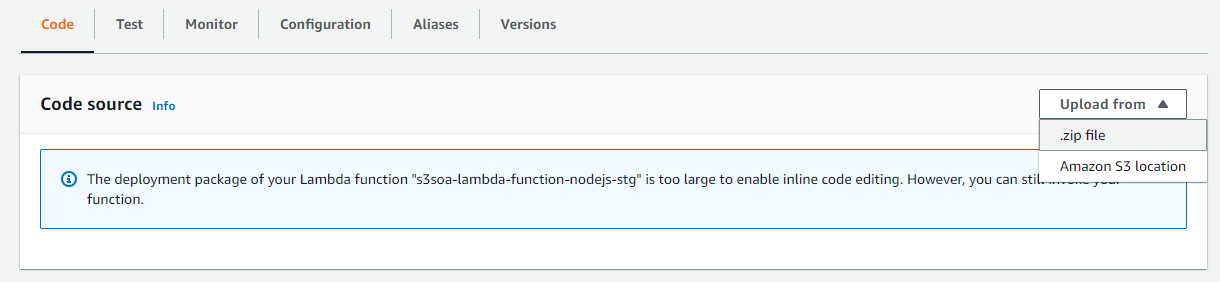
* Open AWS and navigate to Services🡪Lambda🡪Functions
* Select the desired Lambda function from the list
* Go to the ‘Configuration’ tab
* Create an environment variable in AWS Lambda configurations having the key as ‘NODE\_EXTRA\_CA\_CERTS’ and value as ‘/var/task/GEAInternalCARoot.cer’
* Go to the ‘Actions’ menu and then export the Lambda function

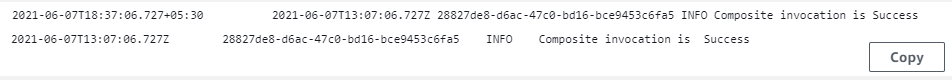


* Extract the ZIP
* Include the new certificate in the Lambda Deployment package root

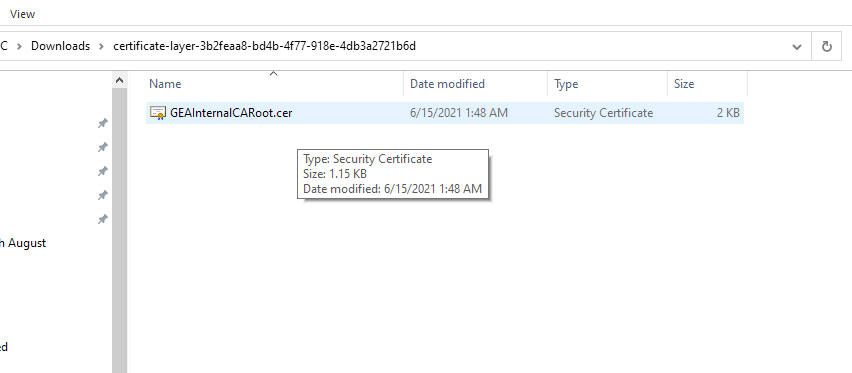
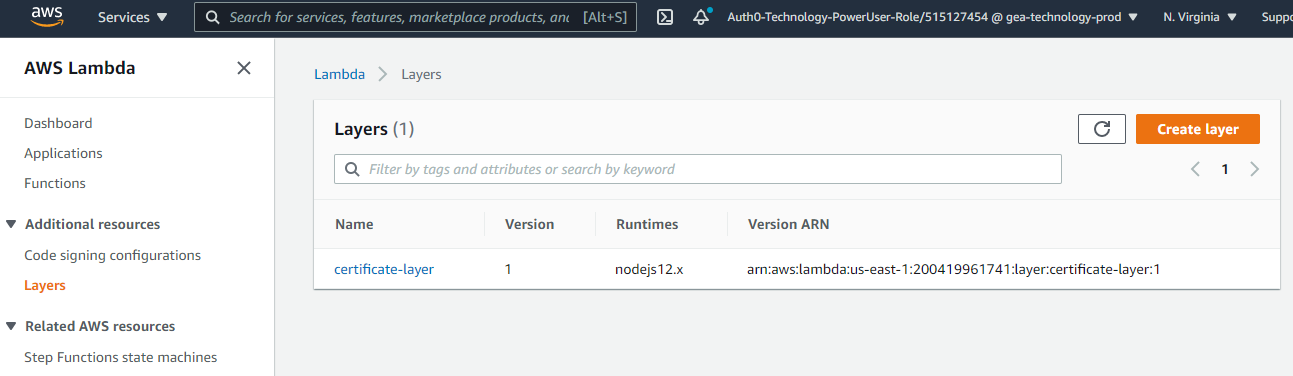
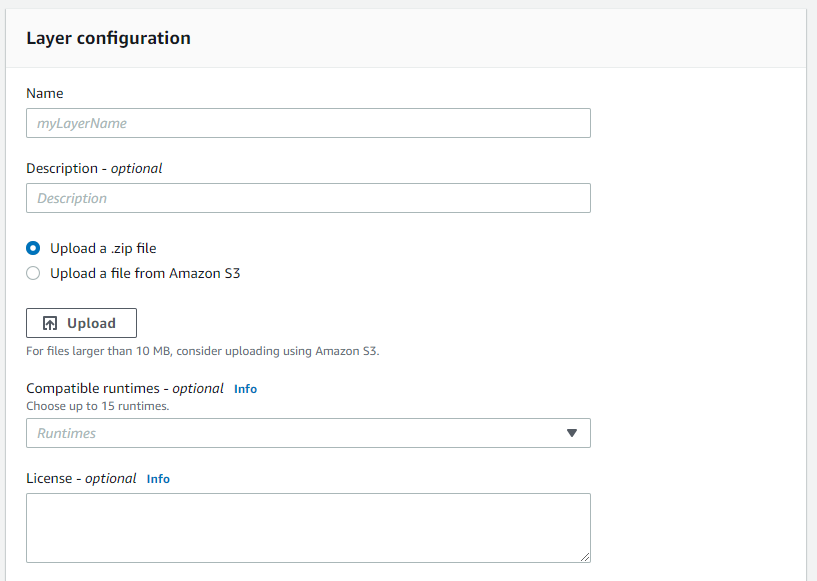
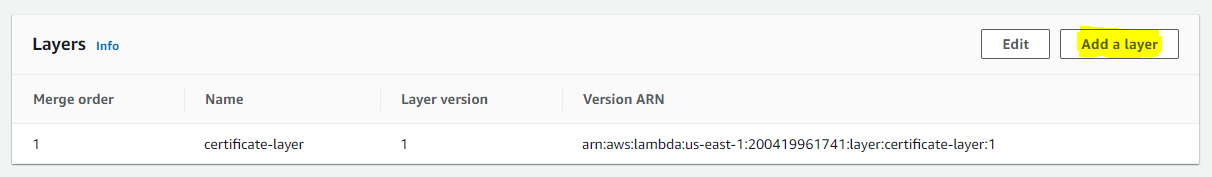
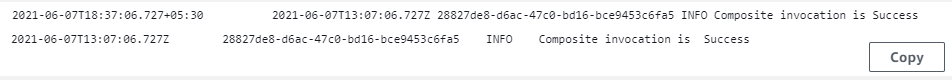


* Compress the contents of the Lambda Deployment package again into a ZIP file
* Go to the ‘Code’ tab on the Lambda function page and upload the edited ZIP



* The connection to SOA composite should succeed with the following log entry

**Method 2 (Using Lambda Layers)**

* Open AWS and navigate to Services🡪Lambda🡪Functions
* Select the desired Lambda function from the list
* Create an environment variable in AWS Lambda configurations having the key as ‘**NODE\_EXTRA\_CA\_CERTS**’ and value as ‘/opt/GEAInternalCARoot.cer’
* Create an empty folder on your local machine and place the new Certificate in it
* Compress the folder into a ZIP file
* Go to Services🡪Lambda🡪Layers🡪Create Layer
* Provide a layer name and other details. Select the runtime as 12.x. Use upload ZIP option to upload our layer ZIP file.
* Go to the Lambda function again and go to the Layers section to add it to our function
* Select your newly created layer and its version to use. If it is a newly created layer, the only version visible will be 1.
* After the above steps. The SOA composite invocation should be a success.

**Troubleshooting steps:**

* Error 503 – Check the AWS Route 53 if the outbound connections are made to the correct IP address
* Error 404 – Check with the SOA team